

2015

Regulation of unauthorised ATM/debit card transactions and consumer protection in Indonesia: a critical analysis of law and practice

Iwan Setiawan
University of Wollongong

Follow this and additional works at: <https://ro.uow.edu.au/theses>

University of Wollongong

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Setiawan, Iwan, Regulation of unauthorised ATM/debit card transactions and consumer protection in Indonesia: a critical analysis of law and practice, Doctor of Philosophy thesis, School of Law, University of Wollongong, 2015. <https://ro.uow.edu.au/theses/4836>

**UNIVERSITY OF
WOLLONGONG**



**REGULATION OF UNAUTHORISED ATM/DEBIT CARD
TRANSACTIONS AND CONSUMER PROTECTION IN INDONESIA:
A CRITICAL ANALYSIS OF LAW AND PRACTICE**

A thesis submitted in fulfilment of the
requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

from

UNIVERSITY OF WOLLONGONG

By

Iwan Setiawan

LLB (Private Law - Gadjah Mada University - Indonesia)

LLM (Internet and Electronic Law - Monash University - Australia)

FACULTY OF LAW, HUMANITIES AND THE ARTS

2015

ABSTRACT

The complex, remote, and seamless nature of ATM/debit card operations, the relatively outmoded and vulnerable technology employed in the ATM/debit card technology, the innovative and adaptive identity theft and fraud methods, and the severe asymmetry of information suffered by the consumer due to bank reluctance to provide fraud risk education have made unauthorised ATM/debit card transactions an inherent risk and real threat in the rapid development of electronic payment in Indonesia.

The absence of specific fraud liability regulation and the lack of a clear understanding of the facts about unauthorised ATM/debit card transactions have contributed to prolonged disputes between banks and consumers about who should bear liability for the losses. The deficiency in adjudicator knowledge about empirical facts that are intertwined with the unauthorised ATM/debit card transactions as well as of relevant economic and technological facts, and the legal aspects specific to ATM/debit card regulation has also made the adjudicator's decisions in the alternative dispute resolution (ADR) forum and courts tend towards being unjust and misleading, and failed to create incentives for optimum identity theft/fraud containment.

This thesis, therefore, investigates quite exhaustively the technicalities and standard operating procedures of ATM/debit card system, methods and typology of identity theft and fraud, the fraudsters, the pertinent laws and regulations, and the adjudicator's verdicts that are relevant to unauthorised ATM/debit card transactions in Indonesia. To enrich the research, comparative analysis was also undertaken with the United States and Australia's fraud liability/fraud loss allocation rules regulations.

To overcome the legal ramifications and disincentives that might otherwise occur because of lack fraud liability regulation and poor adjudicator decisions on unauthorised ATM/debit card transaction disputes, this thesis proposes law reform on Indonesian fraud liability regulations using multi-disciplinary approaches, namely economic, technological and legal. The thesis concludes by arguing that reform can be achieved by creating clear, fair, enumerated, and decisive loss allocation rules for unauthorised ATM/debit card transactions. To assure sensible adjudicator decisions, this thesis also argues that the old and unjust pure contributory negligence in legal proceedings should be replaced by the comparative negligence principle as part of the law reform.

CERTIFICATION

I, Iwan Setiawan, declare that this thesis, submitted in partial fulfilment of the requirements for the award of Doctor Philosophy in the Faculty of Law, Humanities and the Arts, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

Iwan Setiawan

October 2015

ACKNOWLEDGEMENTS

In completing this thesis I am grateful first, to my God, the almighty Allah SWT who gives me strength and guidance throughout my life, and without whom I would have no hope.

I owe so much gratitude to Doctor Charles YC Chew, my supervisor, for his supervision and dedication over the long preceding years at the University of Wollongong. The invaluable help, encouragement, and support of my supervisor, especially in my difficult times, has been inspiring, motivating and always remarkable.

My grateful acknowledgment is also extended to Adjunct Professor Duncan Chappel, Doctor Sheikh Solaiman, and Professor Andrew Goldsmith for the supervision of my thesis at the very first stage. I would also thank Associate Professor Andrew Frazer as well as Ms Elaine Newby (editorial assistance) for their help and encouragement to complete my thesis.

I express my gratitude to Bank Indonesia that sponsored my PhD candidature. I thank Ronald Waas, Doctor Kusumaningtuti Sandriharmy Soetiono, Erman Suherman, Damayanti Johan, Hilman Tisnawan, Garda T Paripurna, and Tantan Heroika Sukmadrajat, superiors and/or friends in Bank Indonesia, for their steadfast support of my PhD candidature.

Finally, I thank my wife Icha and my children Adara, Bhaskara and Chiara, for their invaluable love, help, support, patience and ‘harsh critiques’ that have enabled me to finish my thesis. My appreciation is also dedicated to my parents, my brother, and my sister who always support me and pray for my success.

TABLE OF CONTENTS

ABSTRACT	i
CERTIFICATION	ii
ACKNOWLEDGEMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES AND FIGURES.....	ix
LIST OF ACRONYMS AND ABBREVIATIONS	x
CHAPTER 1 – GENERAL INTRODUCTION	1
1.1. Background and Significance of the Study	1
1.2. The Scope and Limitations of the Study	17
1.3. The Contribution of the Study.....	18
1.4. Literature Review.....	20
1.5. Research Questions	31
1.6. Research Design.....	32
1.6.1. Methodology	32
1.6.2. Data Collection	37
1.6.3. Data Analysis	39
1.7. Outline of the Thesis	39
1.8. Conclusion	41
CHAPTER 2 – OVERVIEW OF TECHNOLOGY, SECURITY, AND PROCEDURES EMPLOYED IN BANKS’ ATM/DEBIT CARD SYSTEMS	43
2.1. Introduction	43
2.2. Banks and Payment Cards.....	43
2.3. ATM and Debit Cards.....	45
2.3.1. Consumer Activated Terminals: ATM and EFTPOS	47
2.3.1.1. Automated Teller Machines	48
2.3.1.2. EFTPOS Terminals	50
2.3.2. Card Technology	50
2.3.2.1. Plastic Card and the Magnetic Stripe	51
2.3.2.2. Integrated Circuit Card (ICC)/Chip Card.....	52
2.4. The Importance of Security Procedures in ATM and Debit Card Transactions	54
2.4.1. The Concepts of Identification, Authentication and Authorisation	55
2.4.1.1. Identification and Authentication.....	55
2.4.1.2. Authorisation.....	57
2.4.2. Identification, Authentication and Authorisation in ATM/Debit Card Transactions: ATM/Debit Magnetic Stripe Card and PIN	58
2.5. Conclusion	61
CHAPTER 3 – TYPOLOGY OF THE INHERENT RISK AND VULNERABILITIES THAT MAKE ATM/DEBIT CARD FRAUD FAVOURED BY FRAUDSTERS.....	62
3.1. Introduction	62
3.2. General Overview of Risk in Retail Payment System	62
3.3. Payment Card Fraud.....	67
3.3.1. Why Are Payment Cards Always Vulnerable to Fraud?.....	70
3.3.1.1. The Trade-off between Cost, Security and Consumer Convenience	70

3.3.1.2. Incentives for Payment Card Fraud.....	73
3.3.1.3. The ‘Balloon Effect’ in Payment Card Fraud	76
3.3.2. Inherent and Known Vulnerabilities in the Payment Card System.....	80
3.4. The Fraudsters.....	84
3.5. Conclusion	87
CHAPTER 4 – IDENTITY THEFT/IDENTITY FRAUD METHODS IN ATM/DEBIT CARD TRANSACTIONS IN INDONESIA: OPPORTUNITIES AND INCENTIVES	89
4.1. Introduction.....	89
4.2. Concept of Identity Theft and Identity Fraud in Payment Cards	89
4.2.1. Identity Theft: Types of ATM/Debit Card Attack	91
4.2.1.1. Cardholder as Point of Compromise	93
4.2.1.1.1. Third Party Fraud.....	93
4.2.1.1.2. Second Party Fraud.....	96
4.2.1.1.3. First Party Fraud	96
4.2.1.2. Consumer-Activated Terminal and Cardholder as Point of Compromise: Card Trapping.....	96
4.2.1.3. Consumer-Activated Terminal as a Point of Compromise	100
4.2.1.3.1. Swallowed ATM/Debit Card Theft at ATM’s ‘Retain Pocket’	101
4.2.1.3.2. Magnetic Stripe Card Data Theft at ATMs.....	104
4.2.1.3.3. Magnetic Stripe Card Data Theft at EFTPOS Terminals	117
4.2.1.4. ATM/EFTPOS Communication Network as Point of Compromise	127
4.2.1.5. Bank and/or Its Counterpart’s Data Centre Computer as Point of Compromise	131
4.2.2. Methods of PIN Theft	132
4.2.2.1. PIN Guessing	132
4.2.2.2. Shoulder Surfing	135
4.2.2.3. PIN Pad Overlay	136
4.2.2.4. Pinhole Camera.....	138
4.2.2.5. PIN Interception/‘Cracking’	139
4.2.3. Identity Fraud: Counterfeit Card Fraud.....	140
4.3. Identity Theft and Fraud Figures, Challenges, and the Dearth of Fraud Reports in ATM/Debit Card Transactions in Indonesia	143
4.3.1. ATM/Debit Card Fraud Figures (Unpublished).....	143
4.3.2. ATM/Debit Card Identity Theft/Fraud Methods in Indonesia	146
4.3.3. ATM/Debit Card Identity Theft/Fraud Challenges	149
4.3.4. The Dearth and Unreliability of ATM/Debit Card Fraud Reports	151
4.4. Conclusion	155
CHAPTER 5 – REGULATION OF ATM/DEBIT CARD TRANSACTIONS, CONSUMER PROTECTION, AND LIABILITY RULES ON UNAUTHORISED ATM/DEBIT CARD TRANSACTIONS IN INDONESIA — WITH A BRIEF COMPARISON TO LOSS ALLOCATION RULES IN THE UNITED STATES AND AUSTRALIA.....	158
5.1. Introduction.....	158
5.2. Legal and Regulatory Framework for ATM/Debit Card Transactions in Indonesia.....	159
5.2.1. Legal Framework for ATM/Debit Card Transactions.....	161
5.2.1.1. Law No 7 of 1992 on Banking as Amended by Law No 10 of 1998 (<i>LB</i>).....	161
5.2.1.2. Law Number 23 of 1999 on Bank Indonesia as Most Recently Amended by Law Number 6 of 2009 on the Stipulation of Government Regulation in Lieu of Law Number 2 of 2008 on the Second Amendment to the Law Number 23 of 1999 on Bank Indonesia (<i>LBI</i>)	163
5.2.1.3. Law Number 11 of 2008 on Information and Electronic Transactions (<i>LIET</i>).....	164
5.2.1.4. Government Regulation Number 82 of 2012 on The Operation of Electronic System and Transaction (<i>GR-OEST</i>).....	166

5.2.1.4.1.	Electronic Systems.....	167
5.2.1.4.2.	Electronic Agents.....	168
5.2.1.4.3.	Electronic Transaction Operation	169
5.2.1.5.	Law No 3 of 2011 on Fund Transfer (<i>LFT</i>)	170
5.2.2.	Regulatory Framework for ATM/Debit Card Transactions: Bank Indonesia Regulations Concerning the Prudential Principle, Risk Management, and Security Improvement..	171
5.2.2.1.	Prudential Provisions for Payment Cards	173
5.2.2.2.	Risk Management for Payment Cards.....	175
5.2.2.3.	Security Improvement for Payment Cards	178
5.3.	Legal and Regulatory Framework for Consumer Protection in ATM/Debit Card Transactions in Indonesia.....	180
5.3.1.	Legal Framework for Consumer Protection.....	180
5.3.1.1.	Constitution of the Republic of Indonesia 1945.....	180
5.3.1.2.	Law No 8 of 1999 on Customer Protection (<i>LCP</i>).....	181
5.3.2.	Regulatory Framework for Consumer Protection	185
5.3.2.1.	Consumer Education	186
5.3.2.2.	Resolution of Consumer Complaints	189
5.3.2.3.	Consumer Protection in Payment System Services.....	190
5.4.	Legal and Regulatory Framework of Liability Rules on Unauthorised ATM/Debit Card Transactions in Indonesia.....	191
5.4.1.	Legal Framework of Liability Rules	191
5.4.1.1.	The Indonesian Civil Code: Tortious Liability	191
5.4.1.2.	Law on Information and Electronic Transactions (<i>LIET</i>)	193
5.4.1.3.	Law No 8 of 1999 on Customer Protection (<i>LCP</i>).....	194
5.4.2.	Regulatory Framework for Liability Rules	195
5.4.2.1.	Bank Indonesia Regulation Number 14/2/PBI/2012 (<i>BIR-CBPI</i>).....	196
5.4.2.2.	Bank Indonesia Regulation Number 13/25/PBI/2011	196
5.5.	Lessons to be Learned from Other Jurisdictions Pertaining to Fraud Liability Rules on Unauthorised ATM/Debit Card Transactions	198
5.5.1.	United States: Electronic Fund Transfer Act 1978 and Regulation E.....	198
5.5.1.1.	Unauthorised and Authorised Fund Transfers	199
5.5.1.2.	Consumer's Liability for Unauthorised Funds Transfers.....	200
5.5.2.	Australia: ePayments Code	202
5.6.	Conclusion	206
CHAPTER 6 THEORY AND PRACTICE OF LIABILITY AND CONSUMER PROTECTION LAW ON DISPUTE RESOLUTION BETWEEN CONSUMER AND BANK CONCERNING UNAUTHORISED ATM/DEBIT CARD TRANSACTIONS IN INDONESIA		209
6.1.	Introduction.....	209
6.2.	Overview of Liability Law in Indonesia	209
6.2.1.	General Concept of Liability Rules and the Cause of Action	212
6.2.2.	Tortious Liability	215
6.2.3.	Vicarious Liability	218
6.2.4.	Occupiers' Liability	220
6.3.	Tort of Negligence	222
6.3.1.	Element of Negligence.....	223
6.3.1.1.	Duty of Care.....	224
6.3.1.2.	Breach of Duty of Care	225
6.3.1.3.	Causation and Scope of Liability	226
6.3.1.4.	Damages.....	228
6.3.2.	Defences in Tort of Negligence	229
6.3.2.1.	Pure Contributory Negligence.....	230

6.3.2.2. Comparative Negligence.....	231
6.3.2.3. Voluntary Assumption of Risk.....	235
6.3.2.4. <i>Novus Actus Interveniens</i> : (‘A New Intervening Act’).....	236
6.4. Consumer Protection for Unauthorised ATM/Debit Card Transactions: Concept and Practice of Dispute Resolution and Redress in Indonesia.....	239
6.4.1. Unauthorised ATM/Debit Card Transaction: Consumer as a True Victim.....	239
6.4.2. Consumer Protection in ATM/Debit Card Transactions.....	243
6.4.3. Forum to Resolve Unauthorised ATM/Debit Card Transactions: Alternative Dispute Resolution (ADR) Body and the Court.....	246
6.4.3.1. Bank Indonesia Banking Mediation Agency.....	247
6.4.3.2. Consumer Dispute Settlement Body (CDSB).....	252
6.4.3.2.1. Brief Overview.....	252
6.4.3.2.2. Unauthorised ATM/Debit Card Transaction Cases in CDSB (Which Are Then Appealed to the Court).....	255
6.4.3.3. Under Court Litigation.....	263
6.4.3.3.1. Brief Overview of Court Structures and Its Procedural Rules.....	263
6.4.3.3.2. Unauthorised ATM/Debit Card Transaction Cases in Court.....	265
6.4.3.3.3. <i>Nasruddin v PT Bank Mandiri Tbk</i> (Card Trapping Case).....	266
6.5. Conclusion.....	270
CHAPTER 7 – LAW REFORM ON THE LOSS ALLOCATION RULES AND DISPUTE RESOLUTION BETWEEN CONSUMER AND BANK CONCERNING UNAUTHORISED ATM/DEBIT CARD TRANSACTIONS IN INDONESIA.....	272
7.1. Introduction.....	272
7.2. Compelling Reasons for Law Reform on Loss Allocation Rules Concerning Unauthorised ATM/debit Card Transaction in Indonesia.....	273
7.2.1. Market Failure and Fraud Asymmetry Information in ATM/Debit Card Operation in Indonesia.....	273
7.2.2. The Absence of Clear, Fair, Detailed, and Decisive Loss Allocation Rules and Presence of Unjust Court Verdicts on Disputes between Consumers and Banks concerning Unauthorised ATM/Debit Card Transactions.....	278
7.2.2.1. Flaws in the Bank’s Internal Dispute Resolution Unit: Unjust Liability Dumping Provisions.....	280
7.2.2.2. Flaws in the Banking Mediation Agency: Increasing the Disparity and Uncertainty...280	
7.2.2.3. Flaws in the CDSB: CDSB’s Decision is not Final and Binding.....	282
7.2.2.4. Flaws in the Court: Unjust Contributory Negligence Principle.....	283
7.3. Multi-Disciplinary Approaches to Law Reform on Loss Allocation Rules concerning Unauthorised ATM/Debit Card Transactions in Indonesia: Economic, Technological, and Legal Perspectives.....	286
7.3.1. Economic Perspective: Facts and Principles.....	288
7.3.1.1. Loss Spreading Principle.....	291
7.3.1.2. Loss Reduction Principle.....	292
7.3.1.3. Loss Imposition Principle.....	293
7.3.2. Technological Perspective: Facts and Principles.....	294
7.3.2.1. Banks’ Moderate Security Technology against Flaws and Vulnerabilities in ATM/Debit Card Operation.....	298
7.3.2.2. Typology of Identity Theft/Fraud in an Unauthorised ATM/debit Card Transaction according to Its Point of Compromise.....	302
7.3.2.2.1. First Party Identity Theft/Fraud Typology.....	302
7.3.2.2.2. Second Party Identity Theft/Fraud Typology.....	302
7.3.2.2.3. Third Party Identity Theft/Fraud Typology.....	303
7.3.2.3. PIN as an Electronic Signature Has Not a Non-Repudiation Value.....	306

7.3.3. Law Perspective: Facts and Principles	310
7.4. Proposed Law Reform Implementation on Loss Allocation Rules concerning Unauthorised ATM/Debit Card Transactions in Indonesia.....	311
7.4.1. Law Reform in Civil Liability Adjudication/Litigation Proceedings	314
7.4.1.1. Civil Lawsuit Based on Tortious Liability: Breach of Statutory Duty (Negligence Per Se) 314	
7.4.1.2. Civil Lawsuits Based on Tortious/Negligence Liability: Comparative Negligence instead of Contributory Principle on Unauthorised ATM/Debit Card Transaction Disputes in ADR/Court Proceedings with Multi-Disciplinary Approaches: Economic, Technological and Legal	317
7.4.1.2.1. Burden of Proof: Plaintiff v Defendant.....	317
7.4.1.2.2. Test for Comparative Negligence: Between Bank and/or Consumer Negligence.....	323
7.4.2. Law Reform on Fraud Liability Rules by Creating Clear, Fair, Detailed, and Decisive Unauthorised ATM/Debit Card Loss Allocation Regulations in Indonesia.....	362
7.4.2.1. Between US and Australia Approaches to Fraud Liability Rules	362
7.4.2.2. The ePayments Code Model and Its Prospects of Settling Unauthorised ATM/Debit Card Transaction Disputes between Banks and Consumers in Indonesia.....	365
7.4.2.2.1. When the Bank is Liable for the Loss.....	366
7.4.2.2.2. When the Consumer/Cardholder is Liable for the Loss.....	367
7.4.2.2.3. Consumer/Cardholder Limited Liability.....	368
7.4.2.2.4. Proof that a User Contributed to Losses	369
7.5. Conclusion	371
CHAPTER 8 – THE FINAL DENOUEMENT	374
BIBLIOGRAPHY	389
APPENDICES	422

LIST OF TABLES AND FIGURES

Tables	Page
Table 1: Type of ATM/Debit Card Fraud and Data	145
Table 2: Consumer Rights v Business actors Obligation	184
Table 3: ATM/Debit Card Point of Compromise, Attacker, Identity Theft, Prevention/Mitigation Method and Least Cost Avoider.....	304
Table 4: ATM/Debit Card Point of Compromise, Identity Theft Methods and Bank Statutory Duties	315
Table 5: ATM/Debit Card Point of Compromise, Identity Theft Methods and Comparative Negligence Loss Allocation Percentage	361
 Figures	
Figure 1: Law Reform Research Process	36
Figure 2: Example of ATM/Debit Card Data on the Magnetic Stripe Card...	52
Figure 3: The Balloon Effect in Payment Card Fraud	80
Figure 4: Card Trapping (Lebanese Loop).....	99
Figure 5: Examples of Fake Bank Call Centre Details Affixed to ATMs in Indonesia.....	100
Figure 6: Mini Magnetic Stripe Card Reader.....	107
Figure 7: MSR206 Magnetic Swipe Encoder	107
Figure 8: The Extracted Components of a Mini-123 Card Reader Removed from its Manufactured Packaging and Repackaged for Use in a Fake ATM Fascia.....	108
Figure 9: Imitation ATM Fascia – Front and Rear View.....	108
Figure 10: Various ATM Skimmers on the ATM.....	109
Figure 11: Rear of an ATM Skimmer with SMS Capability.....	111
Figure 12: Anti-Skimming or ‘Duck Snout’ at a Bank ATM in the South of Sumatra (Indonesia).....	112
Figure 13: ATM Anti-Skimmer Skimmer and Skimmer.....	126
Figure 14: Bank EFTPOS Machine (Blue) and Merchant’s Card Skimmer (in Red Circle).....	126
Figure 15: Author Payment Card Tracks 1 and 2 Data on Merchant Cashier’s Monitor (inside Red Circle).....	135
Figure 16: ATM PIN Pad	137
Figure 17: PIN-Pad Overlay	138
Figure 18: Hidden Camera in False Panel above PIN Pad.....	138
Figure 19: Pinhole Camera in Brochure Holder	335
Figure 20: Flow Chart of Tests for Negligence	

LIST OF ACRONYMS AND ABBREVIATIONS

ABA	American Bankers Association
ABIO	Australian Banking Industry Ombudsman
ACH	Automated Clearing House
ADR	Alternative Dispute Resolution
ASIC	Australian Securities and Investments Commission
ATM	Automated Teller Machine
BCA	Bank Central Asia
BCBS	Basel Committee on Banking Supervision
BI	Bank Indonesia
BID-Chip & PIN	Bank Indonesia Circular Letter Number 14/23/DASP Concerning Amendment of Bank Indonesia Circular Letter Number 13/22/DASP Concerning Implementation Chip Technology and the Use of Personal Identification Number on ATM and/or Debit Card Issued in Indonesia] (BID-Chip & PIN).
BID-CP & Security	Bank Indonesia Decree Number 11/10/DASP Concerning the Operation of Card-Based Payment Instrument Activities as Amended by Bank Indonesia Decree Number 14/17/DASP
BID-RMUITCB	Bank Indonesia Decree Number 9/30/DPNP Concerning Risk Management in the Use of Information Technology by Commercial Banks
BIR RCC	Bank Indonesia Regulation Number: 7/7/PBI/2005 Concerning Resolution of Customer Complaints as Amended by Bank Indonesia Regulation Number 10/10/PBI/2008
BIR-CBPI	Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Card Based Payment Instrument Activity as Amended by Bank Indonesia Regulation Number 14/2/PBI/2012 Concerning Amendment of Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Operation of Card-Based Payment Instrument Activities
BIR-GCG	Bank Indonesia Regulation Number 8/4/PBI/2006 Concerning Implementation of Good Corporate Governance for Commercial Bank as Amended by Bank Indonesia Regulation Number 8/14/PBI/2006
BIR-RMUITCBs	Bank Indonesia Regulation Number 9/15/PBI/2007 Concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks
BIR-TBPI&UBCPD	Bank Indonesia Regulation Number 7/6/PBI/2005 Concerning Transparency of Banking Product Information and the Use of Bank Customers' Personal Data
BIR-CPPSS	Bank Indonesia Regulation Number 16/1/PBI/2014 Concerning Consumer Protection on Payment System Services
BIS	Bank for International Settlement
BNI	Bank Negara Indonesia
BRI	Bank Rakyat Indonesia
CCTV	Closed Circuit Television
CDSB	Consumer Dispute Settlement Body
CI	Consumers International

CNP	Card Not Present
CPSS	Committee on Payment and Settlement Systems
EDC	Electronic Data Capture
EFT Code	Electronic Funds Transfers Code of Conduct
EFT	Electronic Funds Transfers
<i>EFTA</i>	<i>Electronic Fund Transfer Act of 1978</i> (15 USC 1693)
EFTPOS	Electronic Funds Transfer at Point of Sale
EMEAP	Executives Meeting of East Asia-Pacific Central Banks and Monetary Authorities
EMV	Europay, Mastercard and Visa
EPB	Encrypted PIN Block
EU/EEA	European Union/European Economic Area
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institution Examination Council
GR-OEST	Government Regulation of the Republic of Indonesia Number 82 of 2012 on Electronic System and Electronic Transaction
HIR	Herziene Inlandsch Reglement
ICC	Integrated Circuit Card
ICT	Information and Communication Technologies
ID-CERT	Indonesia Computer Emergency Response Team
IDR	Indonesian Rupiah
IDS	Intrusion Detection System
ISO	Independent Sales Organisation
LAADR	Law Number 30 of 1999 Concerning Arbitration and Alternative Dispute Resolution
LB	Law Number 7 of 1992 on Banking as Amended by Law Number 10 of 1998
LBI	Law Number 23 of 1999 was later amended by Law No 6 of 2009 on Stipulation of Government Regulation in Lieu of Law No 2 of 2008 on the Second Amendment Law No 23 of 1999 on Bank Indonesia Becomes Law
LCP	Law Number 8 of 1999 on Consumer Protection
LFT	Law Number 3 of 2011 on Fund Transfer
LIET	Law Number 3 of 2011 on Information and Electronic Transactions
MOTO	Mail Order/Telephone Order
NSW	New South Wales
OECD	Organisation for Economic Co-Operation and Development
PAN	Primary Account Number
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
RBA	Reserve Bank of Australia
RBg	Rechtsreglement voor de Buitengewesten
SEACEN	South East Asian Central Bank
UK	United Kingdom
UN	United Nations
UNCITRAL	United Nation Commission on International Trade Law
US	United States of America
YLKI	Yayasan Lembaga Konsumen Indonesia

I'm quite certain that if the infamous Willie Sutton had his heyday in the present culture, Sutton's fabled answer to the question of why he robbed online banks would have been, "Because that's where the *easy* money is".¹

Brian Krebs (2010)²

CHAPTER 1 – GENERAL INTRODUCTION

1.1. Background and Significance of the Study

In the development of electronic commerce, electronic payment methods and retail electronic banking services and products are very important and provide significant new opportunities for banking business.³ Banking consumers can now access a wide selection of banking products and services more efficiently through an electronic or digital distribution channel referred to as electronic banking or e-banking.⁴ Nowadays, e-banking is used by banking consumers by way of its many features, such as automated

¹ William 'Willie' Sutton (30 June 1901 – 2 November 1980) was a prolific US bank robber. Executing robberies in disguises, he gained two nicknames, 'Willie the Actor' and 'Slick Willie'. He claimed to have stolen approximately \$2 million during his four decade long 'career', and although he broke out of prison three times, he ended up spending more than half his adult life there. See Peter Duffy, 'CITY LORE; Willie Sutton, Urbane Scoundrel', *The New York Times* (online), 17 February 2002 <<http://www.nytimes.com/2002/02/17/nyregion/city-lore-willie-sutton-urbane-scoundrel.html>>.

² Brian Krebs, *Cyber Crooks Leave Traditional Bank Robbers in the Dust* (13 March 2010) <<http://krebsonsecurity.com/2010/03/cyber-crooks-leave-bank-robbers-in-the-dust/>>.

³ Basel Committee on Banking Supervision (BCBS), *Risk Management for Electronic Banking and Electronic Money Activities* (Bank for International Settlements, 1998) 1.

⁴ In the banking industry, the terms 'consumer' and 'customer' are both used frequently and interchangeably. According to <DifferenceBetween.net>, by definition, 'a customer is someone who buys services or goods from someone else while a consumer is someone that consumes a certain product or commodity'. In Indonesia, a difference is seen to exist. A 'bank consumer' or '*nasabah bank*' is someone that has a legal relationship with banks (has signed a bank-consumer contract) to utilise one or more of a bank's services or products, such as contract to open a saving or deposit account, credit line agreement, etc. In contrast, a bank 'customer' is someone that might utilise one or more of a bank's services or products but does not have a specific consumer-bank contract (for example, a 'walk in' customer wanting a bank cheque or money changed). In this thesis, however, 'consumer' is used to cover consumers, and specifically refers to a person who has an account at a bank (business actor) and is equipped with the relevant ATM/Debit card as a means to conduct electronic funds transfer (EFT) at an ATM or via EFTPOS. See Julita, *Difference between Customer and Consumer* (12 January 2011) DifferenceBetween.net <<http://www.differencebetween.net/language/difference-between-customer-and-consumer/>>.

teller machines (ATMs),⁵ credit cards,⁶ ATM cards,⁷ debit cards,⁸ ‘electronic funds transfer at the point of sale’ (EFTPOS) transactions,⁹ mobile transactions, and Internet banking.¹⁰ E-banking also involves ‘electronic funds transfer’ (EFT).¹¹

The rapid development of e-banking services carries both risks as well as benefits. Both brick-and-mortar companies and criminal organisations have shifted their focus to the ‘cyber world’ in the pursuit of wealth opportunities.¹² Fraudsters have found that e-banking transactions can provide great potential rewards with little risk of detection. Both consumers and banks are seriously concerned about e-banking fraud,¹³ particularly

⁵ See Committee on Payment and Settlement Systems (CPSS), *A Glossary of Terms Used in Payment and Settlement Systems* (Bank for International Settlements, revised ed, 2003) 8 (CPSS, *A Glossary of Terms*). Text of this document can be retrieved from: <<http://www.bis.org/publ/cpss00b.pdf?noframes=1>>. Automated teller machine or (ATM) is ‘an electromechanical device that permits authorised users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services, such as balance enquiries, transfer of funds or acceptance of deposits. ATMs may be operated either online with real-time access to an authorisation database or offline.’

⁶ Ibid 16: A credit card is ‘a card indicating that the holder has been granted a line of credit. It enables the holder to make purchases and/or withdraw cash up to a prearranged ceiling; the credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is charged on the amount of any extended credit and the holder is sometimes charged an annual fee.’

⁷ See art 1.5 *Peraturan Bank Indonesia Nomor: 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor 14/2/PBI/2012 Tentang Perubahan Atas Peraturan Bank Indonesia Nomor 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu* [Bank Indonesia Regulation Number: 11/11/PBI/2009 Concerning Card Based Payment Instrument Activity as amended by Bank Indonesia Regulation Number 14/2/PBI/2012 Concerning Amendment of Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Operation of Card-Based Payment Instrument Activities] (*BIR-CBPI*): ‘ATM card is a card-based payment instrument that can be used for cash withdrawal and/or fund transfer in which cardholder obligation fulfil immediately by debiting cardholder fund in Bank or other institution that have authorisation to raise fund in accordance to applicable law.’

⁸ See also: CPSS, *A Glossary of Terms*, above n 5, 19: A debit card is ‘card enabling the holder to have his purchases directly charged to funds on his account at a deposit-taking institution (may sometimes be combined with another function, e.g. that of a cash card or cheque guarantee card).’

⁹ Ibid 38: EFTPOS is a term that ‘refers to the use of payment cards at a retail location (point of sale). The payment information is captured either by paper vouchers or by electronic terminals, which in some cases are designed also to transmit the information. Where this is so, the arrangement may be referred to as “electronic funds transfer at the point of sale” (EFTPOS).’

¹⁰ Saleh M Nsouli and Andrea Schaechter, ‘Challenges of the E-Banking Revolution’ (2002) 39(3) *Finance and Development* <<http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm>>.

¹¹ Federal Trade Commission, *Facts for Consumers: Electronic Banking* (2012) <<http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre14.shtm>>.

¹² Phil Williams, ‘Organized Crime and Cybercrime: Synergies, Trends, and Responses’ (2001) <<http://www.crime-research.org/library/Cybercrime.htm>>.

¹³ For fraud definition in Indonesia, see *Surat Edaran Bank Indonesia Nomor 13/28/DPNP Tanggal 9 Desember 2011 Perihal Penerapan Strategi Anti Fraud bagi Bank Umum* [Bank Indonesia Circular Letter Dated 9 December 2011 Concerning Implementation of Anti-Fraud Strategi for Commercial Bank] (purposeful neglect undertaken in order to deceive, cheat, or manipulate bank, customer, or another party, that occurs inside the bank and/or using a bank’s facility so as to cause the bank, customer, or another party to suffer a loss and/or to cause the fraudster gain a financial benefit, both directly and indirectly’.

unauthorised EFT,¹⁴ that targets internet banking, phone banking, and credit and ATM/debit card (payment card) transactions.¹⁵

Fraudsters have equipped themselves with modern and sophisticated technologies and, in response to anti-fraud security measures adopted by financial institutions, are continuously developing their capabilities to avoid the risk of being caught. They continue to pursue their dishonest activities and reap the benefits of ineffective bank security systems, particularly in relation to obtaining e-banking passwords and account information.¹⁶

Many scholars, such as Gifford,¹⁷ Davidson,¹⁸ and Phair,¹⁹ have noticed that technology creates the possibility of e-banking crimes of great magnitude and complexity being committed quickly and anonymously. Such crimes include unauthorised system access, and both employee fraud (bank employee, merchant or bank's third party agent), and card payment fraud. Iannacci and Morris²⁰ have identified in their studies different types of payment card fraud, including account application fraud;²¹ account takeover;²² use of

¹⁴ See Australian Securities & Investments Commission (ASIC), *ePayments Code* (29 January 2014) <<http://www.asic.gov.au/epaymentscode>> ('ePayments Code'). Text of this document can be retrieved from: <<http://asic.gov.au/for-consumers/codes-of-practice/epayments-code/>>. In Australia, the ePayments Code regulates consumer electronic payment transactions, among other things are ATM, EFTPOS, credit card transactions, online payments, internet and mobile banking, and BPAY. Previously, it was known as the Electronic Funds Transfer Code of Conduct (*EFT Code*) which had existed since 1986.

The ePayments Code defines unauthorised transactions as 'transactions which are not authorised by a user. It does not apply to any transaction carried out by the user or by anyone performing a transaction with the user's knowledge and consent'. Further, under US *Regulation E* § 205.2(m), 'an "unauthorized electronic fund transfer" is "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit...".'

¹⁵ Iman Sjahputra, *Perlindungan konsumen Dalam Transaksi Elektronik* [Consumer Protection in Electronic Transaction] (Alumni, 2010) 87.

¹⁶ Australian Securities & Investments Commission (ASIC), 'Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC Proposals' (2008) 9.

¹⁷ Nick Gifford, *Information Security: Managing the Legal Risk* (CCH Australia Limited, 2009) 29–37.

¹⁸ Alan Davidson, *The Law of Electronic Commerce* (Cambridge University Press, 2009) 292–5.

¹⁹ Nigel Phair, *Cybercrime: The Reality of the Threat* (E-Security Publishing, 2007) 15–40.

²⁰ Jerry Iannacci and Ron Morris, *Access Device Fraud and Related Financial Crimes* (CRC Press LLC, 2000) 30.

²¹ 'A type of ID theft crime in which payment cards are obtained through a fraudulent application process using stolen or counterfeit documents': INTERPOL, *Payment Cards* (2010) <<http://www.interpol.int/Public/CreditCards/Default.asp>>.

²² 'Another type of ID theft crime, usually involving 'deception of a financial institution, re-issue of a payment card and its redirection to a different address': Ibid.

cards that are lost/stolen,²³ altered,²⁴ or counterfeit;²⁵ or criminal activity involving ‘card not present’ (CNP) transactions,²⁶ merchant collusion,²⁷ and cardholder fraud.²⁸

Banks have long been well aware of the range of perpetrators or masterminds of unauthorised EFT targeting bank ATMs or EFTPOS terminal facilities. They can have had an association with the bank (employees, subcontractors or consumers) or be from completely outside its population (external or unrelated fraudsters). In some instances, the fraudster can be a third party, or bank employee or an employee of its agent that has access to or knows how to defraud ATMs or EFTPOS terminals. However, there also is the possibility that the fraudsters are the cardholders themselves who misuse their own PIN deliberately or inadvertently. According to Iannacci and Morris,²⁹ cardholder fraud occurs when a card payment customer receives a card under his or her own identity but with the intent to defraud the issuer.

In Indonesia, from author’s research result — many of the bank ATMs/EFTPOS machines in use today are not state-of-the-art machines. They would require much effort for security to be enhanced to meet more acceptable contemporary standards. This situation is exacerbated by the current practice of operators of ATMs and EFTPOS terminals (banks, Independent Sales Organisations (ISOs) and switching companies)³⁰ which fail to furnish all their infrastructure with the best closed circuit television

²³ ‘This type of fraud involves misuse of actual cards that have been either lost [by] or stolen from the genuine cardholder’: Ibid.

²⁴ ‘Any access device that is changed in any way to change the appearance or electronic information contained within the device is said to be altered. Criminals often use stolen, valid card numbers on stolen devices to create the appearance of a valid card’: Iannacci and Morris, above n 20, 29.

²⁵ ‘Fraud undertaken using plastic cards that have been specifically produced or existing cards that have been altered. These cards are encoded with illegally obtained payment card account data in order to pay for goods and services or to withdraw cash’: INTERPOL, *Payment Cards*, above n 21.

²⁶ Fraud committed ‘using payment card account data to undertake transactions where there is no face-to-face contact between the seller and purchaser. Typically, this type of fraud is committed by Internet, mail order or telephone. Card not present (CNP) fraud is currently the fastest growing payment card related type of fraud in many areas of the world’: Ibid.

²⁷ Sometimes a merchant will work in concert with the criminal to perpetrate the fraud. Not only do employees working for merchants get involved in these schemes, but the company owners also do.

²⁸ Cardholder fraud occurs when a credit card customer receives a credit card under his own identity but with the intent to defraud the issuer.

²⁹ Iannacci and Morris, above n 20, 30.

³⁰ A ‘switching company’ is a company that operates a system used to switch/route card-based payment instrument transactions from certain financial acquirer systems (such as ATM and EFTPOS) to an issuer system for authorisation purposes. In Indonesia, a switching company is one of the payment system providers governed by the Bank Indonesia Regulation (*BIR-CBPI*). In this regulation, a switching company is also treated as a ‘clearing and settlement agent’, because it provides clearing and settlement for banks that utilise its services. In this regard, a switching company requires operational licence prior their operation from Bank Indonesia.

(CCTV) function (that is, fully operational and able to record the ATM/EFTPOS environment for a reasonable length of time with good quality). This situation was later confirmed in the author's interviews with bank officers (conducted during fieldwork in Jakarta), when they admitted that due to storage capacity problems, most ATM CCTV systems only record CCTV footage for one week (depending upon how busy each ATM is — since the recording function of some ATMs is triggered by the consumers attendance). Once the CCTV storage is full, the system will automatically delete the CCTV footage without creating back-up files. The quality of the video-recording (where it does exist) is often also not clear and the footage dark.³¹

Author's investigation also revealed that most banks also do not employ sophisticated transaction analysis and monitoring systems in effecting the EFT (known as neural network application), such as in a credit card's *neural system*.³² Sullivan asserts that in such a neural system, '[r]isk parameters used in the analysis might include the location of the transaction, the number and value of recent transactions, the specific merchant where the transaction is taking place, and so on.'³³

Due to a lack of security standards, monitoring, and consumer education, as well as unclear fraud liabilities regulation and loss allocation rules, and relatively ineffective oversight of the bank payment card system in Indonesia, much payment system infrastructure may operate quite smoothly but fail to maximise the protection of its consumers. This inadequate practice in the payment system seems to go unnoticed by both consumers and authorities, and often leads to a massive occurrence of crime.

³¹ See, eg, Bank Officer 1 (BO-1); BO-2; BO-3. See also Dian Ade Permana, *Rekaman CCTV Gelap, Petugas Terjunkan TIM* [CCTV Record Dark, Law Enforcer Deploy Team] (20 March 2009) Wonogiripos.com <<http://www.wonogiripos.com/2009/jogjapolitan/kota-jogja/rekaman-cctv-gelap-petugas-terjunkan-tim-130451>>. Note persons interviewed are de-identified when reluctant to be named in citation. Category is indicated by letters, the number is the interviewee number (BO =Bank Officer). For details, see Design Methodology [1.6.1] below.

³² Dominique Rambure and Alec Nacamuli, *Payment Systems: From the Salt Mines to the Board Room* (Palgrave Macmillan, 2008) 67. In the credit card system, in order to ensure the authenticity of the card holder, sophisticated transaction monitoring systems are employed by credit card providers. These systems detect unusual activity or behaviour patterns (including geographically separated locations combined with transaction time) on an account and can take the appropriate actions to stop fraud as early as possible. For example of neural network policy, see Visa Neural Networks (24/7 Monitoring): Visa, *Counterfeit Fraud* (2010) <http://www.visa.ca/en/personal/pdfs/counterfeit_fraud.pdf>.

³³ Richard J Sullivan, 'Can Smart Cards Reduce Payments Fraud and Identity Theft?' (2008) 93 *Economic Review (Kansas City)* 35, 40–1. In the absence of the implementation of the neural network system to proprietary ATM/debit cards systems in Indonesia, if there are ATM/debit card transactions that should be suspected to be unauthorised — such as cash withdrawals performed repeatedly on the same ATM or different ATMs (either domestically or overseas) almost at the same time — these will go undetected by both banks and (at least initially) by customers. In most cases, banks in Indonesia will only become aware of the unauthorised ATM/debit transactions if bank customers report them.

Consequently, unauthorised payment card transactions in Indonesia have existed for quite a long time as is evidenced by revelations within bank meetings themselves as early as the 1990s.³⁴ A storm of ATM/debit card fraud incidents was reported in January 2010 throughout all provinces in Indonesia (though more concentrated in Bali) and involved a great loss of funds.³⁵ Based on monthly reports from banks to Bank Indonesia (BI) as the Central Bank of the Republic of Indonesia, skimming devices were very frequently used at various banks' ATMs in Bali to perpetrate fraud on consumer ATM/debit cards. Hundreds of consumers from at least 10 banks became victims of these frauds, involving losses of least IDR12.1 billion. Even more alarming news came from a statement by the Chief of Bali Police suggesting that the fraud was being committed by syndicates with potential links to known criminal groups in Australia, Russia and Canada.³⁶

EFT fraud occurs at varying levels of criminal professionalism and criminal intent. With the proliferation of EFT transactions around the globe and relatively common and standardised technology being used by banks around the world (to enable

³⁴ In 1997, the author attended a meeting at Bank Indonesia, where one of the commercial banks reported the occurrence of ATM skimming that causes the loss of bank consumers' money. In general, consumers do not want to report the loss to the police as they wish to avoid further complications and the possibility of the occurrence of additional 'administrative' costs requested by the police. In the case of crimes reported to police, the police generally enter the data of e-banking fraud as ordinary 'theft', which results in the data related to e-banking fraud in particular to not be accessible as a separate category on the database, making it impossible to know the trends in e-banking crime 'year on year'; however, there are several unauthorised EFT transactions cases that have been successfully prosecuted by the police, where perpetrators have been arrested, tried and sentenced by a court, eg: John Petrus (Indonesian), ATM skimmer, was sentenced to 6 years' imprisonment imposed by the Central Jakarta District Court (verdict number 532/PID.B/2003/PH.JKT.PST, 4 June 2003); Eng Kim Hook (Malaysian), ATM skimmer, was sentenced to 3 years' imprisonment by the Central Jakarta District Court (verdict number 427/PID.B/2003/PN.JKT.PST, 12 June 2003). In 2007, the Indonesian Police Department had much success in uncovering the world's biggest credit card counterfeiting network and apprehended more than 14 suspects in Indonesia, although the two Malaysian citizens believed to be the masterminds of the fraud remained at large. The Indonesia Credit Card Association has asserted that loss due to credit card fraud in Indonesia in 2007 was around IDR 30 trillion. See: *Polri Diakui Berhasil Ungkap Jaringan Pemalsuan Kartu Kredit Terbesar Dunia* [Republic of Indonesia Police (Polri) Admitted has Success to Revealed World Biggest Credit Card Counterfeiting Network] (12 March 2008) Antara News.Com <<http://www.antaranews.com/view/?i=1205297983&c=NAS&s=>>>.

³⁵ Russell, Douglas, *ATM Skimming/Skimming/Data Compromise* (January 2010) ATMSecurity.Com <<http://www.atmsecurty.com/monthly-digest/atm-security-monthly-digest/atm-fraud-security-digest-january-2010.html>>. See also 45 *Nasabah Laporkan Pembobolan ATM di Bali* [45 Consumers Report Thieves on ATM in Bali] (29 January 2010) Antara News <<http://www.antarasumbar.com/berita/nasional/d/0/78396/45-nasabah-laporkan-pembobolan-atm-di-bali.html>>.

³⁶ Anita Rachman and Emmy Fitri, *ATM Skimming Attacks Signal Bank Security Shortcomings* (22 January 2010) JakartaGlobe <<http://www.thejakartaglobe.com/archive/atm-skimming-attacks-signal-bank-security-shortcomings/>>. See also 119 *Foreigners Arrested for ATM Skimming* (20 October 2015) The Jakarta Post <<http://www.thejakartapost.com/news/2015/10/20/119-foreigners-arrested-atm-skimming.html>>.

interoperability of payment system transactions between different banks domestically or internationally), there is a growing trend of involvement of transnational criminal organisations in EFT fraud all over the world. This is exacerbated by easy, low cost and rapid movement of people between countries and the number of underground chat rooms and web pages on the Internet that provide information and access to fraud methods, techniques and devices.

Besides the ATM incident, EFTPOS machines at Body Shop merchants in Indonesia also came under massive attack from fraudsters that affected thousands of payment card consumers in Indonesia ('the *Body Shop case*') at the end of 2013.³⁷ Likewise, in the Body Shop EFTPOS machine attacks, international syndicates were apparently also involved in the fraud operation.³⁸ In early 2014, when Bank's ATM security had been relatively improved, an ATM skimming incident that targeted consumers of Bank Central Asia (BCA) (the biggest private bank) again occurred, causing total losses of around IDR1.2 billion. A group of fraudsters from overseas had once again perpetrated this ATM skimming fraud. This time, they came from a neighbouring country, Malaysia.³⁹ Jahja Setiaatmadja, a Bank Central Asia (BCA) president and director, admitted that ATM transactions are very difficult for the bank to monitor since it involves monitoring more than two million transactions per day that occur at thousands of ATMs. This is exacerbated by the possibility of the use of other banks' ATMs as a result of a national ATM interoperability program in Indonesia.⁴⁰ Meanwhile, Bank Mandiri — the biggest government bank in Indonesia — had to shut down their ATM operation for two days in early May 2014, to prevent loss from suspected ATM/debit

³⁷ Gina Nur Maftuhah, *Pencurian Data Body Shop Terjadi di Jakarta & Padang* [Body Shop Data Theft Happened in Jakarta & Padang] (25 March 2013) Okezone.com <<http://economy.okezone.com/read/2013/03/25/457/780852/pencurian-data-body-shop-terjadi-di-jakarta-padang>>.

³⁸ Ibid.

³⁹ Tri Artining Putri, '*Sindiket Malaysia Pembobol ATM Dibekuk* [Malaysia's ATM Theft Syndicate is Apprehended]', *Koran Tempo*, 4 March 2014, 5. In this fraud event, there were 112 BCA consumer accounts that had been reported compromised by the ATM skimming fraud method, which was accompanied by a hidden pinhole camera to capture a consumer's PIN number. However, it is believed that more accounts were actually being compromised but have not yet been reported. A group of 21 perpetrators from Malaysia is believed to be involved in this fraud; 15 of them are still at large while the rest were successfully apprehended by Indonesian police.

⁴⁰ Ibid.

card data skimming that compromised more than 2000 cardholders' data in their system.⁴¹

Unauthorised payment card transactions can lead to the consumer and/or bank incurring direct financial losses. However, consumers with unauthorised ATM/debit card transactions suffer more compared to those with unauthorised credit card transactions. Even though payment card fraud will cause problems and anxiety for both types of cardholders, the levels differ, with ATM/debit cardholders suffering worse repercussions. Signature credit card holders are 'spoiled' by the many different types of protection offered by the issuer/principal (scheme networks such as Visa and MasterCard), with such protection including state-of-the-art Europay, Mastercard and Visa (EMV) chip technology for these payment cards (also able to be used in the debit card scheme network), zero liability rules for unauthorised transactions,⁴² the existence of a neural network system, monthly statements (along with consumer education material that covers areas such as fraud threat), and proactive notification by a bank officer when unusual patterns of transactions have occurred. In contrast, all these useful risk management features do not yet exist for proprietary ATM/debit card transactions or PIN based scheme network debit card in Indonesia that are a focus of this thesis.⁴³

To make matters more complicated for the ATM/debit cardholder, if fraud does occur, it is their money in the bank that is missing, not the bank's money as is the case in credit card fraud. As indicated previously, most of the banks have not equipped their ATM/debit card system with *neural network programs* nor do they issue regular monthly transaction statements such as is the case for the credit card system. Hence, in most instances, by the time an ATM/debit card consumer notices unauthorised ATM/debit transactions on their account, their money has already been simply drained

⁴¹ See Wahyu Daniel, *ATM Sejumlah Nasabah Diblokir, Ini Penjelasan Bank Mandiri* [Numbers of Consumer's ATM Blocked, this is Bank Mandiri's Explanation] (13 May 2014) <http://finance.detik.com/read/2014/05/12/205424/2580730/5/atm-sejumlah-nasabah-diblokir-ini-penjelasan-bank-mandiri>.

⁴² The zero liability policy of Visa and MasterCard basically eliminates consumer liability for fraudulent transactions. However, this protection has several conditions and only applies to signature-based payment cards. Hence, any fraudulent transactions that happen in PIN based scheme networks - debit/credit card (such as Visa or MasterCard), then the resolution for unauthorised transactions and bank liability will be governed in accordance with the cardholder agreement with the issuing bank. See MasterCard, *MasterCard Zero Liability* (2012) <<http://www.mastercard.com.au/zero-liability.html>>; Visa, Counterfeit Fraud, above n 32.

⁴³ The term 'proprietary ATM/Debit' is used in this thesis to distinguish between the original bank-issued ATM/debit cards and scheme networks debit cards (from Visa and MasterCard). However, all these payment cards cover EFTPOS and ATM transactions.

from the account. This situation can become worse, when money in the account is the only resource for covering daily living expenses or is the source of other payment obligations such as the fund on which cheques are drawn or from which utility accounts are directly debited.⁴⁴

Following the loss, some consumers try to seek recourse (in this case, damages) from their bank. However, most claims regarding unauthorised ATM/debit card transactions (also known as ‘phantom withdrawals’) are rejected by the banks. As a last resort, consumers usually will write of their ordeal to the mass media or utilise social media. The purpose is simple: to seek attention in order to gain help and a better resolution from the bank itself or others. In most cases, a bank will use their right to refute consumer allegations by repeating the reason for their initial decision, that is, that the disputed transactions were deemed valid because of the use of the correct card and PIN.⁴⁵ Nevertheless, some banks will recompense consumers for their loss only if the fraud incident is widely publicised in the mass media (in that instance to avoid

⁴⁴ See Krista Tedder, 'Now You See It, Now You Don't: A Review of Fraud Costs and Trends' (A First Data White Paper, First Data, 2009) 7; Claes Bell, *4 Places Where You Don't Want To Swipe Your Debit Card*, *Business Insider* (4 January 2012) <http://articles.businessinsider.com/2012-01-04/news/30587769_1_debit-card-card-terminals-skimmers>; Gail Hillebrand, 'Before the Grand Rethinking: Five Things To Do Today with Payments Law and Ten Principles To Guide New Payments Products and New Payment Law' (2009) 83(2) *Chicago-Kent Law Review* 769, 774; ConsumerReports.org, *Debit-Card 'Skimming' Scams* (16 January 2010) Media Indonesia Online <<http://www.indonesiamedia.com/2010/01/16/debit-card-skimming-scams/>>. See also Edward A Morse and Vasant Raval, 'PCI DSS: Payment Card Industry Data Security Standards in Context' (2008) 24 *Computer Law and Security Review: International Journal of Technology and Practice* 540, 543.

⁴⁵ For an instance of this matter, see Orlina Simamora, 'Pembobolan Lewat ATM Mandiri [ATM Mandiri Theft]', *Kompas* (Jakarta), 20 November 2006. In this rubric, Ms Simamora reported four unauthorised ATM withdrawals that caused an IDR4 million loss from her account, and made a request for restitution from Bank Mandiri. Later the bank showed her only the decision letter (which cannot be taken home nor a photocopy supplied) that essentially rejected the claim. Upon receiving this decision, Ms Simamora questioned the extent to which the bank was responsible for the security of a consumer's funds held in the bank. Corporate Secretary PT Bank Mandiri (Persero) Tbk then replied to Ms Simamora's letter in the same column in *Kompas* dated 13 December 2006, stating that based on the study by Bank Mandiri, the fourth withdrawal was considered valid because it was done with the card on behalf of Ms Orlina Simamora and via access to the account in question. 'Success' in terms of a transaction involving an ATM means that the ATM has to issue money according to the amount requested and the account in question has been debited accordingly; Hotman Simbolon, 'Transaksi dengan Kartu Mandiri [Transaction with Mandiri Card]', *Kompas* (Jakarta), 13 December 2006. From a technical point of view, unless bank systems have created unique data in each card to distinguish it from a possible counterfeit card, data in a counterfeit card that has been created by the use of data obtained utilising the skimming device method is identical to the genuine card; thus, the ATM/Debit card system will never be able to distinguish the data in counterfeit card from the data in the original ATM/Debit card. See also Mahesa Jati Kusuma, *Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan Informasi dan Transaksi Elektronik (ITE) di Bidang Perbankan [Bank Consumers Protection Law: Legal Measures to Protect Bank Consumers from Information and Electronic Transactions Crime (ITE) in Banking Sector]* (Nusa Media, 2012) 125.

reputation risk) and/or if there is widely publicised encouragement from central bank to do so.⁴⁶

When an unauthorised withdrawal of money from a customer account takes place (and is not widely publicised in the mass media), a legal question reasonably arises as to whether the bank or customer should himself/herself bear the responsibility for the loss incurred from the disputed transaction.⁴⁷ However, failure to meet customer expectations regarding the safety of their accounts can undermine customer confidence and trust. This could hinder the bank's ability to retain existing customers and to offer other e-banking products and services in the future. Significant consumer confidence or trust issues have been created through the common defensive bank position in fraud cases,⁴⁸ as well as prompting some debate about the appropriate level of consumer education in Indonesia.⁴⁹ Many scholars (such as Tyree,⁵⁰ Glaessner, Kellermann and McNevin,⁵¹ Edwards)⁵² and institutions (for example, the American Bankers Association)⁵³ believe that e-banking will not survive without consumer confidence. Before consumers will widely embrace e-banking, they must be convinced of the trustworthiness of this system. Within the banking industry, public confidence is very important and long touted as paramount.⁵⁴ Sound consumer protection regulation to

⁴⁶ See Tri Artining Putri, above n 39. See also REI et al, *Bank Harus Bayar Nasabah* [Bank Has to Pay Consumer] (22 January 2010) *KOMPAS.COM* (online) <<http://bisniskeuangan.kompas.com/read/2010/01/22/07010927/Bank.Harus.Bayar.Nasabah>>.

⁴⁷ Reinhard Steennot, 'Allocation of Liability in Case of Fraudulent Use of an Electronic Payment Instrument: The New Directive on Payment Services in the Internal Market' (2008) 24(6) *Computer Law and Security Report* 555, 555. See also Dana Aditiasari, *Bank Mandiri Akan Ganti Seluruh Dana Nasabah yang Dibobol* [Mandiri Bank to Make Restitution for All Consumer Funds Which had been Robbed] (3 September 2014) *Detik.com* <<http://finance.detik.com/read/2014/06/03/134152/2598382/5/bank-mandiri-akan-ganti-seluruh-dana-nasabah-yang-dibobol?f990101mainnews>>.

⁴⁸ See, *Kompas*, 31 January 2010. In response to recent ATM fraud in Indonesia, *Kompas*, one of the largest newspapers in Indonesia, conducted an ATM survey and found that most respondents (75.5%) worried about the safety of their money in the bank, and that such incidents jeopardised their trust in the bank.

⁴⁹ Russel, above n 35.

⁵⁰ Alan Tyree and Andrea Beatty, *The Law of Payment Systems* (Butterworths, 2000).

⁵¹ Thomas C Glaessner, Tom Kellermann and Valerie McNevin, 'Electronic Safety and Soundness: Securing Finance in a New Age' (The World Bank, 2004) 8.

⁵² Robin Edwards, 'Working Out Loss Liability in the Light of Efficiency Principles' in Wickrema Weerasooria (ed), *Financial Regulation and Payment Systems* (Prospect Media, 2001) 13.

⁵³ American Bankers Association (ABA), *Security in Electronic Banking* (2010) <http://www.aba.com/Issues/Issues_SecurityElectronic.htm>; American Bankers Association (ABA), *Security in Electronic Banking* (2012) <http://www.aba.com/Issues/Index/Pages/Issues_SecurityElectronic.aspx>.

⁵⁴ Anita K Pennathur, "'Clicks and Bricks': e-Risk Management for Banks in the Age of the Internet' (2001) 25 *Banking and Finance* 2103, 2112.

protect bank consumers against unfair contract provisions when dealing with the allocation of liability for unauthorised EFT is then very important.⁵⁵

Although modern technology facilitating e-banking has been popularly used in Indonesia for more than two decades, the laws and policies governing fraud liabilities of parties (loss allocation rules) involving such transactions remain uncertain, unclear and ineffective. These problems occur in many respects, such as in regard to the definitions of 'valid transactions', what conduct is deemed to constitute fault or negligence, what sort of principle can be used in the determination of parties liable for incidents of unauthorised e-banking transactions, the basis for defence to such liabilities, onus of proof, and what is the most appropriate forum for settlement of liability disputes. One can argue that these weaknesses are contributing to the rise of irregularities and criminal activities surrounding EFT in Indonesia, as alluded to earlier.

In general, the allocation of losses in e-banking transactions in Indonesia occurs via a combination of government regulation and private ordering (contract). Very unfortunately, the most recent funds transfer legislation amongst others, namely Law Number 3 of 2011 on Fund Transfer (LFT),⁵⁶ does not regulate the loss allocation rule (civil liability) in the event of e-banking fraud. Law Number 7 of 1992 on Banking as amended by Law Number 10 of 1998 (LB)⁵⁷ is also silent about this issue.⁵⁸

However, some other Indonesian law such as the Civil Code,⁵⁹ Law Number 8 of 1999 on Consumer Protection (LCP)⁶⁰ and Law Number 11 of 2008 on Information and

⁵⁵ In the United States, the importance of consumer protection is established by the enactment of the *Federal Electronic Fund Transfer Act (EFTA)* as a consumer protection statute governing consumer rights and liabilities vis-à-vis financial institutions. In Indonesia, the consumer protection aspect has been established as one of the six important aspects that underpin Indonesian banking architecture. In practice, consumer protection provisions exist in many Bank Indonesia regulations, such as in the card-based payment system regulation whereby banks are obligated to improve their e-banking/EFT security features. Bank Indonesia also provides mediation services in order to assist and overcome disputes between consumers and banks.

⁵⁶ *Undang-Undang Republik Indonesia Nomor 3 Tahun 2011 Tentang Transfer Dana* [Law No 3 of 2011 on Fund Transfer] (Indonesia) ('LFT').

⁵⁷ *Undang-undang Republik Indonesia Nomor 7 Tahun 1992 Tentang Perbankan Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 10 Tahun 1998* [Law No 7 of 1992 on Banking as Amended by Law No 10 of 1998] (Indonesia) ('LB').

⁵⁸ AZ Nasution, *Aspek Hukum Perlindungan Konsumen: Tinjauan Singkat UU Nomor 8 Tahun 1999-L.N. 1999 No 42* [Consumer Protection Legal Aspect: Brief Analysis Law Number 8 of 1999] (2010) Masyarakat Pemantau Peradilan Indonesia 12 <http://www.pemantauperadilan.com/index.php?option=com_content&task=view&id=121&Itemid=12>.

⁵⁹ *Kitab Undang-Undang Hukum Perdata* [Civil Code] (Indonesia). See art 1365: 'A party who commits an illegal act which causes damage to another party shall be obliged to compensate therefore'; art 1366: 'An individual shall be responsible, not only for the damage which he has caused by his act, but also for

Electronic Transactions (LIET),⁶¹ in general have provisions that govern liabilities. Specific to LCP, Samsul,⁶² Azhari,⁶³ and Owen et al,⁶⁴ argue that although generating much hope regarding the protection of bank customers, the LCP still fails to clearly define the rights and liabilities of parties involved in banking activities.

Referring to the complex and compounding issues described above, most of the problems pertaining to the specific liabilities of the parties to such an unauthorised ATM/debit card transaction are, therefore, at the first stage usually governed by, and settled almost exclusively in accordance with, the terms and conditions of the contract that exists between the consumer and the bank.

However, contentious issues between banks and customers are also generally derived from what are termed the banks' 'standard agreements', which in most cases distribute risks associated with consumer e-banking transactions in a manner that seems to strongly favour the banks (exemption clauses) and which consequently may be viewed by consumers as 'unjust'.⁶⁵ According to the standard agreement of a number of banks about payment card transactions, all consumer transactions will be deemed valid if the correct consumer card data and PIN is used, and the bank will not be responsible for unauthorised use of it by an unauthorised party (liability dumping).⁶⁶

that which was caused by his negligence or carelessness'; art 1367: 'An individual shall be responsible for the damage which he has caused by his own act, as well as for that which was caused by the acts of the individuals for whom he is responsible, or caused by matters which are under his supervision.'

⁶⁰ *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen* [Law No 8 of 1999 on Consumer Protection] (Indonesia) ('LCP'). See art 19(1): 'Business actors are obligated to give compensation for the damage, taint and/or losses the consumers suffer as a result of using or consuming the goods and/or services produced or traded by the business actors.'

⁶¹ *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik* [Law No 11 of 2008 on Electronic Information and Transactions] (Indonesia) ('LIET'). See art 21(3): 'If the loss in an Electronic Transaction takes place due to the operation failure of the electronic agent caused by the third party's action directly to the electronic system, all of legal outcome shall become the responsibility of the electronic agent organizer.'

⁶² Inosentius Samsul, 'Pengembangan Model Penyelesaian Sengketa Perbankan Dalam Perspektif Perlindungan Kepentingan Konsumen [Development of Banking Dispute Settlement Model from Consumer Protection Perspective]' (2009) 7(1) (January) *Buletin Hukum Perbankan dan Kebangsentralan* 15.

⁶³ H M Azhari, *Perlindungan Hukum Bagi Nasabah Perbankan Syari'ah [Legal Protection For Sharia Banking Consumer]* (2009) <<http://www.pa-tanahgrogot.net/utama/images/stories/pdf/artikelazhari.pdf>>.

⁶⁴ Darrell E Owen et al, 'Indonesia - Information and Communications Technologies (ICT) Assessment (Technical Report)' (USAID/ECG, 16 January 2001) 24.

⁶⁵ Iwan Setiawan, 'Pembobolan ATM Bank [Theft from Bank ATMs]', *Gatra* (Jakarta - Indonesia), 24 February 2010, 57.

⁶⁶ Try Widiyono, *Aspek Hukum Operasional Transaksi Produk Perbankan di Indonesia* [Legal Aspect of Operational Transaction Banking Products in Indonesia] (Ghalia Indonesia, 2006) 73. It is important to note that the standard form for ATM card usage issued by PT Bank Perkreditan Rakyat Karyajatnika Sadaya (BPR KS) states that liability is attributed to the consumer, such as: 1. Consumer is obligated to

Thus, it is easy to assume that unless there is strong evidence indicating that the unauthorised ATM/debit card transaction was performed by a third party fraudster or cardholder or is associated with family, work colleagues and the like, most of the ‘phantom withdrawals’ will be deemed valid because the transaction used the correct consumer card data and PIN. Banks usually believe consumers to be, at least to some extent responsible for the transaction, accusing them of having disclosed their PIN to someone else, either accidentally or deliberately. Hence, money lost from a consumer account most likely will not be redeemed from the bank.⁶⁷ Fuady contends that the bank’s rejection of a consumer’s claim of unauthorised ATM/debit card transactions is mostly based on the implementation of the ‘non repudiation principle’, where all successful transactions (based on a consumer’s correct data, that is card and PIN data) will be treated as valid transactions, regardless of whether they were authorised or unauthorised transactions.⁶⁸

Even more severe from a consumer protection point of view, there was an occasion when a bank consumer became a victim of card trapping fraud at an ATM, and the bank confirmed the fact after re-playing the CCTV footage which showed that there had been a fraudster tamper with the ATM by using card trapping devices and the display of a sticker with a fake call centre’s phone number. However, the consumer’s claim for redress was eventually rejected by the bank for three reasons: (1) that the bank does not have a legal basis for the restitution (unless there is a court decision); (2) as the government bank, it would be accused of corruption if it redressed the consumer’s loss without a court verdict; and (3) the payment for redress if any, would trigger similar

safeguard the ATM card and keep its PIN secret; 2. Any use of consumer ATM and PIN by an unauthorised party becomes the consumer’s responsibility and [the] bank will not be responsible for unauthorised use of ATM card and PIN by unauthorised party. See also, eg, point number 6 at PT Bank Mandiri (Persero) Tbk ‘Syarat dan Ketentuan Penggunaan Mandiri Debit’ [General Condition and Provision of the Usage of Debit Mandiri]: The cardholder shall maintain the confidentiality of the PIN of the card and take full responsibility for its use, hence the Bank will not in any way responsible for the misuse of the PIN. Point VII.D.7 PT Bank Negara Indonesia (Persero) Tbk, Ketentuan Umum dan Persyaratan Pembukaan Rekening [General Terms and Conditions for Account Opening] (2012): User ID and PIN of electronic channel facilities only known by and become the consumer’s secret. Any abuse of consumer user ID and PIN of electronic channel make consumers fully responsible and risk-bearing, and bank is indemnified from any kind of lawsuit resulting from such abuse; Point 6 of ‘Pernyataan & Persetujuan Anda Sebagai Pemohon [Consumer Statement and Agreement as an Applicant] – PT Bank Permata (Persero) Tbk, *‘Formulir Pembukaan Produk Terpadu [Integrated Product Opening Form]’* (2012): ‘... I [the consumer] will keep PIN secret and will not reveal it to anyone and I herewith declare to be responsible upon any loss associated with card and PIN abuse and indemnify bank from any risk, damage, or liability that may occur due to it.’

⁶⁷ See, eg, Simamora, above n 45.

⁶⁸ Muhamad Djumhana, *Asas-Asas Hukum Perbankan Indonesia* [Principles of the Indonesian Banking Law] (PT Citra Aditya Bakti, 2008) 283.

claims from other victims. The dispute became even worse for the consumer, since the bank indicated that it is only willing to settle the dispute by using the court litigation instead of an alternative dispute resolution body such as the Consumer Dispute Settlement Body (CDSB).⁶⁹

Fraudulent transactions could potentially jeopardise consumer trust and hinder the viability of payment system development. Hence, the existing legal provisions with respect to civil/fraud liability for unauthorised EFT transactions will be critically analysed as a legal alternative for consumers to obtain redress from bank when a consumer's claim regarding unauthorised ATM/debit card transaction/s was rejected by a bank based on the bank's liability dumping provisions in the bank-consumer contract.

It is argued that the question of liability then can be established clearly and more easily if the party responsible for the fraud can be determined as well as the method of attack that has enabled an unauthorised ATM/debit card transaction to be made. However, even if the fraudsters and their attack method could not be revealed, for the sake of certainty, fairness and justice to the victim, the law should determine which party is most likely to have to bear the burden of the loss and the circumstances in which they should do so.

From the point view of Indonesian statutes,⁷⁰ the basic concept of civil liability in Indonesia is that an at fault or negligent party must bear any losses that other parties or themselves incur because of his or her negligence. Sometimes frauds have occurred not only due to a bank's security weaknesses but also because consumers might have contributed or been responsible via their own 'fault/negligence' (that is, demonstrated a degree of negligence), such as by writing their PIN on the ATM/debit card, or using a date of birth as their PIN.

Electronic banking is a special product offered by banks and one that utilises extensive technology. In spite of its nascent development, it is very rare for banks in Indonesia to offer enough education to consumers regarding how to safeguard ATM/debit card transactions from the risk of fraud, that is, about the exhaustive methods adopted by fraudsters and how to avoid them. Indeed, as the author's fieldwork research later

⁶⁹ A Bank DKI legal officer statement made before the Jakarta Consumer Dispute Settlement Body hearing concerning unauthorised ATM withdrawal claimed by Mr Samuel Panggabean, Jakarta, 30 July 2013. See text above footnote n 1040 (below) for detailed case of Mr Samuel Panggabean. For *pros* and *cons* of dispute settlement in the court and CDSB, see their description in Chapter Six of this thesis.

⁷⁰ See Chapter Five / section 5.4.1 of this thesis.

revealed, education by banks generally revolves around the necessity to keep cardholder PIN secret and on the prohibition on writing the PIN on a card/storing a PIN record in a wallet. Based on an interview conducted with the head of a major bank's ATM Division, it can be observed that banks are reluctant to educate consumers regarding transaction risks (such as the various risks associated with ATM/Debit card transactions) in order to avoid a false perceptions among bank consumers that the bank system was not secure. In addition, a private bank consumer services officer interviewee noted that while some of her duties were to facilitate account opening, supply an ATM/debit card and provide consumer education about bank products or services (including their inherent risk) for new customers, she herself used her own birth date as her ATM PIN (in the banking industry, for security reasons most banks forbid consumers using this as a PIN). Though this fact probably cannot be used to create a general picture of the Indonesian banking industry, it nevertheless raises concerns about the seriousness of the bank's attempt to mitigate fraud risk by educating its own employees correctly.⁷¹

From a technical viewpoint, every fraud might have different techniques or *modus operandi*. What constitutes being at fault or negligent for one party in one fraud case might differ from that in another case. A deeper understanding about who committed the fraud, and when, where, and how that fraud was committed, including the specific fraud technique or method employed by the culprit, should enlighten fraud liabilities stakeholders regarding the circumstances of the case.

Along with economic framework for loss allocation and legal principles on civil liabilities, it is argued that the party that should be liable for damage in unauthorised ATM/debit card transactions will be easier to nominate if the point of compromise that enabled the fraudulent transaction to occur can be determined. On the other hand, a failure to understand the technical background in a case involving the extensive deployment of electronic and technical knowledge will lead to decisions that are far less likely to demonstrate fairness, justice and certainty. Thus, information security/technology infrastructure used in a payment card system relating to

⁷¹ This first interviewee cited is Siti Sekarwati, Division Head ATM Operation, PT Bank Mandiri, Tbk (Persero) (Jakarta, 5 August 2012); the second interviewee is a consumer services officer (BO 5).

unauthorised ATM/debit card transactions will be analysed extensively to provide a basis for establishing liability in the event of fraud.⁷²

Referring to the problems of unauthorised ATM/debit card transactions mentioned above, this study attempts to examine the adequacy and effectiveness of the relevant laws of Indonesia in dealing with increasing levels of ATM/debit card fraud. This thesis argues that creating the legal framework for fair and clear loss allocation rules in the case of unauthorised ATM/debit card transactions is very important. Such a framework could become a common guide to settling any disputes between banks and consumers, either in the banking industry itself, or in any Court or alternative dispute resolution (ADR) forum. It could also provide incentives to the liable party to increase their level of ‘duty of care’ both in the administrative and technological sense. It is to be hoped that the uncertainty that has long existed in relation to the results of disputes involving unauthorised EFT transactions will then be reduced.

Nonetheless, to the best of the writer’s knowledge, no in-depth studies have been undertaken thus far on Indonesian law and practice concerning economic, technological, and legal aspects of unauthorised ATM/debit card transactions. The need for a comprehensive investigation of loss allocation rules (civil/fraud liability) for losses derived from unauthorised ATM/debit card transactions in Indonesia has become more important as the proliferation and greater popularity of payment cards systems has unfortunately also been accompanied by increased payment card fraud.

The dearth of studies on what is an increasingly important area of law and regulation demands a comprehensive investigation into the problems in order to arrive at recommendations for the development of the banking sector in regard to strengthening the protection of banking consumers in Indonesia.

Legal reform in the electronic banking area — especially in payment card system — is thus always essential, simply to keep abreast of the changing technology and the challenges such technology presents. It requires a greater understanding and knowledge of the technology involved.⁷³ In addition, it is submitted in the thesis that the apportionment of liability rules in the payment system requires greater attention not

⁷² Carl H Meyer and Stephen M Matyas, *Cryptography: A Guide for the Design and Implementation of Secure Systems* (John Wiley & Sons, 1982) 451.

⁷³ Glaessner, Kellermann and McNevin, above n 51, 25.

only to the legal aspects, but also to a multitude of factors such as economic factors, and human factors (for example, consumer awareness and education) as well as the processes and technology utilised.⁷⁴ Failure to do so tends to render loss allocation rules misleading and inaccurate.

1.2. The Scope and Limitations of the Study

E-banking/EFT has a very wide array of manifestations. However, for the purpose of this thesis the study will be restricted to payment card transactions in Indonesia where the consumer (and also fraudster) is directly involved in initiating the ATM/debit card transaction in the brick-and-mortar world⁷⁵ (card present transaction) for transactions at ATM/EFTPOS terminals. In terms of the technology used in payment cards, this thesis will only focus on ATM/debit cards that are most widely used in Indonesia, where identification, authentication and authorisation of consumer transactions still rely on a magnetic stripe and PIN.⁷⁶

⁷⁴ Relevant processes and technological factors for consideration include the strength or sophistication of electronic systems used for identification, authentication and authorisation of ATM/debit transactions, fraud methods, and the points at which ATM/debit card data is being compromised. The technological aspects of ATM/debit card transactions also will be discussed from a legal perspective, especially in regard to testing the validity of electronic card data and electronic signatures used in e-banking transactions in Indonesia in order to ascertain and legitimise the mandate of customers. In this respect, issues to be taken into account include how the law ensures authentication and authorisation in terms of integrity, confidentiality and non-repudiation for card-based payment transactions.

⁷⁵ A traditional 'street-side' or 'shop front' business that deals with its customers face-to-face in an office or store that the business owns or rents. The local grocery store and the corner bank are examples of brick-and-mortar companies. For more, see Investopedia, *Dictionary: Brick and Mortar* (2012) <<http://www.investopedia.com/terms/b/brickandmortar.asp#ixzz1aJkP6Zm9>>. 'Brick-and-mortar' and 'bricks-and-mortar' are used interchangeably by various writers.

⁷⁶ There are other reasons why this thesis focuses on unauthorised ATM and debit card transactions: In terms of card-based payment transaction data in Indonesia, the Bank Indonesia, *Payment System Annual Report 2010* concluded that in Indonesia ATM and debit card transactions are the most prevalent in the retail payment systems market place as compared to other non cash payment instruments such as credit cards, prepaid cards, Internet banking or SMS banking (at 11). However, the popularity in the use of ATM and debit cards has also attracted criminals, as evidenced by an increase in card-based payment fraud to IDR 11 billion in 2010. By contrast, credit card fraud data decreased both in volume and value by 7.06% and 20.88% respectively in 2010.

From 1 January 2010, all new credit cards issued in Indonesia were equipped with new 'chip' or 'smart card' technology. The new secure and tamper resistant cards resulted in a decrease in credit card fraud figures in 2010 (at 51). In contrast, there are not yet such obligations to implement smart card technology for proprietary ATM and debit cards, even though the draft of national standard for ATM/Debit card based on chip technology was created (at 30). Most ATM and debit cards in Indonesia are proprietary cards (issued by the bank with its own local brand) and still rely on magnetic stripe technology, and are thus more vulnerable to fraudster attack. See: Biro Pengembangan dan Kebijakan Sistem Pembayaran Tim Perizinan dan Informasi Sistem Pembayaran, Direktorat Akunting dan Sistem Pembayaran, 'Laporan Sistem Pembayaran dan Pengedaran Uang 2010. "Arah dan Kebijakan Sistem Pembayaran dalam Menyongsong Era Integrasi Ekonomi serta Upaya Meningkatkan Kualitas Uang dan Keandalan Manajemen Pengelolaan Kas" [Payment System Annual Report 2010. "Payment System Direction and Policy in the Era of Economic Integration and Efforts to Improve the Quality and Reliability of Cash

Hence, this study will focus first on unauthorised ATM/debit card transactions and relevant loss allocation rules (fraud liabilities) between consumers and the ATM/debit card issuer bank.⁷⁷ Therefore, it does not cover:

- Disputes caused by: a) technical malfunction or system errors; b) unauthorised ATM/debit card transactions involving non-consumer transactions; and c) unauthorised ATM/debit card not present (CNP) transactions conducted without the physical use of ATM/debit cards, such as in Internet transactions or mail order/telephone order (MOTO) transactions;
- debit card transactions where the authentication and authorisation method is using a handwritten signature; and
- transactions between merchants and financial institutions.

Secondly, with a view to strengthening the existing provisions concerning prevention and legal mitigation of ATM/debit card related crimes in Indonesia, this study will investigate and examine legal flaws in the existing unauthorised ATM/debit card transaction dispute resolution processes between consumers and their bank in the ADR and/or court of justice based on payment cards and their liability regulation, and propose better rules and procedures to further safeguard consumer transactions and encourage consumer confidence in the system and its use.”

Even though the study is limited to unauthorised ATM/debit Card transactions, to some extent all the principles, findings and recommendations pertaining to fair and just loss allocation rules basically can be applied to other e-banking or EFT transactions, such as credit card, Internet banking, mobile banking, phone banking, and so on.

1.3. The Contribution of the Study

Indonesia introduced electronic banking in the early 1990s.⁷⁸ This new method of transacting has been popular since its inception, resulting in a significant increase in electronic banking transactions in Indonesia. This has been followed by a

Management"]' (Bank Indonesia, 2010) 51–2. This document can be retrieved from <http://www.bi.go.id/NR/rdonlyres/71144447-A46645A0B756D9C0A627B710/22745/LSPPU2010_Final_Publish_Web.pdf>. More recent developments that indicate the delay in implementing such technology in relation to ATM/debit card payments are also detailed in this thesis.

⁷⁷ Unauthorised ATM/debit card transactions in this thesis means: those ATM or debit card transactions not authorised by the legitimate cardholder but limited to bricks-and-mortar card present transactions.

⁷⁸ Dyah Nastiti K Makhijani, 'Payment Systems in Indonesia' in *Payment Systems in EMEAP Economies* (Executives' Meeting of East Asia-Pacific Central Banks and Monetary Authorities (EMEAP) 2002) 148.

commensurate increase in the number of consumer complaints due to a continued rise in the number of unauthorised ATM/debit card incidents. According to the 2010 payment system report from Bank Indonesia, fraud loss in ATM/debit card transactions increased by IDR11 million compared to previous year, that is, from just IDR44.997 million in 2009 to IDR55.224 million in 2010. The biggest fraud losses were from counterfeit card fraud where consumer data was obtained using the card skimming method.⁷⁹

Despite these momentous changes in the banking sector in terms of method of transactions and fraudulent transfers of customer deposits, there has been no comprehensive study carried out thus far addressing the problems referred to earlier.

In view of the dearth of material in this area of study in Indonesia and the fact that there is no clear, simple, fair and decisive set of laws covering unauthorised ATM/debit card transactions in Indonesia, this study intends to make a significant contribution towards the development of comprehensive loss allocation rules and EFT regulation in Indonesia. It will conduct a critical analysis of the economic, technological, and legal framework for this electronic banking service.

The study will be the first of its kind in Indonesia, and will comprehensively:

- Critically review the implementation of the laws addressing civil liability resulting from fraud or unauthorised ATM/debit card transactions in Indonesia (fraud liability) and examine the fraud from legal, economic, and technological points of view in order to make a comprehensive analysis of unauthorised ATM/debit card transactions and the ramifications for Indonesian law.
- Compare and benchmark other countries' unauthorised EFT regulations covering loss allocation (allocation of liability) between consumers and banks, including the *Electronic Funds Transfer Act (EFTA)*⁸⁰ and *Regulation E* in the United States⁸¹ and the e-Payments Code in Australia.⁸² The thesis will analyse liability allocation thoroughly, according to its context, background policy and possible appropriateness within an Indonesia context.

⁷⁹ Biro Pengembangan dan Kebijakan Sistem Pembayaran Tim Perizinan dan Informasi Sistem Pembayaran, Direktorat Akunting dan Sistem Pembayaran, above n 76, 52.

⁸⁰ *Electronic Funds Transfer Act of 1978 (EFTA)*, 15 USC 1693 et seq.

⁸¹ *Regulation E* 12 CFR § 205. For more, see US National Archives and Records Administration, *Electronic Code of Federal Regulations e-CFR*, as at 13 September 2012 <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=635f26c4af3e2fe4327fd25ef4cb5638&tpl=/ecfrbrowse/Title12/12cfr205_main_02.tpl>.

⁸² ASIC, *ePayments Code*.

- Fill the gap resulting from the relative legal vacuum concerning clear and detailed allocation rules for (enumerated) losses resulting from unauthorised ATM/debit card transactions. Therefore, the thesis will propose a comprehensive ATM/debit card regulation addressing the perspectives and interests of both the consumer and the bank, which will provide clear, fair, just, simple, and decisive loss allocation rules concerning unauthorised ATM/debit card transactions, along with relevant considerations and principles that will fit Indonesia's specific situation and its civil liability regime.

1.4. Literature Review

One of the most important outcomes for consumers in the development of electronic commerce (e-commerce) has been the introduction of the electronic means of making banking transactions, better known as electronic-banking or e-banking. Many researchers, scholars, and practitioners, such as Geva,⁸³ Nitsure,⁸⁴ Nsouli,⁸⁵ Tyree,⁸⁶ Gleason and Heimann,⁸⁷ and Schachter,⁸⁸ and international institutions such as the Bank for International Settlement,⁸⁹ the Federal Financial Institutions Examination Council, and the International Monetary Fund agree on the significant benefits of e-banking service delivery.

The Basel Committee on Banking Supervision – Bank for International Settlements in their study noted that the development of e-banking may contribute to improved efficiencies in the banking and payment system, which could give banks greater capabilities to offer a newer and wider range of products and services with lower operating costs, expand their market for traditional deposit-taking and credit extension activities, and strengthen their competitive position in offering existing payment services.⁹⁰ Schachter⁹¹ further noted that e-banking enables new and existing

⁸³ Benjamin Geva, *The Law of Electronic Funds Transfer* (LexisNexis, Release No 9 ed, 2001) 1–33.

⁸⁴ Rupa Rege Nitsure, *E-Banking: Challenges and Opportunities* (ICFAI University Press, 2006) 1.

⁸⁵ Nsouli and Schachter, above n 10, 3.

⁸⁶ Alan L Tyree, *E-Commerce and Retail Banking* (2000) <<http://www2.austlii.edu.au/~alan/bla-2000.html>> 1.

⁸⁷ Kristeen Gleason and Dan Heimann, *Electronic Banking, Doing Business Electronically* (Springer-Verlag, 1998) 177–80.

⁸⁸ Nsouli and Schachter, above n 10, 1.

⁸⁹ Bank for International Settlements (BIS) has conducted many studies in regard to e-banking and banking payment instruments, such as *Risk Management for Electronic Banking and Electronic Money Activities* (March 1998) and *Risk Management Principles for Electronic Banking* (July 2003).

⁹⁰ BCBS, *Risk Management for Electronic Banking and Electronic Money Activities*, above n 3, 1.

customers to no longer be subject to time and geographic limits, with a form of banking that was relatively convenient, easy and involved low transaction costs.⁹² In relation to the banking processing capabilities, Storer furthermore explained how e-banking could convey large quantities of data over great distances, quickly and securely.⁹³

In contrast, a study conducted by the Basel Committee on Banking Supervision⁹⁴ as well as those by Akindemowo,⁹⁵ Pennathur,⁹⁶ and Nsouli and Schaechter,⁹⁷ found that besides a standard risk for traditional banking activities, particular risks are pertinent across e-banking activities or an electronic payment system, namely operational risk,⁹⁸ reputational risk⁹⁹ and legal risk.¹⁰⁰

Many scholars (such as Gifford,¹⁰¹ Davidson,¹⁰² and Phair)¹⁰³ have noticed that technology creates the possibility for e-banking crimes of great magnitude and complexity to be committed quickly and anonymously. Such crimes include unauthorised system access, employee fraud (both bank employee and merchant), and card payment fraud. Techniques used to obtain the information necessary to perform unauthorised e-banking consumer transactions include the insertion of key logging applications, 'shoulder surfing', illegal interception of transaction data, 'packet sniffing', and 'social engineering' (described in Chapter 4).

In most cases, it is not possible to identify the person who has committed the fraud. Unauthorised e-banking transactions can lead to the consumer and/or bank incurring

⁹¹ Andrea Schaechter, 'Issues in Electronic Banking: An Overview - IMF Policy Discussion Paper' (International Monetary Fund, 2002) 2.

⁹² See also, Tyree, *E-Commerce and Retail Banking*, above n 86, 1.

⁹³ Charles Storer, 'Global Cash Management and Security' in Brian Welch (ed), *Electronic Banking and Treasury Security* (Woodhead Publishing, 1999) 36.

⁹⁴ BCBS, *Risk Management for Electronic Banking and Electronic Money Activities*, above n 3, 5–9.

⁹⁵ Olujoke Akindemowo, 'Electronic Payment Systems and Cyberbanking' in Jay Forder and Patrick Quirk (eds), *Electronic Commerce and the Law* (John Wiley & Sons, 2001) 126–7.

⁹⁶ Pennathur, above n 54, 2111–13.

⁹⁷ Nsouli and Schaechter, above n 10, 3–5.

⁹⁸ Operational risk arises from the potential for loss — due to significant deficiencies in system reliability or integrity — that can derived from external or internal attacks on their system or product, including from customer misuse.

⁹⁹ 'Reputational risk' is the risk of significant negative effect on public opinion of the institution that results in a critical loss of funding or customers. Reputational risk may arise from (among other things) a significant breach of security, whether as a result of external or internal attacks on a bank's system, including mistakes, malfeasance, and fraud by third parties.

¹⁰⁰ Legal risk arises from violations of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established.

¹⁰¹ Gifford, above n 17, 29–37.

¹⁰² Davidson, above n 18, 292–5.

¹⁰³ Phair, above n 19, 15–40.

direct financial losses. When an unauthorised withdrawal of money from a customer account takes place, a question reasonably arises as to whether the bank or customer himself/herself should bear the responsibility for the loss incurred from the disputed transaction.¹⁰⁴

It is submitted that the central issue of this thesis, and an issue that has been a concern of many scholars (such as Cooter and Rubin,¹⁰⁵ Rusch,¹⁰⁶ Geva,¹⁰⁷ Pennathur,¹⁰⁸ Radhakrishna,¹⁰⁹ Steennot,¹¹⁰ White,¹¹¹ Franz and Asbill,¹¹² Edwards,¹¹³ and Levitin)¹¹⁴ and for institutions (such as the Federal Financial Institutions Examination Council (FFIEC))¹¹⁵ is how to allocate liability between banks and their consumers for unauthorised EFT transactions.

The importance of loss allocation rules has been long recognised by many scholars, because such rules distribute consequences to and create incentives for the parties involved in the transactions. Moreover, as Levitin observes, there is a relationship between liability and preventive behaviours: 'The greater a party's liability for fraud losses, the greater incentive the party will have to take care to avoid fraud.'¹¹⁶

The more difficult legal issue to be resolved in terms of liability is when there is no clear evidence concerning who actually accessed the e-banking system and transferred funds from the consumer account or when both the consumer and the bank have by their own contributory negligence or fault enabled the fraud to occur. To complicate matters

¹⁰⁴ Steennot, above n 47, 555.

¹⁰⁵ Robert D Cooter and Edward L Rubin, 'A Theory of Loss Allocation for Consumer Payments' (1987) 66 *Texas Law Review* 63, 63.

¹⁰⁶ Linda J Rusch, 'Reimagining Payment Systems: Allocation of Risk for Unauthorized Payment Inception' (2009) 83(2) *Chicago-Kent Law Review* 561, 561.

¹⁰⁷ Benjamin Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers' (2003) 38 *Canadian Business Law Journal* 207, 208.

¹⁰⁸ Pennathur, above n 54, 2103, 2115.

¹⁰⁹ Gita Radhakrishna, 'Liability Issues in Internet Banking in Malaysia' (2009) 7 *IUP Journal of Bank Management* 47, 51–2. For text, see IBMA Publishing <<http://www.ibmapublishing.com/journals/CIBIMA/volume7/v7n1.pdf>>.

¹¹⁰ Steennot, above n 47, 555–7.

¹¹¹ Paul White, *The Regulation of Electronic Funds Transfer in Australia: An Integrated Multidisciplinary Approach* (DBA Thesis, Victoria University, 2007) 3–4.

¹¹² Charles R Franz and Sharon A Asbill, 'Liability Implications in Electronic Fund Transfers' (1982) 5 *Information & Management* 87, 91–2.

¹¹³ Edwards, above n 52, 179–200.

¹¹⁴ Adam J Levitin, 'Private Disordering: Payment Card Fraud Liability Rules' (2011) 5 *Brooklyn Journal of Corporate, Financial and Commercial Law* 1, 1.

¹¹⁵ Federal Financial Institutions Examination Council (FFIEC), 'E-Banking' (2003) 3.

¹¹⁶ Levitin, above n 114, 1, 3.

further, concerning problems of identity and authentication, the studies of Sharpe,¹¹⁷ Edwards,¹¹⁸ Niven,¹¹⁹ and Zahir¹²⁰ reveal the difficulties in identifying who actually performed unauthorised EFT transactions. Generally, banks maintain that most transactions are indeed ‘authorised’ since they are made using correct consumer PIN and card data. Banks and cardholders are often involved in contentious disputes concerning who should be liable for loss of funds suffered by cardholders/consumers.

Currently, many countries have different approaches both to the form of regulation and liability principle adopted to resolve this liability issue. The differences can be attributed to each country’s consumer policy, formal or informal regulatory approach, level of consumer awareness, existence of pressure groups, stage of technological development, and/or fraud incident rates.

In regard to the degree of variation between jurisdictions, a few details prior to presenting further relevant review materials could prove helpful. The United States chose to govern liability rules by statute, with the adoption of a strict liability principle that apportions liability to the financial institution (with just a single limitation imposed regarding consumer reporting). Levitin maintains that such regulation uses strict regulation combined with contributory negligence, with a responsibility on the banking consumer to report unauthorised EFT transactions as soon as they come to the consumer’s attention; nevertheless, the term ‘negligence’ here relates only to the *reporting* of the unauthorised transactions and not to the conduct or situation that caused the loss.¹²¹ In stark contrast to banking entities in Indonesia, banks in the United States bear the risk of unauthorised EFT transactions, regardless of consumer negligence, with — as Douglass notes — consumers only liable for (limited) losses should they fail to

¹¹⁷ Anna Sharpe, ‘The Legal Framework in Relation to EFT Contracts and Disputes, Including Onus of Proof, Bankers’ Duty of Care and Evidentiary Problems, and the Adequacy/Effectiveness of the Law in Resolving EFT Disputes’ (Paper presented at the Electronic Funds Transfer: Trade Practices Commission Workshop, Melbourne, 1989) 59.

¹¹⁸ Edwards, above n 52, 13.

¹¹⁹ David Niven, ‘Comments on Institutions’ Dispute Resolution Procedures and the Ombudsman Proposal’ (Paper presented at the Electronic Funds Transfer: Trade Practices Commission Workshop, Melbourne, 1989).

¹²⁰ Ansy Lema, *Perlindungan Terhadap Nasabah Bank Masih Lemah* [Banks Consumer Protection Still Weak] (15 February 2010) *Perspektif Baru* <<http://www.perspektifbaru.com/wawancara/725>>.

¹²¹ See Levitin, above n 114, 39.

immediately report such transactions.¹²² Conversely, Australia regulates liability with liability rules based on negligence principles (a fault-based system).

In their ePayments code (previously known as Electronic Funds Transfer Code of Conduct 2008), the liability rules are enumerated, prescribed and precise; and in these jurisdictions, a bank is basically responsible for unauthorised EFT transactions, unless it can prove on the balance of probability that consumers have contributed to the losses. Clearly, the Australian and the United States of America (US) systems place a greater degree of responsibility on the banking sector.

Nonetheless, regardless of which international variant of form and liability principle is adopted, it is important to understand the philosophy about liability rules before determining the particular approach to be adopted.

More than two decades ago, Cooter and Rubin in their well-known work used economic analysis to develop three general principles of loss allocation between consumers and financial institutions: loss spreading,¹²³ loss reduction,¹²⁴ and loss imposition.¹²⁵ They concluded that when unauthorised transactions occur, the financial institutions should bear most of the loss because they are in the better position (compared to the consumer) to spread the losses or prevent the fraud. Meanwhile, the consumer should only be strictly liable for the loss up to a relatively low and fixed limit.¹²⁶ Geva echoes this finding.¹²⁷

Many other scholars or experts, such as Rusch,¹²⁸ White,¹²⁹ and Gillette,¹³⁰ extend the findings of Cooter and Rubin in exercising existing liabilities rules. Rusch extends

¹²² Duncan B Douglass, 'An Examination of the Fraud Liability Shift in Consumer Card-Based Payment Systems' (2009) 33 *Economic Perspectives* 43, 45.

¹²³ The 'loss spreading principle' is to 'assign liability for a loss to the party that can achieve risk neutrality at the lowest cost. In general, the party that can achieve risk neutrality at the lowest cost is the one that has greater economic resources and is in a position to spread the loss most effectively': Cooter and Rubin, above n 105, 70–3.

¹²⁴ The 'loss reduction principle' is much more complex than the loss spreading principle, because it relates to human behaviour that can change over time according to specific circumstances. In essence, this principle will place fraud liability on the party in the best position to protect against the unauthorised EFT transactions.

¹²⁵ The 'loss imposition principle', unlike the two previous liabilities principle, is only concerned about the enforcement of these assigned liabilities that it should be efficient (inexpensive as possible). Cooter and Robin, above n 105, 73–7.

¹²⁶ Ibid 109–10.

¹²⁷ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 211.

¹²⁸ Rusch, above n 106, 561, 593, 597, 599.

¹²⁹ White, above n 111, 15.

Cooter and Rubin's work by considering a policy perspective as a determinant factor in creating new rules that should be feasible to be implemented with the current state of technology. According to her, this policy should balance the cost of operating the current system against the cost and feasibility of implementing clear, transparent and functional liability rules in order to create incentives to the appropriate party to reduce the loss.¹³¹

White, in his thesis, found that US regulations are examples of regulations that apply Cooter and Rubin's third principle (loss imposition), while Australia's regulations are examples that apply a mixture of Cooter and Rubin's first and second principles (producing a 'hybrid' of the 'spreading loss' and 'loss reduction' principles).¹³² Further, he asserted that the Australian EFT Code of Conduct,¹³³ which follows a fault-based system, is ambiguous and does not clearly assign definitive apportionment of liability, burden of proof, or outline how to weigh the evidence, and leaves the Australian Banking Industry Ombudsman (ABIO) in the difficult situation of having to make judgments on unclear facts.¹³⁴ In contrast, he compares this to the US regulation that seems to be simpler because it always apportions liability to the financial institution unless the consumer does not report the loss in the acceptable timeframe, or if the transaction is due to theft or misuse of an access device. Therefore, the US approach is easier to adjudicate and administer and could avoid contentious disputes between the financial institution and consumer. However, most of these studies were based on an economic and legal perspective with only little consideration of the technology inherent in ATM/debit card systems.

As can be seen above, issues that exercise authors include fault/negligence and its effects (if any) on loss allocation, and its attribution whether to one party or the other or jointly (according to the various circumstances and legislation, regulation, voluntary code or contract). The knowledge base differential is one source of justification for change as is the banking sector's resistance to implementing safer, more modern

¹³⁰ Clayton P Gillette, 'Rules, Standards, and Precautions in Payment Systems' (1996) 82 *Virginia Law Review* 181, 184.

¹³¹ Rusch, above n 106, 561, 605.

¹³² White, above n 111, 123–4.

¹³³ Now, this EFT Code of Conduct has been transformed into the ePayments Code.

¹³⁴ White, above n 111, 4, 187. Later, this EFT Code of Conduct was replaced by the ePayments Code on 20 September 2011.

technology, as well as consumer education programs. The lack of such changes leaves consumers vulnerable, but without redress.

This knowledge asymmetry was later confirmed by the author in his field research. Prominent fraud methods for ATM/EFTPOS, such as skimming, card trapping, and so on have long been known to banks. They commonly are members of an EFT security association, a network scheme like Visa and/or MasterCard, and have regular gatherings with other banks and/or the central bank. Such memberships and/or routine meetings can be sources of information as to current fraud methods in EFT/card-based transactions. One bank respondent reporting document to the central bank regarding its payment card service (unpublished) revealed that risks in payment cards include skimming, lost and stolen cards, and so on (hence these are foreseeable risks). In contrast, most consumers from major banks that have been interviewed during the author's field research in Jakarta, Yogyakarta and Denpasar (Indonesia) do not have any idea about the function and vulnerability of the magnetic stripe in their ATM/Debit card nor the fraud risks or methods that are commonly employed by fraudsters in Indonesia, such as skimming, shoulder surfing, card trapping and so on (and so for consumers the risks are unforeseeable).¹³⁵

Given the lack of consumer knowledge and the failure by banks to provide safer systems, the numerous instances of unauthorised ATM/debit card transactions (as fraudsters take advantage of both) cannot come as a surprise, nor can the resulting disputes that are further complicated by unclear fault or negligence terminology within the legislation. Geva nevertheless argues that 'any such rule may lead to wasteful litigation and may be unfair to a consumer who may have underestimated the risk'.¹³⁶

This point of view is reflected in many unauthorised ATM/debit card transaction dispute cases in Indonesia. There are no rules linking liability to enumerated prescribed and precise acts or omissions constituting negligence in regard to EFT transactions. This unfortunate situation is further exacerbated by the judges' lack of knowledge of consumer dispute cases, current development of tort law (especially regarding the law of negligence), and the technology, ATM/debit card security standards required by authority (Bank Indonesia), and identity theft/fraud methods involved.

¹³⁵ Interviewee results: BO-1; BO-2; BO-3; BO-4; BO-5, 12; and BO 6; Consumers (C-1–C-12).

¹³⁶ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 207, 240.

Court decisions tend, therefore, to be varied and inconsistent, even where cases are relatively similar. Most court decisions concerning unauthorised ATM/debit card transaction disputes between banks and consumers tend to be always in favour of banks, even though it could be proved that consumers were the victims of fraud. The fact that the bank failed to secure its consumer activated terminal/electronic agent that enable the occurrence of fraudulent activities, was denied.¹³⁷

Along with the practice of unauthorised EFT transactions, the forums to settle disputes arising from such transactions have also become a big problem in their own right in Indonesia. This is mainly because court proceedings in Indonesia are very costly and time consuming, as mentioned by Sukarmi,¹³⁸ Irawan,¹³⁹ and Samsul.¹⁴⁰ In terms of time-frames for court proceedings, Carl and Reni have noted that in practice a trial judgment in the District Court (court of first instance) is usually rendered within one year, while appeals to the High Court may take around two or three years, and the Supreme Court appeals may take between three to five years.¹⁴¹ Hence, total litigation processes in these three different stages of court proceedings will take approximately six to eight years to complete.

¹³⁷ See *PT Bank Mandiri (Persero) Tbk v Muhajidin Taher, SE and PT Advantage CSM* [Supreme Court of Indonesia], 769 K/Pdt.Sus/2011, 27 February 2012. The verdict can be downloaded from Indonesia's Supreme Court Website: <<http://putusan.mahkamahagung.go.id/putusan/163751e4607c4f911d53c3f6e0938714/>> . This verdict is in contrast with that in *Tuan Bahari v PT Bank Negara Indonesia (Persero) Tbk* [Supreme Court of Republic of Indonesia], 718 K/Pdt.Sus/2008, 10 December 2008. See Supreme Court's website: <<http://putusan.mahkamahagung.go.id/putusan/1fad1638a58bd4f455125056361001a8/>>. There is an argument that the court is not the most appropriate venue to resolve consumer disputes when compared to a mediator in a specific consumer body, since a judge only has legal education, while a mediator generally is chosen on his or her professional background with better knowledge and credibility in the consumer dispute area. See MVT/Yoz, *BPSK Enggan Putusannya Diuji Pengadilan* [BPSK Reluctant its Decision Being Review by Court] (26 April 2011) <<http://hukumonline.com/berita/baca/lt4db6805fb81c8/bpsk-enggan-putusannya-diuji-pengadilan>>. See more cases concerning unauthorised ATM/debit card transaction at Chapter Six.

¹³⁸ Sukarmi, *Cyberlaw, Kontrak Elektronik Dalam Bayang-Bayang Pelaku Usaha* [Electronic Contract Within Business Business actorship] (Pustaka Sutra, 2008) 56.

¹³⁹ Candra Irawan, *Aspek Hukum dan Mekanisme Penyelesaian Sengketa di Luar Pengadilan (Alternative Dispute Resolution) di Indonesia* [Legal Aspect and Alternative Dispute Resolution Mechanism in Indonesia] (CV Mandar Maju, 2010) 5–6.

¹⁴⁰ Samsul, 'Pengembangan Model Penyelesaian Sengketa', above n 62, 16.

¹⁴¹ Michael Carl and Dewi Savitri Reni, *A Guide to Dispute Resolution in Indonesia: Litigation Process* (30 September 2011) SSEK Indonesian Legal Consultant <<http://blog.ssek.com/index.php/2011/09/a-guide-to-indonesian-dispute-resolution-litigation-process/>>. In fact, the judicial justice system in Indonesia has a maxim whereby the judicial proceeding in the court should be 'simple, fast, and cheap'.

Adding to this constraint, Priliasari and Winarta observes that judicial decisions often do not reflect a unified approach to the resolution of disputes.¹⁴² The findings of different courts may differ on the same issues, creating uncertainty concerning the expected outcomes of the legal proceedings.¹⁴³

This uncertainty occurred partly because of the lack of status of the principle of precedent in the Indonesian court (relative to its use in common law countries). In Indonesia, there are several types of courts over which the Supreme Court (*Mahkamah Agung*) ultimately presides.¹⁴⁴ As a Dutch colony, its legal system was formed as a civil law system.¹⁴⁵ After independence, Indonesia continued to follow the civil law tradition of the Dutch;¹⁴⁶ thus, 'Indonesian courts do not apply the principle of precedent,¹⁴⁷ which is so familiar among common law jurisdictions'.¹⁴⁸ As Manan observes, 'In a civil law system, the courts are not bound by decisions of the courts at the same level or higher level (District Court or High Court).' Therefore, the court's verdict is a very common cause of legal uncertainty,¹⁴⁹ a point also emphasised by Pompe in his book.¹⁵⁰

¹⁴² For example, between the District Court, High Court and Supreme Court.

¹⁴³ See Yahya Harapan, 'Perlawanan Terhadap Eksekusi Grose Akta Serta Putusan Pengadilan dan Arbitrase dan Standar Hukum Eksekusi [Appeal toward "Grose Akta" Execution along with Court Verdict and Arbitration and Execution Legal Standard]' in Erna Priliasari, '*Mediasi Perbankan Sebagai Wujud Perlindungan Terhadap Nasabah Bank* [Banking Mediation as Promulgation of Banking Customer Protection]' (2008) 5(2) (Juni) *Jurnal Legislasi Indonesia* 42, 48; Frans H Winarta, 'Legal Consistency in Indonesia: What Justice is All About' in Thang D Nguyen (ed), *The Indonesian Dream: Unity, Diversity and Democracy in Times of Distrust* (Marshall Cavendish, 2004) 136. See also Kusuma, above n 45, 125.

¹⁴⁴ Indonesia's judicial institutions are general courts, religious courts, military courts, state administrative courts, the constitutional court, and the commercial court (among others). See further Benny S Tabalujan, *The Indonesian Legal System: An Overview* (2 December 2002) LLRX.Com <<http://www.llrx.com/features/indonesia.htm>>. See also Baker & McKenzie, *Dispute Resolution Around the World: Indonesia* (2010) Baker & McKenzie <http://www.bakermckenzie.com/files/Uploads/Documents/Global%20Dispute%20Resolution/Dispute%20Resolution%20Around%20the%20World/dratw_indonesia_2009.pdf>.

¹⁴⁵ Peter Mahmud Marzuki, *An Introduction to Indonesian Law* (Setara Press, 2011) 65.

¹⁴⁶ Sebastiaan Pompe, *The Indonesian Supreme Court: A Study of Institutional Collapse* (Cornell Southeast Asia Program, 2005) 429.

¹⁴⁷ 'Precedent', in Common Law systems, is the principle that previous cases with similar facts on an identical point of law will bind courts of equal or lower status. In Civil Law systems, courts are not bound by decisions of courts at the same level or higher. This means that there is little need for law reporting in Indonesia and certainly not for published authoritative sets of judgments. Some limited collections of judgments are published (for example, *Yurisprudensi* (jurisprudence)) but they are ad hoc in nature. In fact, statements as to preferred interpretation or policy issued by the Supreme Court in the form of *surat edaran* (circular letters), rather like practice notes in the Common Law System, tend to be more influential than previous decisions, even of the Supreme Court. See Marzuki, '*An Introduction to Indonesia Law*', above n 145; See also Tim Lindsey, *Indonesia Trial Process and Legal System: Background Notes* (2009) Melbourne Law School - Asian Law Centre <http://alc.law.unimelb.edu.au/files/indo_trial_process.pdf>.

¹⁴⁸ Tabalujan, above n 144. See also Zaky Tandjung, Maurice Burke and Herbert Smith, 'Effective Dispute Resolution in Indonesia' (2006) July/August *AsiaLaw* 53.

¹⁴⁹ Bagir Manan, *Menegakkan Hukum Suatu Pencarian* [Raising the Law: A Search] (Asosiasi Advokat Indonesia, 2009) 166.

Nevertheless, there was encouragement for change expressed at the first National Law Seminar in 1963, which recommended that the judges in Indonesia develop national law based on case law.¹⁵¹

According to Mertokusumo, in the Continental law (or Civil Code) system, a court's verdict has what is called 'persuasive precedent', where the court's verdict only has the power to convince, and lacks binding force.¹⁵² Instead, the courts 'will use the statutes as their basis for deciding the cases'.¹⁵³ As a consequence, many relatively similar cases have produced different verdicts. Although this is legally possible since each judge or panel of judges has the independence to decide their own verdicts, the absence of the doctrine of precedent and the lack of adequate publication of and publicity for judicial decisions prevents a court becoming aware of, and learning from, the decisions of another. Hence, this often creates legal uncertainty.

Lemek concluded that the blame for legal uncertainty in Indonesia can be attributed to Indonesia's legal doctrine which gives court judges freedom to examine each case very individually (without utilising a system of 'precedents') and to interpret law. Furthermore, he hypothesised that given the freedom to judge, some were sometimes biased because their judgment may have been influenced by personal feelings and certain 'X' factors.¹⁵⁴ Nurdin further indicates that many court decisions were not independent but driven by corruption, collusion, nepotism, and/or having been subject to interference from the executive or legislative arms of government.¹⁵⁵

¹⁵⁰ Pompe, above n 146, 432.

¹⁵¹ Marzuki, 'An Introduction to Indonesian Law', above n 145, 65.

¹⁵² Sudikno Mertokusumo, *Mengenal Hukum: Suatu Pengantar* [Knowing the Law: An Introduction] (Universitas Atma Jaya Yogyakarta, 2010) 145–50. See also Sudikno Mertokusumo, *Hukum Acara Perdata Indonesia* [Indonesia's Proceeding Law] (Liberty Yogyakarta, 2006) 16.

¹⁵³ Baker & McKenzie, *Dispute Resolution around the World*, above n 144.

¹⁵⁴ Jeremias Lemek, *Mencari Keadilan: Pandangan Kritis Terhadap Penegakan Hukum di Indonesia* [Searching for Justice: Critical View toward Law Enforcement in Indonesia] (Galang Press, 2007) 163–5. In Indonesia, what constitutes 'X' factors vary but mostly they are associated with something that encourages judges to make a decision in favour one party not on the basis of justice or law, but because of such things as tribute, bribery, close friends or family, etc.

¹⁵⁵ Boy Nurdin, *Kedudukan dan Fungsi Hakim Dalam Penegakan Hukum di Indonesia* [The Position and Function of Judges in Law Enforcement in Indonesia] (PT Alumni, 2012) 237. See also Peter Mahmud Marzuki, *Pengantar Ilmu Hukum* [An Introduction to Law] (Kencana, 2008) 124; Irawan, above n 139, 7; Winarta, above n 143, 129–30; Satjipto Rahardjo, *Sisi-sisi Lain dari Hukum di Indonesia* [The Other Sides of Law in Indonesia] (Kompas, 2003) 240–1; Nur Khafifah, *Banyak Suap, Kinerja Lembaga Peradilan Masih Mengecewakan* [Many Bribes, the Performance of the Judiciary is Still Disappointing] (2013) detik.com <<http://news.detik.com/read/2013/04/09/130408/2215371/10/banyak-suap-kinerja-lembaga-peradilan-masih-mengecewakan?9911012>>; 'Penegakan Hukum: Separuh Lebih Responden Tak Puas [Law Enforcement: More than Half of Respondents are not Satisfied]', *Kompas* 8 April 2013, 2. In

As a result of the legal hurdles mentioned above, most bank consumers are not keen to go to court to contest a bank's unfavourable decision, especially if the disputed amount of money that was lost through the fraudster's activities was not significant. There is no guide to what amount is to be considered as 'significant' or 'insignificant'; however, in interviews conducted by the author many bank consumer respondents seem to consider an amount in excess of IDR10 billion as sufficient to drive consumers to seek justice beyond just writing a complaint to the mass media.¹⁵⁶

In order to undertake legal and regulatory reforms, Owen et al argue that Indonesia should take advantage of the best practices and experiences of other countries with respect to the complicated issues surrounding the law and policy of e-commerce.¹⁵⁷ Adding to the complexity, rules regarding liability of the legitimate cardholder for an unauthorised use of the card differ from country to country, as Rosenberg observes.¹⁵⁸ This is a disadvantage but also an opportunity.

Contemporary developments of substantive law in Indonesia tend to follow the world trend towards harmonisation on global issues. Many other countries' regulations (regardless of the origin of the country's law system) and international conventions (such as the EU convention on cybercrime or UNCITRAL model law on e-commerce and electronic 'signatures') have already been adopted in many of Indonesia's regulations.

Lemek argues that it is all right for Indonesia, a country that follows a civil law system, to learn from the experience of Anglo Saxon countries since the demarcation line between Anglo Saxon and civil law countries is now 'a blur' and codes adopted in common law countries can be transposed into civil law countries.¹⁵⁹ Irianto further

the Kompas article, Dewi Arum from *Lingkaran Survey Indonesia (LSI)* stated that 56% of 1200 respondents claimed they were unsatisfied over law enforcement in Indonesia. This figure was mostly caused by the respondents' distrust over law enforcer's capability to resolve or adjudicate problems in a fair manner. Meanwhile, in a detik.com article, Khafifah quoted the survey conducted by the Indonesia Legal Roundtable, the results of which were apparently quite similar to those of the LSI survey results, and which had revealed that 60% of a total of 1220 respondents had noted that Indonesia's judicial system was still affected by bribery. Further, the survey revealed parties that interfere with a judge's impartiality were businessmen (32%), political parties (30%) and government/executives (24%).

¹⁵⁶ Interviewee C1-24.

¹⁵⁷ Owen et al, above n 64, 16.

¹⁵⁸ Arnold S Rosenberg, 'Better Than Cash? Global Proliferation of Debit and Prepaid Cards and Consumer Protection Policy' (Working Paper No 766, Bepress Legal Series, 2005) 47.

¹⁵⁹ Lemek, above n 154, 166.

argues that even in the Netherlands from which Indonesian law was derived, judicial decisions now are deemed a very important source of law, which proves that there is closer intersection between the common law system and the continental law system than some maintain.¹⁶⁰ Hence, relevant legislation and regulations for consideration include *EFTA* and *Regulation E* (US), and the ePayments Code (Australia).

Whilst one can argue that weaknesses in legislation and policy¹⁶¹ as well as technological lag in the area are contributing to the rise of EFT-related irregularities and criminal activities in Indonesia, nonetheless, to the best of the writer's knowledge, no in-depth studies have been yet undertaken on Indonesian law and practice concerning EFT, in particular related to unauthorised ATM/debit card transaction; and it was without success that the writer searched for such materials to include in the literature review. This reinforced the writer's conviction of the need for this study.

Hence, a comprehensive investigation of the problems needs to be conducted in order to gain a true picture of the situation in Indonesia. Investigation results will be analysed comprehensively to enable appropriate law reform recommendations to be made, in order to strengthen consumer protection in banking industry practice in Indonesia.

1.5. Research Questions

To attempt the analysis of the problems briefly introduced in the previous sections of this chapter, the central questions to be addressed by this research project are:

Primary Questions:

1. What sort of legal principles can be used and how to formulate fair, clear and decisive loss allocation rules between banks and their customers for unauthorised ATM/debit card transactions, especially when:
 - a. there is no clear evidence in regard to who has actually performed unauthorised ATM/debit card transactions and whether there is a fault or negligence on the banks' or consumers' side; and

¹⁶⁰ Sulistyowati Irianto, '*Hukum dan Hakim* [Law and Judge]', *Kompas* 16 October 2013, 7.

¹⁶¹ That is, the laws and policies governing the liabilities of parties to such transactions remain unclear and ineffective in many respects, such as in relation to the definitions of valid transactions, what conduct is deemed to constitute fault or negligence, what is the nature of principles that can be used in the determination of parties liability for incidents of unauthorised EFT, the basis for defence to such liabilities, onus of proof, and what is the most appropriate forum for settlement of liability disputes.

- b. both banks and customers had demonstrated negligence that enabled the fraudster to perform unauthorised ATM/debit card transactions.

In order to ascertain the apportionment of fraud liability, a number of issues need to be resolved: what are the methods employed by fraudsters to commit e-banking fraud in Indonesia and where were the point of compromised?

Secondary Questions:

When an unauthorised ATM/debit card transaction occurs, and a process of dispute resolution is required in order to settle contentious disputes between consumer and banks regarding the fraud liability, then:

1. What system of burden of proof should be adopted and who should bear the burden of proof in establishing an allegation of unauthorised ATM/debit transaction between a cardholder and bank? And
2. What sort of approach is required in order to create legal reform for unauthorised ATM/debit card transactions?

1.6. Research Design

1.6.1. Methodology

This research emanates from the observation of the frustrating experiences of numerous helpless victims of e-banking frauds or unauthorised ATM/debit transactions in Indonesia. The victims accrue substantial and/or damaging losses (a small loss can disproportionately affect a person of little means) before becoming aware of the situation and their apparent lack of access to redress. Having been concerned about such a serious problem, several commentators have contended that it is necessary to engage in research to devise appropriate legal principles to redress the loss sustained by such innocent victims.¹⁶²

This research aims to enhance the effectiveness of regulation pertaining to unauthorised ATM/debit card transactions in Indonesia, by establishing clear, detailed and just loss allocation rules for unauthorised ATM/debit card transactions (civil liability), whereby on the one hand, incentives will be provided to banks and consumers to increase their awareness and duty of care to ATM/debit card system, and on the other hand, the

¹⁶² Judith Bell, *Doing Your Research Project: A Guide for First-Time Researchers in Education and Social Science* (McGraw-Hill, 1999) 21.

number of unresolved disputes between customers and their banks regarding unauthorised ATM/debit card transactions will be reduced and/or existing disputes more equitably and predictably resolved.

In order to answer the research questions and address the problems stated above, a theoretical legal research framework¹⁶³ will be developed in regard to civil liability associated with unauthorised ATM/debit card transactions. The relevant legal doctrines will be identified and analysed. In order to achieve the aims of this study (as outlined above), a qualitative research study will be carried out relying upon the personal extensive practical experience of the present author gathered by working with the central bank of Indonesia (Bank Indonesia) and both primary and secondary archival resources available in hard copy and/or electronic forms. Quoting from Denzin and Lincoln, Creswell noted that qualitative research could be defined in the following terms:

Multi methods in focus, involve an interpretive, naturalistic approach to its subject matter. This means that qualitative researchers study things in their natural settings, attempting to make sense of or interpret phenomena in terms of the meanings people bring to them. Qualitative research involves the studied use and collection of a variety of empirical materials – case study, personal experience, introspective, life story, interview, observational, historical, interactional, and visual texts that describe routine and problematic moments and meaning in individual lives.¹⁶⁴

In order to determine a set of updated and improved fraud/civil liability rules for banking regulation in Indonesia and recommendations for their implementation, a specific framework for legal and regulatory reforms will be furnished by this study.

William Hurlburt defines ‘law reform research’ as denoting ‘the alteration of the law in some respect with a view to its improvement’.¹⁶⁵ Law reform research is chosen in order to provide advice on changes to and reform of existing law. It involves the process of analysing fundamental social problems in order to provide policy-makers with action-

¹⁶³ Terry Hutchinson, *Researching and Writing in Law* (Thomson Lawbook, 2nd ed, 2006) 43–4.

¹⁶⁴ N K Denzin and Y S Lincoln, *Handbook of Qualitative Research* (Sage Publications, 1984) [at 2] quoted in John W Creswell, *Qualitative Inquiry and Research Design: Choosing among Five Traditions* (Sage Publications, 1998) 15.

¹⁶⁵ William H Hurlburt, *Law Reform Commissions in the United Kingdom, Australia and Canada* (Juriliber, 1986) as quoted in Hutchinson, above n 163, 56.

oriented and practical legal recommendations to assuage the problems.¹⁶⁶ Therefore, this research will use both descriptive and normative theories approaches.¹⁶⁷

This research is characterised by a multidisciplinary approach. Beside the legal aspects, the technological and economic aspects will be investigated and hopefully will provide a comprehensive approach to reforming the law concerning civil liability that is derived from unauthorised ATM/debit card transactions. The researcher will conduct interviews with and gather information from relevant parties (stakeholders) involved in ATM/debit card transactions in relation to the problem as it exists in practice, such as in regard to the denial of consumer rights or the improper application of law by banks and/or by court. As a main part of the strategy to obtain information, an open-ended interview will be devised to target consumers from several banks, victims of unauthorised ATM/debit card transactions, relevant bank officers/bank maintenance officers, law enforcement personnel, Bank Indonesia officers, alternative dispute resolution institution officers, and practitioners in related areas.

As part of law reform research, and given the fact that unauthorised ATM/debit card transactions involve cross jurisdictional problems where many countries share common EFT technology (including its perceived risks), comparative and benchmarking methodology will also be employed and become an important source for understanding current trends and regulatory standards in other countries that have similar problems concerning unauthorised EFTs and how they have resolved the loss allocation problems.¹⁶⁸ Other countries' regulations on loss allocation rules for unauthorised ATM/debit card transaction losses will be reviewed. Key requirements in regard to their approaches to overcoming the problems (and the degree to which they succeed) will be examined, interpreted and assessed under Indonesian conditions in order to fill the vacuum regarding the provision of detailed guidance on ATM/debit card regulation with respect to loss allocation rules. This will allow recommendations as to possible adoption to be made.

¹⁶⁶ Hutchinson, above n 163, 55–61.

¹⁶⁷ See Stephen Bottomley and Simon Bronitt, *Law in Context* (Federation Press, 3rd ed, 2006) 338–9. According to Bottomley and Bronitt, descriptive theories focus on evolution of legal form and the structure of legal system itself. They seek to explain why the laws are the way they are. Meanwhile, normative theories embody value judgments as to what the law ought to be.

¹⁶⁸ See Hutchinson, above n 163. According to him, the difference between comparison and benchmarking lies in the objectives. Comparisons tend to be theoretical and academic in approach. Benchmarking is comparison 'in the field'.

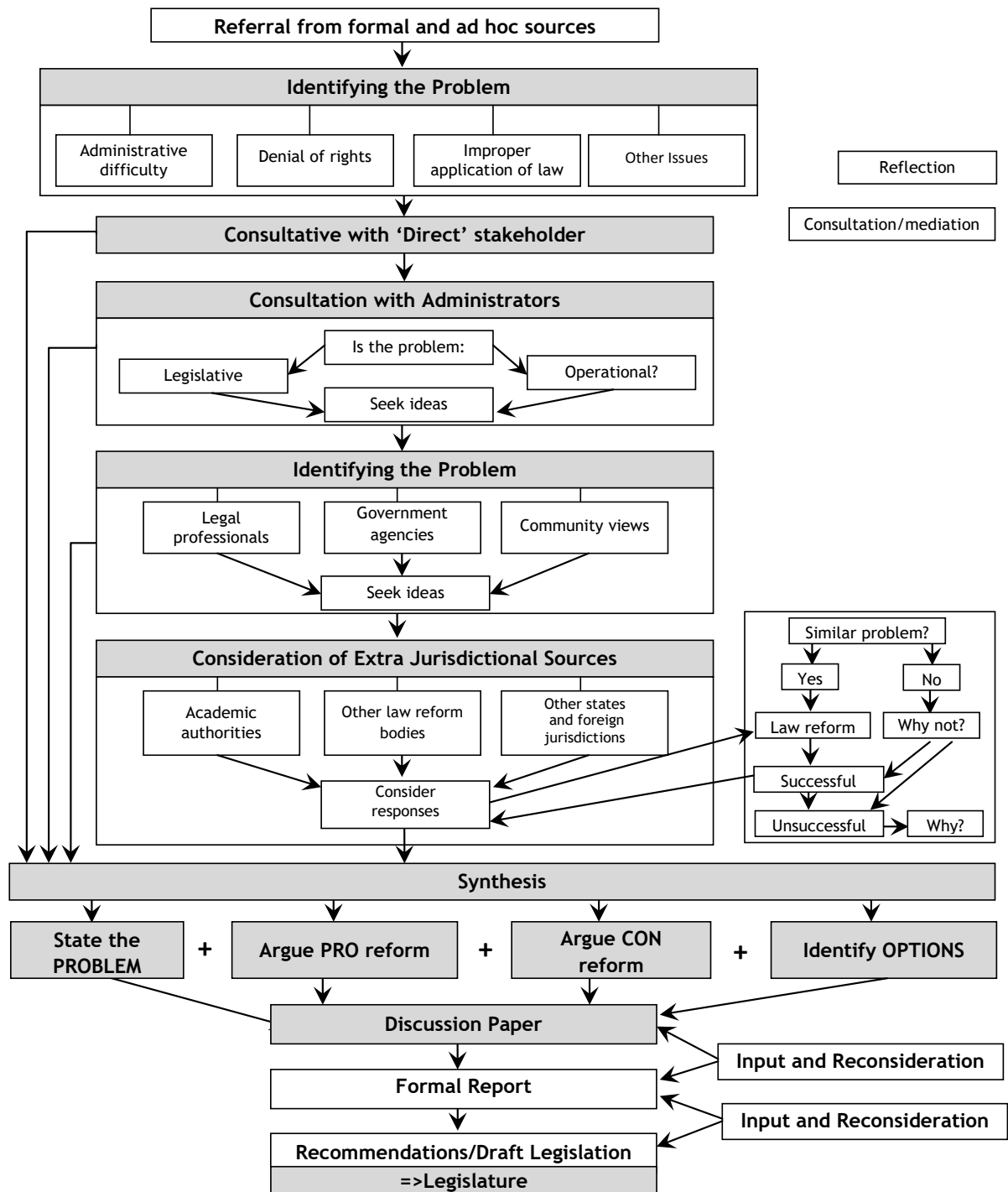
Pertinent provisions from Indonesian regulations will be critically analysed where appropriate from the relevant perspectives in this research. The data analysis method is used to interpret the statistical information to elicit relevant data, and to determine the wrongdoing patterns of, and regulatory trends in, unauthorised ATM/debit card transactions in Indonesia. This is an important aspect of the contextual background for understanding the threat posed by such transactions to the banking sector. This analysis will also contribute to a better understanding of banking practices concerning unauthorised ATM/debit card transactions and the legal aspects pertinent to such transactions.

The rise of ATM/debit card fraud commensurate with the growth of e-banking has been a common problem in many countries, some of which have already worked out viable solutions. Considering the dearth of literature in Indonesia and law governing e-banking, regulations dealing with unauthorised ATM/debit card transactions in different jurisdictions will also be identified and analysed with a view that Indonesia could 'identify solutions to specific or novel legal problems already encountered in other jurisdictions and learn from other practices and performance'.¹⁶⁹ As an end result, an in-depth analysis of materials will be provided in this thesis together with recommendations. Hutchinson provides an apt diagrammatic representation of the process to be undertaken in this thesis in his work on legal research. It is reproduced below.

¹⁶⁹ Ibid 106.

Figure 1: Law Reform Research Process

Law reform research process



Source: Terry Hutchinson, *Researching and Writing in Law* (Thomson Lawbook, 2nd ed, 2006)

1.6.2. Data Collection

This normative legal research will be conducted based on various primary and secondary sources of data. The primary sources of data are collected from interviews or surveys. Interviews were conducted with banking consumers, unauthorised ATM/debit card transaction victims, bank officials from seven big banks that were victims of the deluge of ATM/debit card fraud in Indonesia in early 2010 (namely: PT Bank Permata, PT Bank Central Asia, PT Bank Danamon Indonesia, PT Bank International Indonesia, PT Bank Mandiri (Persero), PT Bank Negara Indonesia 1946, and PT Bank Rakyat Indonesia),¹⁷⁰ law enforcement agency and judiciary personnel (such as police, prosecutors and/or judges), external disputes resolution officers, personnel from the payment system regulator (Bank Indonesia), banking experts, technology experts, academic lecturers, and personnel from Indonesia's payment system associations.

In principle, participants will be chosen on voluntary basis, and they will be selected based on their interest and consent to participate. The participants have the right to decide what questions they wish to answer and those which they do not wish to answer. The interview material will generally be de-identified for use in this thesis (unless the person gives permission for their identity to be divulged).

In order to ensure access to information, the possibility of anonymity was offered to informants reluctant to have their identity divulged. (Such requests from interviewees are understandable in the context of their employment). If respondents refused permission for their identity to be revealed, their interview responses and information supplied was de-identified in the author's database, using letters to identify a category of respondent (BO for bank Officer, C for consumer, BMO for bank maintenance officer) and a number allocated for the particular respondent in that category. For example Mr X (bank officer) will be written as BO-1; Mr Y (bank maintenance officer) will be written as BMO-1; Mrs. XY (consumer respondent) will be written as C-1; and so on.

Confidentiality and privacy of the participants will be protected in every stage of the research, i.e. collection stage, processing stage, and use stage. Processed information data will be stored in digital format on a password protected computer. The data will be

¹⁷⁰ ATMs owned by these seven banks represent 82% of total ATMs owned by banks in Indonesia.

held securely for five years after the research is completed. Only the researcher and supervisor will have access to this information. Appended to this thesis is the required ethics permission as well as an example of the open-ended interview questions used with interviewees.

The secondary sources of data are gathered from various law resources available in various libraries or online and consist of two sources of law, which are primary sources of law and secondary sources of law. The primary sources of law are those authoritative records of law made by law-making bodies.¹⁷¹ These records are the legislation made by parliament, the rules, regulations, orders and by-laws (known as delegated legislation of those bodies to whom legislatures have delegated their authority to make laws), and the formal reports containing authoritative judicial decisions, mainly from common law jurisdictions and referred to as judge-made law, case law or precedential law.

In this regard, primary data refers to any legislation in respect of e-banking activities, unauthorised ATM/debit card transactions, and consumer protection; rules, regulations, orders and by-laws from Bank Indonesia, consumer protection agency, and judicial decisions on cases involving e-banking frauds. All other sources not being primary materials are regarded as secondary sources of law, which generally include legal commentaries, legal textbooks, encyclopaedias, dictionaries, digests, journals, and the like. This data can be collected by using library facilities at universities, public and private libraries, manual and electronic journals, newspapers, magazines, official websites, and so on.

The secondary sources will be principally based on the following documents: journal articles, reports, convention commentaries, convention official records and synopses, records of cooperation programmes, and other documents both from domestic and international institutions concerning e-banking activities and e-banking fraud — such as those from Bank Indonesia, commercial banks (such as Bank Central Asia (BCA), Bank Mandiri, Bank Permata, Bank Negara Indonesia (BNI) Citibank, and Bank Rakyat Indonesia (BRI)), *yayasan lembaga konsumen Indonesia* (YLKI) (Indonesia's Consumer Organisation), switching company, the Bank for International Settlement (BIS), the United Nations (for example, the United Nation Commission on International Trade Law (UNCITRAL) Model Law), the South East Asia Central Bank (SEACEN),

¹⁷¹ Robert Watt, *Concise Legal Research* (Federation Press, 4th ed, 2001).

the European Union (for example, the EU *Convention on Cyber-Crime* and the *Payment Services Directive*), the Australian Securities and Investments Commission (ASIC), and Australia's Banking Ombudsman.

1.6.3. Data Analysis

The author collected, examined and critically analysed the relevant data systematically and in accordance with to the adopted research framework so as to be able to reach the most appropriate conclusions and ensure the submission of useful and feasible recommendations and reform proposals for the regulation of e-banking activities in Indonesia.

1.7. Outline of the Thesis

The balance of this thesis is organised as follows.

In Chapter 1, there is an examination of the reasons for the research being conducted, the background and research questions necessary to undertake this research, including the legal ramifications of unauthorised ATM/debit card transactions in Indonesia. Various opinions of scholars, experts and prominent institutions concerning unauthorised EFTs and losses allocation rules have also been revealed to be a stepping-stone for discussion within the thesis, along with the methodology used in collecting and processing data.

In Chapter 2, there is consideration of the fact that Indonesian laws regarding payment systems are still relatively unknown although electronic payment systems have been widely adopted in public transactions. The various conceptions of payment systems that are related to the scope of the thesis are therefore explored. This includes the explanation of retail payment system, bank and payment cards, ATM and debit card flow, their security and technological features such as the PIN magnetic stripe, and so on. Such material is needed as a gateway to understanding the overall context of this thesis. It also forms an introduction to the various risks and legal liability issues that might arise due to the fraud involving one or more specific technologies employed by one or more parties in the ATM/debit card system.

In Chapter 3, there is an examination of the risks that normally occur as a result of the inherent vulnerabilities in the ATM/debit card systems. The different terminology relating to identity theft and identity fraud in the payment card environment is also

explained, along with the motives, incentives and typology of fraudsters. The problems that nurture the proliferation of fraudulent activities are also revealed. Last but not least, the real victim and the significance of the cost exposure of unauthorised ATM/debit card transactions are also canvassed, so that the problems of fraud in the payment card system can be understood comprehensively.

In Chapter 4, there is an exploration of the rapid development of ATM/debit card transactions in Indonesia. There is also in-depth discussion of the general typologies of fraudulent methods employed by the fraudsters to perpetrate identity theft and identity fraud on consumer ATM/debit card data, including popular fraudulent methods employed by the fraudsters in Indonesia. Fraudster activities involving ATM/debit card data are divided according to the point of compromise and the degree of involvement of the bank and/or consumer. By understanding the technical methods involved in such frauds, including the possibility of consumer/bank negligence and/or fault in failing to secure the ATM/debit card transactions, it is expected that the party that should be responsible and liable for the fraud can be determined.

In Chapter 5, there is a discussion of the legal and regulatory framework regarding operational, technological, and security aspects related to the implementation of the payment card system in Indonesia. Last but not least, consumer protection regulation and issues related to weak consumer protection practices, fraud liability, and dispute resolution over unauthorised ATM/debit card transactions in Indonesia are also canvassed. To enhance the discussion and in order to have different illustrations of benchmarks on liabilities, liabilities regulation regarding unauthorised ATM/debit card transactions from several selected developed countries (such as the United States and Australia) will be examined for the purposes of a comparative study.

In Chapter 6, the theory and practice of liability and consumer protection law on dispute resolution between consumer and bank concerning unauthorised ATM/debit card transactions in Indonesia is drawn quite exhaustively. Tortious liability as the main principle in the law that is utilised by most in their claims for redress for such transactions in Indonesia is also discussed quite deeply along with its relevant liabilities rules such as occupiers' and vicarious liability. The defence that is commonly raised by banks in regard to a consumer's tortious liability claim is also discussed, including the defence's development and the latest CDSB and court decisions on these matters.

Therefore, this chapter clearly depicts to what degree or level the consumer protection principles and provisions are really operating in the practice of consumer payment card transactions in Indonesia.

In Chapter 7, there is a synthesis of the findings and data collected from archival research and interviews in respect of liabilities regulation and practice from the previously mentioned selected countries. To establish law reform for better liabilities regulation and practice in the banking industry in Indonesia, integrated analysis involving economic, technological and legal aspects will be undertaken in order to create clear, fair, detailed, and decisive liability regulation for unauthorised ATM/debit card transactions. Such law reform aims to create fair and just loss allocation regulation which will give the responsible party/parties the incentive to improve efficiency and security in card-based payment transactions.

In Chapter 8, there are conclusions and recommendations for better fraud liabilities regulation pertaining to unauthorised ATM/debit card transactions in Indonesia.

1.8. Conclusion

In this chapter, the background and significance of the study have been canvassed. In Indonesia, proliferation of the payment card system was also rapidly followed by increasing fraudulent activities (such as skimming and card trapping) being used to drain consumer funds from consumer bank accounts. Unlike credit cards that have more protection for consumers in term of technology employed (chip with EMV standard) and legal protection ('zero liability rules' for fraudulent use of the card), proprietary ATM/debit card consumers have less protection in both senses.

Unfortunately, many consumer efforts to seek recourse for their losses due to unauthorised payment card transactions are rejected by banks on the ground that the disputed transactions were deemed valid because they had been made using the right card (data) and PIN. This decision by the banks has been frequently criticised by security experts and consumer advocacy groups as unfair. To complicate the matter, most court verdicts regarding the matter also favour the banks. Consequently, many of the fraudulent ATM/debit card victims then air their negative experience in the mass media, which might also create reputational risk for banks and jeopardise trust between consumers and the banks.

Research questions, objectives, scope and research methods have been presented in sufficient depth, particularly with respect to civil liability that arises as a result of unauthorised ATM/debit card transactions in Indonesia. Since Indonesian law still does not have clear and enumerated regulations concerning fraud liability, proposals for law reform methodology can be put forward in regard to creating fair, just and decisive loss allocation rules for when consumers sustain monetary losses in the bank accounts because of unauthorised ATM/debit card transactions.

By contrast, many other countries already have relatively comprehensive regulations regarding fraud liabilities in electronic banking transactions. These include the *EFTA* and *Regulation E* (US) and the ePayments Code (Australia). In these regulations, the party or parties liable for damages if unauthorised ATM/debit card transactions occur have been clearly defined as have the conditions under which liability applies and the extent to which it applies. Hence, these regulations can be used as a common guidance to resolve disputes between banks and their consumers, regardless of which dispute resolution venue is chosen by the victims.

Therefore, detailed, comprehensive and just loss allocation rules (civil liability) for unauthorised ATM/debit card transactions in Indonesia are required to provide clear guidance, to avoid prolonged disputes between banks and consumers, and to provide incentives for parties appointed to improve duty of care and security in their own right. Considering that ATM/debit card transactions involve business value and the dominance of technological aspects, both in terms of the operational aspects of the banking process and in the methods employed by fraudsters, it is argued that to build detailed, comprehensive and just loss allocation rules, the regulations prescribed need not only take into consideration legal aspects, but also economic and technological ones.

CHAPTER 2 – OVERVIEW OF TECHNOLOGY, SECURITY, AND PROCEDURES EMPLOYED IN BANKS’ ATM/DEBIT CARD SYSTEMS

2.1. Introduction

The use of payment cards as part of the retail payment system has grown exponentially over the years and become one of the most attractive examples of the development and success of electronic banking throughout the world. Banks are keen to be involved in the payment card business because it gives significant fee based income and attracts consumer loyalty. One of the success factors for the proliferation of payment cards is the advance of technology, its standardisation and security features employed. Technology enables payment card transactions to be implemented in a relatively fast, secure, and efficient way compared to traditional banking business methods.

This chapter generally delivers information about how basically payment cards, in particular ATM/debit card transactions, work. The institutions involved in payment card infrastructure from one end to the other end are also described briefly. Besides covering the mechanisms involved and the flow of transactions, this chapter also covers the technological features of consumer activated terminals, such as ATM and EFTPOS devices, and the ATM/debit card with its magnetic stripe as an access device that is commonly used in the payment card system. In regard to ensuring that banks identify their consumers correctly in on-line transactions, the security aspect in general and the steps related to identification, authentication and authorisation methods in ATM/debit card transactions are also described.

2.2. Banks and Payment Cards¹⁷²

The ability of a bank to provide its products and services in the most effective and efficient way to its consumer/customers in forms that are (among other characteristics) more diverse, user friendly and easily accessible will provide a competitive advantage in comparison to other banks in the competition to attract more customers.¹⁷³

¹⁷² ‘Payment card system’ also known by different names such as ‘Card-Based Payment System’ or ‘plastic card payment’.

¹⁷³ Zeti Akhtar Aziz, *Electronic Payment in Malaysia* (2003) Bank for International Settlement, <<http://www.bis.org/review/r030516e.pdf>>.

The payment system as one of the major bank services is very important for commercial banks because the payment system's products and services provided to its consumers/customers prove to be a very important source of income for banks.¹⁷⁴ Further, Stewart highlights the importance of the payment system as an entry window for a bank's other services that will suit the consumer's needs and enable the development of a profitable and loyal consumer relationship.¹⁷⁵

Banks as financial intermediaries provide consumers with a variety of payment instruments in either debit or credit, for moving deposit balances held in banks. Payment orders can involve the transfers of balances between accounts held at the same bank (referred to as an 'on us' transaction or a 'book transfer') or more complicated transfer of balances where accounts are held at different banks.¹⁷⁶ Pingitzer and Summers further revealed that the increasing use of bank accounts in banks (and e-banking) marks a continuing trend for individual and business consumers to switch from using cash toward using an e-payment or cashless instrument by which current account balances held with banks are transferred.¹⁷⁷

The inception of payment cards as a replacement for money (cash) in trade has become one of the most important payment system innovations.¹⁷⁸ It is believed that payment card transactions and automated payments will become the primary cashless payment instruments in the future.¹⁷⁹ Recent research has concluded that there is a significant increase in the use of electronic payment by consumers, and debit and credit cards are

¹⁷⁴ Rambure and Nacamuli, above n 32, 188. See also Jamie B Stewart (Jr), 'Changing Technology and the Payment System' (2000) 6 (11) *Current Issues in Economics and Finance* 1, 2.

¹⁷⁵ Stewart (Jr), above n 174, 2.

¹⁷⁶ Hans J Blommestein and Bruce J Summers, 'Banking and the Payment System' in Bruce J Summers (ed), *The Payment System: Design, Management and Supervision* (International Monetary Fund, 1994) 18. See also Rambure and Nacamuli, above n 32, 7.

¹⁷⁷ Jurgen C Pingitzer and Bruce J Summers, 'Small-Value Transfer Systems' in Bruce J Summers (ed), *The Payment System: Design, Management, and Supervision* (International Monetary Fund, 1994) 108, 113. See also Rusch above n 106, 561, 563–4; Rambure and Nacamuli, above n 32, 8; Committee on Payment and Settlement Systems (CPSS), 'Policy Issues for Central Banks in Retail Payments' (Bank for International Settlements, 2003) 26.

¹⁷⁸ OECD Competition Committee, *Competition and Efficient Usage of Payment Cards* (Organisation for Economic Cooperation and Development, 2006) 10. See also: CPSS, *Policy Issues for Central Banks in Retail Payments*, above n 177, 20–3; Robert E Litan and Martin Neil Bailly, 'Introduction' in Robert E Litan and Martin Neil Bailly (eds), *Moving Money: The Future of Consumer Payments* (Brookings Institution Press, 2009) 6; Santiago Carbo-Valverde and Francisco Rodriguez Fernandez, 'Competing Technologies for Payments: ATMs, POS Terminals and the Demand for Currency' (Federal Reserve Bank of Chicago, 2009) 3.

¹⁷⁹ Pingitzer and Summers, above n 177, 113.

key factors in this development.¹⁸⁰ In addition, Rambure and Nacamuli claim that processing costs for payment cards are relatively low and driven by economies of scale. Consumers, merchants, and banks are keen to be involved in payment card transactions because it gives them many benefits.¹⁸¹

Banks can be involved in a payment cards system either as card issuers or as acquiring banks. Banks as the card issuer offer payment cards to consumers and, based on the contract with the consumer, will determine what type and the relative charges will be imposed on the consumer, and also determine and supply any other financial information pertaining to card usage. Banks that have an account relationship with merchants regarding any purchase using payment cards are called ‘acquiring banks’ or ‘acquirers’. Acquiring banks process consumer payment cards on their behalf; and for these services, merchants pay them by accepting a merchant ‘discount’ (in effect a charge against them as they receive an amount in their account that is slightly lower than the total charged for their products or services).¹⁸²

2.3. ATM and Debit Cards

From the inception of the card payment system until now, there have been two generations of cards that have emerged in the finance industry. Hayashi and Wang

¹⁸⁰ Federal Financial Institutions Examination Council (FFIEC), 'Retail Payment Systems' (Federal Financial Institutions Examination Council, 2004) 4. See also OECD Competition Committee, above n 178, 10.

¹⁸¹ Rambure and Nacamuli, above n 32, 37. According to Rambure and Nacamuli, benefit of payment card is as follows:

From the consumer’s standpoint, cards are cheap and convenient when used as a payment instrument, much less however as a source of credit. They also offer the best reconciliation facilities through statements listing full details of all transactions: date, name of merchant, amount in foreign and home currencies, and lately under regulatory pressure exchange rate and fees. These statements are generally sent by mail but also recently electronically, allowing automated reconciliation through home-finance or corporate accounting packages;

From the merchant’s standpoint, sales volumes rise as consumers are more prone to impulse buying if payment is deferred. The merchant fee paid to the acquirer is effectively an insurance premium that he will be paid, providing it has followed the security and anti-fraud measures dictated by the scheme. Retailers also benefit from the reduction in cash handling and safekeeping costs; and

For banks, cards can be an extremely profitable activity. The word “can” is used intentionally as profitability depends on service offered and sophisticated customer relationship management (CRM). Profitability is negligible on the basic domestic payment functions for debit cards and deferred debit cards, which explains why there is little competition in countries where those instruments prevail and why customers there rarely carry a card not issued by the bank holding their current account”.

¹⁸² Robert M Hunt, 'An Introduction to the Economics of Payment Card Networks' (Federal Reserve Bank of Philadelphia, 2003) 2. In the instance of a merchant discount that applies as follows: ‘[W]hen a consumer makes a \$1 purchase using a payment card, the acquiring bank pays the merchant slightly less than \$1 for that transaction’.

define these as follows: '[T]he first one is an ATM-only card, which allows card users to withdraw cash from ATMs. The second generation is the ATM/debit card, which allows card users to withdraw cash from ATMs as well as pay at the point of sale (POS)',¹⁸³

The innovation that extends the ATM card function from just cash withdrawal to payment instruments in various retail locations changes 'the industry from a one-sided market of ATM services into a two-sided market serving both consumers and merchants at the point of sale (POS)',¹⁸⁴

Regarding the debit card, Mann posits the view that, in general, there are two basic uses of a debit card. First, debit cards enable a bank consumer at any time to deposit money in and withdraw money from their bank account using an ATM, instead of going to the bank branch during banking hours. At the ATM, consumers can carry out any transactions that normally can only be performed with a bank teller's help, such as withdrawals, deposits, balance inquiries, or funds transfers.¹⁸⁵ The second function of a debit card — and one that boosts its use — is its use more as a payment instrument at a merchant.¹⁸⁶

Debit cards can be used as a substitute means of payment (for transactions otherwise conducted in cash or by cheque) for goods and services at the point of sale by authorising a withdrawal from their cheque or savings account, routed via an electronic funds transfer (EFT) network.¹⁸⁷ Hunt describes in his work the debit type of card transactions that utilise EFT network as '(on-line) PIN debit transactions because the cardholder must enter a four-digit personal identification number (PIN) to authorise the

¹⁸³ Fumiko Hayashi and Zhu Wang, 'Product Innovation and Network Survival in the US ATM and Debit Card Industry' (2009 (Revised 2011)) *SSRN Working Paper Series* 1, 6. See also FFIEC, *Retail Payment Systems*, above n 180, 14.

¹⁸⁴ Hayashi and Wang, above n 183, 2.

¹⁸⁵ Ronald J Mann, *Payment Systems and Other Financial Transactions; Cases, Materials, and Problems* (Aspen Publishers, 3rd ed, 2006) 160.

¹⁸⁶ A merchant must have a contract in advance either with card-issuing bank (propriety network) or with a network (switching company) that processes debit cards for the card-issuing bank, in order to enable payment by debit card.

¹⁸⁷ Geva, *The Law of Electronic Funds Transfer*, above n 83, 1–33. See also Rambure and Nacamuli, above n 32, 33–4; Committee on Payment and Settlement Systems (CPSS), 'Retail Payments in Selected Countries: A Comparative Study' (Bank for International Settlements, 1999) 4–5.

transaction. Funds are then immediately withdrawn from the associated bank account'.¹⁸⁸

2.3.1. Consumer Activated Terminals: ATM and EFTPOS

An alternative technology that has become more popular recently is electronic funds transfers that are initiated on a consumer-activated terminal. According to UNCITRAL, a consumer activated terminal is the EFT method where the instructions can be communicated directly to the bank's computer using a public access terminal such as an ATM and a POS terminal at merchants, or using an exclusive-access terminal such as a computer (home banking terminal), telephone, or mobile phone used solely by payer or payee and located at the payer's/payee's place of business or home.¹⁸⁹

Technological development and change has altered the way in which consumers interact with banks, reducing the significance of a bank's physical location and face-to-face interactions. Consumer activated terminals enable the automation of the EFT process without human intervention where authentication and authorisation of transaction is fully represented by a consumer's access device that has been provided by the financial institution.

Consumer activated terminals allow consumers to take advantage of banking products and services independently, optimally, efficiently and conveniently without being limited by geographic factors or restricted business hours as in conventional banking.

¹⁸⁸ Hunt, above n 182, 83–4.

¹⁸⁹ United Nations Commission on International Trade Law (UNCITRAL), 'UNCITRAL Legal Guide on Electronic Funds Transfers' (United Nations, 1987) 24–5, where in reference to this, UNCITRAL described the process as follows:

A large number of funds transfers which are initiated on customer-activated terminals pass through the entire funds transfer process with no human intervention on the part of the banks concerned. The computers of the banks verify that the technical norms required to make the transfer have been met, that the proper authentication for the transfer has been given and that the account of the transferor has a sufficient balance to support the debit to the account. In some cases, especially those involving large sums, an official of the sending bank may need to authorize the funds transfer before the instruction is acted upon, even though it has been initiated from a customer-activated terminal.

Electronic funds transfers which can be initiated by use of a plastic card with a magnetic stripe on the back containing information for identification of the card holder and his account, including either the personal identification number (PIN) or the information by which the bank's computer can derive the PIN by use of the proper algorithm, constitute a special sub-set of customer-activated electronic funds transfers. The concerns over the use of magnetic stripe cards as access devices arise in large part because of the technical problems in achieving an adequate level of security against fraud. These concerns have been highlighted by the fact that the vast majority of magnetic stripe cards are used for the initiation of consumer funds transfers, giving rise to concerns for consumer protection.

Consumers can make payments from their accounts by using various electronic instruments such as a credit card, a debit card or an automatic payment or telephone transfer feature. Consumers can also use ATMs to obtain cash and conduct other financial transactions (such as interbank funds transfers and account inquiries) at any time and anywhere.¹⁹⁰

ATM and Debit cardholders require consumer activated terminals to effect payment. Consumer activated terminal or card-accepting devices have many forms of independent terminals that connect to a bank's network by wire or wireless. These terminals may take several forms, such as PC card readers, PIN pads, EFTPOS terminals, ATMs, vending machines, and access control terminals.¹⁹¹

Nowadays, the proliferation of card-based payment is evident in almost every economy in their cashless transactions. Payment cards have boosted commerce in the bricks-and-mortar world as well as in an e-commerce environment. Payment cards have significantly changed the way consumers shop and merchants sell goods and services. As Carbo-Valverde and Fernandez observe: 'A common feature in banking systems all over the world is the deployment, in parallel, of both ATM and EFTPOS devices.'¹⁹² Payment cards facilitate access to funds in a cardholder's bank account either at an EFTPOS terminal or ATM. At an EFTPOS terminal, payment cards are commonly used for making payments to merchants for goods or for purchasing services, At ATMs, payment cards are mainly used for cash withdrawal; however, some other bank features such as inter-account transfers, balance query and bill payments can also be performed at ATMs.¹⁹³

2.3.1.1. Automated Teller Machines

ATMs are one of the obvious electronic banking forms that has enjoyed great acceptance by consumers since their inception for commercial business in 1968.¹⁹⁴ Basically, an ATM is a computerised device that enables banking consumers to perform

¹⁹⁰ Board of Governors of the Federal Reserve System, 'Report to the Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Product' (1997) 8.

¹⁹¹ This thesis will only focus on ATM and EFTPOS terminals.

¹⁹² Carbo-Valverde and Fernandez, above n 178, 3.

¹⁹³ Geva, *The Law of Electronic Funds Transfers*, above n 83, 1–33.

¹⁹⁴ Jayaram Kondabagil, *Risk Management in Electronic Banking: Concepts and Best Practices* (John Wiley & Sons (Asia) 2007) 3.

financial transactions independently without assistance from bank officers or tellers.¹⁹⁵ According to Claessens et al, 'The ATM is the first well-known system that was introduced to facilitate the access of the user to his banking activities.'¹⁹⁶

The main purpose of the first ATMs was cash withdrawal. By the early 1970s, ATM technology had developed many additional features, so that today they are able to take deposits, transfer money, provide cash advances from credit cards, and provide answers to balance enquiries, even produce 'mini-statements' for recent transactions. Interoperability of ATMs of multiple banking and other financial institutions or shared ATM networks began to emerge in the early 1970s.¹⁹⁷ However, until recently cash withdrawals were still the most frequent transactions at ATMs.¹⁹⁸ The probable rationale for this is that ATMs are more convenient and less expensive for the customer for cash withdrawal compared to accessing the bricks-and-mortar bank branch.¹⁹⁹

¹⁹⁵ Lawan Ahmed Mohammed, 'On the Design of Secure ATM Systems' in Lawan Ahmed Mohammed and Mubarak S. Al-Mutairi (eds), *Cases on ICT Utilization, Practice and Solutions: Tools for Managing Day-to-Day Issues* (IGI Global, 2010) 213–14. See also Australian Payments Clearing Association, *Regulations for Consumer Electronic Clearing System (CS3)* (2012) <http://www.apca.com.au/docs/payment-systems/cecs_regulations.pdf> 1.1. According to the Australian Payments Clearing Association (APCA) definition in its Regulations for Consumer Electronic Clearing System, ATM means:

An approved electronic device capable of automatically dispensing cash in response to a cash withdrawal transaction initiated by a Cardholder. Other transactions (initiated by a debit card) such as funds transfers, deposits and balance enquiries may also be supported. The device must accept either magnetic stripe cards or smart (chip) cards where transactions are initiated by the Cardholder keying in a Personal Identification Number (PIN). Limited service devices (known as "cash dispensers") that only allow for cash withdrawal are included.

¹⁹⁶ Joris Claessens et al, 'On the Security of Today's Online Electronic Banking Systems' (2002) 21(3) *Computers & Security* 253, 253.

¹⁹⁷ Hayashi and Wang, above n 183, 3. See also Anu Arora, *Electronic Banking and the Law* (IBC Financial Books, 1988) 111.

¹⁹⁸ In Indonesia, the ATM cash withdrawal also predominates ATM transaction volume with a 66.80% share compared to intra-bank transfer (19.23%), inter-bank transfer (7.55%) and merchant payment (6.43%). See Bank Indonesia, 'Laporan Bulanan Sistem Pembayaran Periode Maret (Payment System Monthly Report: March 2013)' (2013) 22. Given this fact, it is not surprising that banks in Indonesia tend to increase the number of their ATMs every year in order to 'spoil' their consumers and create reliable fee based income source. However, this fact probably also explains why fraudsters in Indonesia tend to target ATMs as a favourite point of compromise compared to EFTPOS. Some reasons for their choice are: (1) most ATMs are located outside bank branches and unguarded, hence proceeding with such crime is definitely more secure with its high level of anonymity; (2) consumer transaction volume at ATMs is very high, hence great opportunity for the potential victims data to be compromised by fraudsters conducting identity theft at ATMs with the various fraud methods available (such as card trapping, skimming or infected malware).

¹⁹⁹ Diana Hancock and David B Humphrey, 'Payment Transactions, Instruments, and Systems: A Survey' (1998) 21 *Journal of Banking & Finance* 1573, 1587. See also, Fumiko Hayashi, Richard Sullivan and Stuart E Weiner, 'A Guide to the ATM and Debit Card Industry' (Federal Reserve Bank of Kansas City, 2003) 19–20.

In terms of location, at the inception of ATMs, bank branches were the most common place for the installation of ATMs (also known as on-premises ATMs). However, later (as commonly seen today), ATMs are also deployed at off-premises locations, generally where people tend to gather or come frequently, such as malls, airports, restaurants, petrol stations, and grocery and convenience stores. From the business viewpoint, the proximity of ATMs as sources of cash for customers can build customer traffic as well as the value and volume of transactions per customer.²⁰⁰

2.3.1.2. EFTPOS Terminals

The EFTPOS network has emerged as a further development of on-line financial services provided by the banking industry that facilitate bank consumer access to their funds at point-of-sale retailers for the purchase of goods and services. Some retailers also allow the cardholder to withdraw cash from EFTPOS, which made EFTPOS (as well as ATMs) an alternative device that can operate as a facility for banking consumers to source cash from their accounts. Arora defines EFTPOS as ‘a payment system which enables goods or services to be paid for by transmitting over a communications network details of the transaction to both the customer’s and retailer’s bank without the use of paper vouchers’.²⁰¹

2.3.2. Card Technology

Payment cards have been recognised as a payment instrument and for identification purposes for quite some time. Hendry notes that ‘Diners Club issued the first plastic cards (what we would now call a “travel and entertainment card”) in 1950; the first plastic credit cards were issued by Bank of America in 1960’.

Basically, the payment card system employs what is called a ‘token’ in their operation. The token systems typically authenticate the token or payment card (such as ATM card or debit card) as an access card and assume that the user who was issued the token is the one who is requesting access to the system.²⁰² According to Hendry, the ‘payment card is one element in a distributed computer system. In some cases, it is providing data to

²⁰⁰ Hayashi, Sullivan and Weiner, above n 199, 22. See also Adelowo Solomon Adepoju and Mohammed Enagi Alhassan, ‘Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria - A Case Study of Selected Banks in Minna Metropolis’ (2010) 15(2) *Journal of Internet Banking and Commerce* 1, 3.

²⁰¹ Arora, above n 197, 83.

²⁰² Federal Financial Institutions Examination Council (FFIEC), *Information Security* (Federal Financial Institution Examination Council, 2006) 29.

the system; in other cases, it allows access to a program or to data on the host system.²⁰³

The most striking occurrence of the payment card in the banking industry has been the development of the credit card, debit card and ATM card. Prepaid cards or ‘electronic money’ is the latest development of payment card in payment system industries around the world.²⁰⁴ ATM and debit cards allow consumers to access their bank accounts using consumer-activated terminals in a direct debit mode. Besides the data recorded in the magnetic stripe of the payment card (or inside the chip for payment cards that have already embraced chip card technology), the security of the payment card transaction is mainly protected through the use of a PIN which functions as a password for the system.²⁰⁵

2.3.2.1. Plastic Card and the Magnetic Stripe

The magnetic stripe card was first invented by IBM in 1960 and used for the first time in the United States for security purposes. In terms of the technology employed, the security of the magnetic stripe technology used today has been improved but basically still uses the same technology that was developed in 1960. A 12.7mm (or half inch) wide strip of magnetic stripe tape that is bonded to the physical card remains the most popular form of card technology for the automatic reading process.²⁰⁶ According to Greenstein and Feinman, ‘a magnetic stripe card is a small plastic card that has some form of magnetically encoded strip or strips on its exterior’.²⁰⁷ They note that generally

²⁰³ Mike Hendry, *Smart Card Security and Applications* (Artech House, 2nd ed, 2001) 138–9.

²⁰⁴ Electronic money normally used for micro payment or for transportation fee payment.

²⁰⁵ M S Madan and M A Reid, ‘Data Processing Aspects of the Integrated Circuit and Magnetic Stripe Cards’ (1992) 22(1) *Information & Management* 41, 41.

²⁰⁶ Hendry, above n 203, 37. According to Greenstein and Henry:

On-line magnetic strip cards are used to read customer information from the strip. ... information is then used to access information about the cardholder from a central computer. These types of cards are commonly used for debit cards, credit cards, library cards, and building and machine access. Off-line magnetic strip cards actually store information that can be interpreted by the card reader and altered. For example, vending machine and telephone cards often use this technology to store the amount of money or call units to the cards. Some magnetic strip cards serve both on-line and off-line purposes. Lastly, magnetic strip cards that are combined with smart card technology are called hybrid cards.

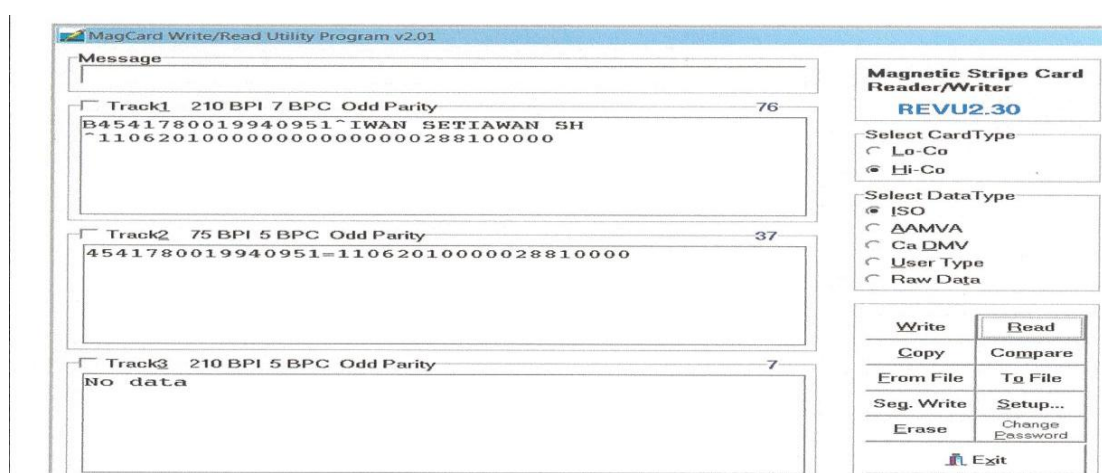
See Marilyn Greenstein and Todd M Feinman, *Electronic Commerce: Security, Risk Management and Control* (Irwin McGraw-Hill, 2000) 306.

²⁰⁷ Greenstein and Feinman, above n 206, 305–6.

magnetic stripe cards have three types: on-line strip, off-line strip or a smart-card hybrid.²⁰⁸

In the banking industry, the main purpose of the plastic card's magnetic stripe is to supply cardholder identity and account information rapidly and accurately when the card is used at a consumer activated terminal, such as ATM or EFTPOS.²⁰⁹ As Radu further states: '[T]he tracks contain extensive financial data about the cardholder, the issuer, as well as the financial parameters that serve in the process of terminal risk management'.²¹⁰ There are three data tracks within a magnetic stripe.²¹¹ However, bank payment cards such as the credit card, debit card and ATM card, typically use only track 1 and 2 as shown at Figure 2 below.

Figure 2: Example of ATM/Debit Card Data on the Magnetic Stripe²¹²



2.3.2.2. Integrated Circuit Card (ICC)/Chip Card

Most card payments are conducted using ATMs and debit cards equipped with a magnetic strip or stripe. The magnetic stripe is a technological device facilitating a faster authorisation process using the pre-recorded information stored on a card. Due to fraud issues, many new payment cards (especially credit cards) have more recently been

²⁰⁸ Ibid 306.

²⁰⁹ Madan and Reid, above n 205, 43–4. See also Diebold Incorporated, *White Paper: Battling Card Fraud through Chip and PIN Technology* (2011) 2. Document can be retrieved from: <http://www.diebold.com/atmsecurity/security/EMV_WhitePaper.pdf>.

²¹⁰ Christian Radu, *Implementing Electronic Card Payment Systems* (Artech House, 2003) 21.

²¹¹ Radu, above n 210, 22. See also Madan and Reid, above n 205, 43–4.

²¹² The author used a magnetic card reader/writer MSR805 to read the payment card. This device is legitimately bought on-line from e-bay and was purchased along with a portable mini skimmer for only around AUD300. Once the data was captured from a magnetic stripe card and moved to a computer (as shown in Figure 2), it is then ready to write (encode) on to any other magnetic stripe card, such as the card of another bank (it will override the existing data), a white plastic card, hotel access door cards, and so on. All the read and write processes only take only a few seconds.

equipped with a memory chip — such cards are also known as ‘smart’ cards.²¹³ This is a card with a built-in microchip that carries a wider range of information than a card with a magnetic stripe alone. The stored data is far more protected from physical damage and it is not susceptible to damage from magnetic fields. Furthermore, smart cards can store at least 100 times more data than magnetic stripe cards.

Payment cards have traditionally employed magnetic stripe technology on the back of the card. This records the cardholder’s essential financial information in connection with an account at the bank, and enables this information to be automatically captured at ATMs or EFTPOS terminals. Chip cards, a newer and more advanced and secure technology compared to magnetic stripe technology has been introduced in card-based payments. However, the implementation of this new technology has been very slow, as the technology is still relatively expensive,²¹⁴ and banks have to withdraw and re-issue payment cards for their entire consumer base and also enhance or replace EFTPOS terminals.²¹⁵

Many commentators have said that a smart card is far more secure than a magnetic card. As Master and Turner suggest, it overcomes many frauds that target magnetic stripe cards especially skimming fraud, and is being introduced to accompany magnetic stripe card technology. They argue that a chip card offers greater protection for cardholder data on the card, because it provides a better method of storing data and includes a control microprocessor, an encryption/decryption engine, a read-only memory containing an operating program, and a small amount of reusable memory.²¹⁶ The adoption of chip technology is being driven worldwide by Visa and Mastercard under

²¹³ James R Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering* (CRC Press, 1999) 68.

²¹⁴ In the Indonesian context, see Caroline Damanik, *Mahal, Realisasi "Magnetic" ke "Chip" Pelan-Pelan* [Expensive, the Realisation from "Magnetic" to "Chip" Slowly] (2010) Kompas.com <<http://megapolitan.kompas.com/read/2010/01/23/09164112/Mahal.Realisasi.Magnetic.ke.Chip.Pelan-pelan>>. See also Herdaru Purnomo, *Perbankan Nasional Butuh Rp 2 Triliun Untuk Beralih ke Kartu Chip* [National Banks Need Rp2 Trillion to Switch to Chip Card] (2010) Detik.com <<http://finance.detik.com/read/2010/01/22/120138/1283899/5/perbankan-nasional-butuh-rp-2-triliun-untuk-beralih-ke-kartu-chip>>.

²¹⁵ Pingitzer and Summers, above n 177, 112. See also Geva, *The Law of Electronic Funds Transfers*, above n 83, 6–13. See also Radu, above n 210, 10. See also Rambure and Nacamuli, above n 32, 35.

²¹⁶ Gerry Masters and Philip Turner, 'Forensic Data Recovery and Examination of Magnetic Swipe Card Cloning Devices' (2007) 4 *Digital Investigation* 16, 21–2.

the EMV (Europay, MasterCard, Visa) standard and has proven to be quite a success in combating and reducing fraud.²¹⁷

However, due to a business approach to ensure that the chip card can be accepted in the foreign countries that still have not implemented chip card technology, the ATM/debit card with chip technology is always still coupled with a magnetic stripe. Hence, the issue of skimming cardholder data within the magnetic stripe on the chip card still exists. In addition, the chip card has some similar vulnerabilities to the magnetic stripe card, including some conventional fraud methods such as lost or stolen card, card trapping, malware, packet sniffing or data breach.²¹⁸ However, the chip card will not be discussed in this thesis, because until recently ATM/debit cards transactions in Indonesia were still using magnetic stripe cards.²¹⁹

2.4. The Importance of Security Procedures in ATM and Debit Card Transactions

The payment card, as one of the most popular and pervasive payment instruments in the 21st century, can increase economic efficiency as a result of the employment of advanced computer technology and help transform the modern payment system. Advancements in computer technology enable banks to continue to expand the variety of retail payment services to their customers and obtain better profits for shareholders at a relatively lower cost.

As more bank payment system instruments such as the payment card system increasingly rely on information and network technology, there remains a need for banks to have proper technological standards and adequate security levels in order to

²¹⁷ Rambure and Nacamuli, above n 32, 35. See also Mark Rennie Davis, Jeff Stroud and Steven Paese, 'EMV: The Catalyst for a New US Payment Ecosystem' (MasterCard Advisors, 2012) 3.

²¹⁸ For more information about various identity theft and fraud methods on ATM/debit card, see Chapter 4.

²¹⁹ See Surat Edaran Bank Indonesia Nomor 14/23/DASP Perihal Perubahan Atas Surat Edaran Bank Indonesia Nomor 13/22/DASP perihal Implementasi Teknologi *Chip* dan Penggunaan *Personal Identification Number* pada Kartu ATM dan/atau Kartu Debet yang diterbitkan di Indonesia [Bank Indonesia Circular Letter Number 14/23/DASP Concerning Amendment of Bank Indonesia Circular Letter Number 13/22/DASP Concerning Implementation Chip Technology and the Use of Personal Identification Number on ATM and/or Debit Card Issued in Indonesia] Text of this circular letter can be retrieved from: <http://www.bi.go.id/NR/rdonlyres/0BB65029-579D-4EB0-88EE-A47B22610782/27021/se_142313.pdf>. According to this letter, chip technology and a six digit PIN should be employed on Indonesia ATM/Debit cards no later than 31 December 2015. However, Board of Governors' Bank Indonesia after their meeting on Thursday, 11 December 2014, has decided to delay the implementation of six digit credit card PIN until 2020 and will amend the relevant regulation accordingly.

reap the potential benefits from electronic payments without undermining the security and confidence of the bank consumers.

2.4.1. The Concepts of Identification, Authentication and Authorisation

2.4.1.1. Identification and Authentication

Generally, all computer systems are concerned with access control. Access control establishes restriction on access and on the ability to grant only authorised transactions access. An access control mechanism plays an important role in defending the system from unauthorised access. Typically, an access control becomes a point in between a user that tries to engage the system and the system resources as a target of engagement (such as applications, operating systems, firewalls, routers, files and database).²²⁰

Stallings and Brown briefly address how the access control works:

The systems first authenticate an entity seeking access. Typically, the authentication function determines whether the user is permitted to access the system at all. Then the access control function determines if the specific requested access by this user is permitted. A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this users. The access control functions consult this database to determine whether to grant access. An auditing function monitors and keeps a record of user accesses to system resources.²²¹

In banking activities, verifying consumer identity and acknowledging their authority before conducting any payment systems transactions is considered a basic security requirement. The idea of these procedures is to avoid or minimise the possibility of the occurrence of unauthorised banking transactions.

In traditional bricks-and-mortar banking transactions where face-to-face transactions were the only means to make paper-based transactions, generally the bank teller authenticated consumers by several means, among them by checking:

- the appropriateness and/or consistency of a consumer's name in her/his pass book against his/her identification card;
- consumer's identification card photo against his/her actual face; and

²²⁰ FFIEC, *Information Security*, above n 202, 22.

²²¹ William Stallings and Lawrie Brown, *Computer Security: Principles and Practice* (Prentice Hall, 2nd ed, 2012) 106–107. Authentication: 'verification that the credentials of a user or other system entity are valid'; Authorisation: 'the granting of a right or permission to a system entity to access a system resource. This function determines who is trusted for a given purpose'; Audit: 'an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures'.

- consumer's signature against his/her specimen signature that is normally recorded by the bank when a consumer initially opens an account.

However, since the inception and further advanced development of electronic banking in banking industries worldwide, the traditional identification and authentication methods are no longer feasible. Identity-related information consequently became more important for recognising consumers in non face-to-face transactions.

With the pervasive deployment of consumer-activated terminals by banks and their broad acceptance by bank consumers, there is frequently no face-to-face contact between banks and their consumers. Hence, banks have to adopt a substitute identification and authentication method based on consumers' identity-related information that is adequate and appropriate for implementation in terms of both banking technology and bank security policies.

Glaessner, Kellermann and McNevin argue that in order to be reliable, e-banking that involves financial transactions should be properly authenticated, verified and authorised.²²² Likewise, Kondabagil asserts that before a financial transaction takes place, the node or the user of the system should be tested in advance by identification, and authorisation processes.²²³

Although the term 'authentication' is used widely in the security system industries, its definition varies. The FFIEC states: 'Authentication is the verification of identity by a system based on the presentation of unique credentials to that system.'²²⁴ Meyer and Matyas define it as 'a process which proves that someone or something is valid or genuine'.²²⁵ Pipkin on the other hand depicts authentication as a 'verification of identity

²²² Glaessner, Kellermann and McNevin, above n 51, 125. According to them:

Authentication is used to assure the system that the party attempting to engage in an activity is, in fact, the party so designated. Verification is the means used to confirm that the party claiming a certain identity is legitimate. Finally, authorization is the means used to determine that the party engaging in a transaction has the requisite authority to access that portion of the system or to engage in that type of activity.

²²³ Kondabagil, above n 194, 98. According to him, identification 'determines who you are', authentication 'tries to ascertain that you are really who you claim to be', and authorisation 'determines what you are actually allowed to do'.

²²⁴ FFIEC, *Information Security*, above n 202, 26. See also Meyer and Matyas, above n 72, 474–5.

²²⁵ Meyer and Matyas, above n 72, 350.

to prevent impersonation and provide the level of trust necessary to utilise authorisations’.²²⁶

However, despite variations in the definition, the importance of authentication in the security system is not doubted by all players in the banking industries. A strong authentication method is important to ensure that the system has the ability to determine that the user who is gaining access is really who they are meant to be.²²⁷ An authentication method typically consists of unique credential factors. The factors must be acknowledged by both the entity being authenticated and the process authenticating the entity, which are user and the system itself.²²⁸

2.4.1.2. Authorisation

In e-banking, authorisation procedures are employed by banks to govern access and utilised in electronic payment system resources accordingly by authenticated users or consumers.²²⁹ Pipkin notes: ‘Authorization defines what attributes of which resource an authenticated user is allowed to utilise. They are what provide an entity’s privileges.’²³⁰

The importance of authorisation in payment transactions is twofold. For payers in payment transactions, it gives some kind of assurance that their resources in the bank will be safe because no one else could access them using their payment instrument. For merchants, authorisation gives them confidence that they will receive payment associated with the use of a valid payment instrument by the authenticated payer. As a result, payment instruments with strong authentication and authorisation procedures will most likely be well accepted by both bank consumers and merchants.²³¹

According to Sullivan, there are three requirements to authorise a transaction successfully: ‘First, the payment instrument and other hardware are authenticated.

²²⁶ Donald L Pipkin, *Information Security: Protecting the Global Enterprise* (Prentice Hall PTR, 2000) 131.

²²⁷ Ibid 129.

²²⁸ Ibid 129–30.

²²⁹ Claire Goddard and Michael Deakin, ‘Managing Treasury Security’ in Brian Welch (ed), *Electronic Banking and Treasury Security* (Woodhead Publishing, 1999) 5. See also CPSS, *Retail Payment in Selected Countries*, above n 187, 5, where it is stated:

An “authentication method” used during authorization procedures is a device or procedure which verifies that the user is authorized to use the payment system. Most, but not all, authentication methods also identify the account to be debited with the amount of the payment. Authentication is assuring the system that the person trying to gain access or engage in a certain activity is, in fact, the person s/he claims to be and that the person is authorized to engage in the act.

²³⁰ Pipkin, above n 226, 141.

²³¹ Sullivan, ‘Can Smart Cards Reduce Payments Fraud and Identity Theft?’, above n 33, 40–1.

Second, the identity of the payer is verified. Third, details of the transaction must satisfy risk parameters set by the merchant and the card issuer.²³²

2.4.2. Identification, Authentication and Authorisation in ATM/Debit Card Transactions: ATM/Debit Magnetic Stripe Card and PIN

In information security today, information security management has become one of the most important features to be established by institutions. Authentication as part of information security is probably one of the most essential processes to set up at the first stage since it typically poses the first line of defence against the possibility of fraudulent activities.²³³

In the payment card industry, the need to secure the system has been recognised from its inception. The security of card payment transactions is deemed a basic requirement as this will give confidence to institutions and customers. Consumer authentication is required to ensure the authenticity and integrity of a transaction.²³⁴

Because of the increasing incidence of frauds in e-banking environments, banks have developed improved security measures as demanded by legal and regulatory requirements to enhance the consumer authentication methods used to combat fraud in e-banking transactions. Because of this requirement, along with handwritten signatures, the PIN has become a primary choice by many institutions, including banks, to secure their transactions. From legal perspective, the recognition of electronic signature such as PIN as an equivalent to the signature of a person on a written document has long been known recognized as the adoption of the “functional-equivalence approach” doctrine.²³⁵

The PIN is a secret number created by banks or other card issuers as selected by individual cardholders and serves as an authentication method in electronic funds transfer transactions (EFT). Further, as Meyer and Matyas explain, ‘[a] PIN is a simple form of passwords, consisting usually of four to six digits, which can be used with a numeric keypad rather than a full keyboard.’²³⁶ They further assert that ‘the PIN is

²³² Ibid 40.

²³³ Jie Zhang et al, 'Improving Multiple-Password Recall: An Empirical Study' (2009) 18(2) *European Journal of Information Systems* 1.

²³⁴ Madan and Reid, above n 205, 41, 43–4.

²³⁵ CPSS, *Retail Payment in Selected Countries*, above n 187, 5. See also United Nations Commission on International Trade Law (UNCITRAL), 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment' (United Nations, 1996), 20. 40.

²³⁶ Hendry, above n 203, 76.

basically the cardholder's electronic signature, and serves the same role in an EFT transaction as a written signature serves in a conventional financial transaction'.²³⁷ Therefore, in consumer transactions, a PIN is not used to identify the customer, instead its function is as a signal for the legitimacy of the payment authorisation.²³⁸ Given its crucial role in payment card transactions, it is important to understand how a PIN really works.²³⁹

However, Mohammed has argued that for payment card authentication, such as for use at an ATM, there has been no significant improvement since its inception in the 1960s.²⁴⁰ He states that the authentication method typically involves an ATM card or token and the cardholder's PIN as a password.²⁴¹ In other words, consumers are identified by something that the consumer has (a banking card with a magnetic stripe) and something the consumer knows (their PIN).²⁴² The use of a PIN is also described by Pipkin as an old authentication method. He says that, 'using a password to authenticate an identity is as old as [using] a sentry [to guard] ... the gate of an ancient city'.²⁴³ Nevertheless, Hendry argues that 'PINs should only be regarded as a secondary identity check; the card is the primary identification'.²⁴⁴

²³⁷ Meyer and Matyas, above n 72, 430–1. See also Madan and Reid, above n 205, 48.

²³⁸ Marco Gercke, 'Legal Approaches to Criminalize Identity Theft' in United Nations Office on Drugs and Crime (ed), *Handbook on Identity-related Crime* (United Nations, 2011) 12. See also Australian Payments Clearing Association, above n 195. One of the clearest definitions regarding the PIN as an authentication method in payment transactions can be found in the regulations for Consumer Electronic Clearing System (CECS)-Australia. In this regulation, a PIN is described as follows: "PIN" means a personal identification number which is either issued by an Issuer or selected by a Cardholder for the purposes of authenticating the Cardholder by the Issuer of the Card'.

²³⁹ It is important to understand the detailed flow of PIN in payment card transactions since a PIN might be captured during transmission from a consumer activated terminal, node, or switching point to host terminal, in particular when a PIN in an unencrypted form when being re-formatted at switch points. See Omer Berkman and Odelia Moshe Ostrovsky, 'The Unbearable Lightness of PIN Cracking' (2007) 4886 *Lecturer Notes in Computer Science* 224, 224–5. The material comprises part of a collection of 2007 conference and workshop proceedings: Sven Dietrich and Rachna Dhamija (eds), *Financial Cryptography and Data Security*, 11th International Conference (IFCA 2007) Scarborough, Trinidad and Tobago, 12–15 February 2007, and 1st International Workshop on Usable Security (USEC 2007) Scarborough, Trinidad and Tobago, 16 February 2007. Text of this document at: <http://cs5128.userapi.com/u11728334/docs/5ad84be07c9d/Sven_Dietrich_Financial_Cryptography_and_Data_S.pdf#page=243>.

²⁴⁰ Credit card or debit card schemes under the Visa and Mastercard brands have implemented new chip card technology to store cardholder information (smart card) under their EMV programme. This new chip card has proven to be more secure and has greater capabilities compared to magnetic stripe cards; however, most proprietary cards issued by banks typically still rely on magnetic stripe cards.

²⁴¹ Mohammed, above n 195, 214. See Hendry, above n 203, 37. See also: Meyer and Matyas, above n 72, 475. See also Radu, above n 210, 388.

²⁴² Meyer and Matyas, above n 72, 481. See also Mohammed, above n 195, 214.

²⁴³ Pipkin, above n 226, 130.

²⁴⁴ Hendry, above n 203, 76.

In on-line ATM/debit transactions with a PIN as a means of identification, authentication and authorisation happen automatically in a consecutive manner, through a bank network or via a switch that links the EFTPOS/ATM terminal of the acquiring bank (payee) with the issuer card institution (payer). This process relies upon a telecommunication network (line or wireless) as a bridge and computer devices routing the card and account information between computer activated terminals and the cardholder's financial institution or its substitute if the process has been outsourced to third party institutions.²⁴⁵

From the work of Radu,²⁴⁶ and Meyer and Matyas,²⁴⁷ we can define in brief payment card identification, authentication and authorisation, as follows:

1. Identification:
 - a. Cardholder at consumer activated terminal, such as an ATM or EFT-POS terminal, dips or swipes their magnetic stripe card into the machines.
 - b. The machines then read the cardholder's information from the magnetic stripe card.
2. Authentication:
 - a. Cardholder types PIN into the PIN pad of an ATM or POS terminal.
 - b. Magnetic stripe card and PIN data are transmitted from the consumer-activated terminal to the issuer host system.
3. Authorisation:

If cardholder enters the correct PIN, the funds in the cardholder's account are still adequate to cover the amount of transactions, and the type of transaction is permitted, then the system will authorise the electronic funds transfer.²⁴⁸

Continued innovation in authentication technology has recently resulted in the development of improved authentication methods, which in general, can now be classified into 'shared secrets such as smart cards or tokens, digital certificates, and

²⁴⁵ Committee on Payment and Settlement Systems (CPSS), 'Clearing and Settlement Arrangements for Retail Payments in Selected Countries' (Bank for International Settlement, 2000) 3.

²⁴⁶ Radu, above n 210, 388.

²⁴⁷ Meyer and Matyas, above n 72, 475. See also: Sullivan, 'Can Smart Cards Reduce Payments Fraud and Identity Theft?', above n 33, 40–1; CPSS, *Clearing and Settlement Arrangements for Retail Payments in Selected Countries*, above n 245, 28–9.

²⁴⁸ See CPSS, *Clearing and Settlement Arrangements for Retail Payments in Selected Countries*, above n 245, 3, 43. According to CPSS, authorisation in payment card system means 'the approval or guarantee of funds to be transferred'.

biometric identifiers’.²⁴⁹ However, the PIN as a fixed password is still widely used because of its ease of implementation and use with relatively low investment, even though it has many drawbacks (such as password guessing, dictionary attacks and being subject to social engineering).²⁵⁰

2.5. Conclusion

The development of the payment system and the proliferation of electronic funds transfer in the banking industry benefited from advances in information technology and communications networking. The payment card system as one of the most prolific features of the electronic retail payment system offers many benefits to consumers, such as, relatively unlimited access to banking services outside office hours, greater convenience and easy access to pervasive consumer activated terminals. For the banks, the benefit of payment card products comes from greater consumer-generated fee based income, deposits and loyalty.

What appears to be a seamless and simple transaction in payment cards transactions actually involves many complex technical infrastructures (such as ATM, electronic data capture (EDC), networks, host computers, switch networks, storage and so on) and the involvement of many parties (such as issuer and acquirer banks, third party processors, ISOs, switching companies, network vendors, consumers, and so on). However, the nature of consumer activated terminals such as the ATM and EFT-POS terminals that are located mostly outside of bank premises, empirically create a security issue for consumer due to lack of supervision.

Magnetic stripe cards and PINs are still heavily used in most ATM/debit card transactions. Unlike scheme credit cards that have moved to chip technology with EMV standards driven by Visa and MasterCard, scheme debit cards and proprietary ATM/debit card systems mostly still rely on old and relatively weak magnetic stripe technology as a means of identification, and PINs as a means of authentication and authorisation — and hence are relatively vulnerable to fraudulent activities.

²⁴⁹ Kondabagil, above n 194, 99–101.

²⁵⁰ Claessens et al, above n 196, 253, 263.

CHAPTER 3 – TYPOLOGY OF THE INHERENT RISK AND VULNERABILITIES THAT MAKE ATM/DEBIT CARD FRAUD FAVOURED BY FRAUDSTERS

3.1. Introduction

The development of ATM/debit card payments as an example of electronic payment in e-banking activities has given greater efficiency and many benefits to the banking industry and its consumers. This did not create new risks; however, e-banking transactions that heavily depend on information technology and computer networks have amplified existing risks in traditional banking activities.

Specific risks that commonly intertwine with ATM/debit card operations other than operational risk are fraud risk, reputation risk and legal risk. These inherent risks have occurred because of the nature of retail payment system operations that generally only employ moderate security features to balance their security costs, the use of inherited computers/software, and consumer convenience. The relatively open and un-guarded environment of consumer-activated terminals is a great incentive for fraudsters to perpetrate identity theft and/or fraud. As a result, the payment system industry and the regulator are keen to contain payment system risk, especially payment card fraud, in order to maintain a robust and trusted payment system, as consumer trust and confidence are paramount in the payment system.

This chapter generally explains the inherent risk and vulnerability of the payment card to fraud, and factors that affect it; and the typology of fraudsters in regard to payment cards, and their application in payment card fraud. The costs and the real victims of the ATM/debit card fraud are also described, so that the provider of the ATM/debit card system and payment system authority can give more attention to and show greater responsibility in protecting the consumer from fraudulent activities.

3.2. General Overview of Risk in Retail Payment System

The development of e-banking may contribute to improved efficiencies in the banking and payment system. E-banking could give banks greater capability to offer a new and wider range of products and services such as electronic payment systems with lower operating costs, expand their market for traditional deposit-taking and credit extension

activities, and strengthen their competitive position in offering existing payment services.²⁵¹ Schaechter noted that e-banking enables new and existing customers to no longer be subject to time and geographic limits.²⁵²

Along with opportunities, e-banking generates expanded risks for financial institutions.²⁵³ It increases the bank's dependence on information technology and the computer-networked environment.²⁵⁴ All of these factors increase the technical complexity of many operational and security issues, and greatly magnify the importance of security controls, customer authentication techniques, data protection, and customer privacy standards.²⁵⁵ Not to mention that the ramifications include effects on various legal aspects, such as the rights and liabilities of the parties involved in e-banking transactions.

With the pervasive development of electronic payment system technology, the dimension and scale of payments fraud has grown accordingly. Electronic communication and technology that support electronic payment system and e-commerce have been utilised in recent years exhaustively by fraudsters to commit fraud.²⁵⁶ The natural advantages of electronic payment systems, where computer data is easily stored, copied and manipulated, can also be a disadvantage when it comes to fraud.²⁵⁷ Gates and Jacob argued that this specific condition along with the swiftness of electronic payments, modern databases, online information sharing, and the number of bank

²⁵¹ Basel Committee on Banking Supervision, 'Risk Management for Electronic Banking and Electronic Money Activities', above n 3, 1.

²⁵² Schaechter, above n 91, 2. See also Tyree, *E-Commerce and Retail Banking*, above n 86, 1.

²⁵³ Rambure and Nacamuli, above n 32, 63. See also Bruce J Summers, 'The Payment System in a Market Economy' in Bruce J Summers (ed), *The Payment System: Design, Management, and Supervision* (International Monetary Fund, 1994) 4.

²⁵⁴ A computer network is the connection of multiple computers owned by multiple owners under contract or agreement, so that all information, applications and equipment as an object of the arrangement can be shared, typically through telephone lines, cable systems and/or wireless connection. The purpose of a computer network is to increase efficiency, convenience and access to bank consumers. However, this design by nature is more difficult to control compared to 'stand alone' computers that used to be used in traditional banking services. See Division of Supervision, Federal Deposit Insurance Corporation (FDIC), 'Electronic Banking: Safety and Soundness Examination Procedures' (Federal Deposit Insurance Corporation, 1998) 1–2.

²⁵⁵ Atiqur Rahman Khan and Masud Karim, 'E-Banking and Extended Risks: How to Deal with the Challenge?' (Working Paper, University of Rajshahi, 2010) <http://www.ru.ac.bd/finance/images/stories/working_papers/ebanking-edited.pdf> 2.

²⁵⁶ Drugs and Crime Prevention Committee, 'Inquiry into Fraud and Electronic Commerce' (Parliament of Victoria, 2004) 1.

²⁵⁷ Rambure and Nacamuli, above n 32, 63. See also Richard J Bolton and David J Hand, 'Statistical Fraud Detection: A Review' (2002) 17(3) *Statistical Science* 235; Hayashi, Sullivan and Weiner, above n 199, 99.

access points increased by bank, non-banks and third-party service providers have caused the scope of fraud to become more extensive.²⁵⁸

Glaessner, Kellermann and McNevin discovered that fraudsters now have more efficient and quicker ways to perpetrate old crimes such as fraud and theft, facilitated by an on-line environment, remote access, high-quality graphics and printing, and new multipurpose tools and platforms that are easily obtained.²⁵⁹ Furthermore, they state that the most distressing aspect of this fraud is that fewer skills are required to commit electronic payment crimes. This can occur because underground hacker websites provide multifaceted tools necessary to break into financial platforms.²⁶⁰

System efficiency in e-banking depends on public confidence and trust.²⁶¹ Confidence in the safety of payments is particularly important.²⁶² CPSS-BIS further emphasises that safety in retail payment systems is very important because it attracts public interest and affects consumer confidence and the functioning of commerce.²⁶³ Hence, any actual and reported risks could shake consumer confidence in retail payments systems.²⁶⁴

However, to maintain safety in retail payment systems is not an easy task. The regulator and the payment system industry have to be able to identify and understand what sort of risks may be involved in payment system transactions from time to time. Some questions — such as how they occur and are transmitted within the system, by whom they are borne, who are the perpetrators — are very important to know, before trying to find the right risk mitigation answer.

The retail payment system generally does not take elaborate and costly security measures, such as in the wholesale payment system. It would be far too expensive, involve longer processing times, or otherwise not be suitable for the retail payment

²⁵⁸ Tiffany Gates and Katy Jacob, 'Payments Fraud: Perception versus Reality - A Conference Summary' (2009) XXXIII(1) *Economic Perspectives* 7. See also Glaessner, Kellerman and McNevin, above n 51, 1; Pattama Malakedsuwan and Kenneth J Stevens, 'A Model of E-Fraud' (Paper presented at the 7th Pacific Asia Conference on Information Systems, Adelaide, 2003) 18–19.

²⁵⁹ Glaessner, Kellerman and McNevin, above n 51, 5.

²⁶⁰ Ibid 9.

²⁶¹ Federal Reserve Bank of Kansas City, 'The Changing Retail Payment Landscape: What Role for Central Banks?' (2009) xlv.

²⁶² Richard J Sullivan, 'The Changing Nature of US Card Payment Fraud: Industry and Public Policy Options' (2010) 95 *Economic Review* 101.

²⁶³ CPSS, 'Policy Issues for Central Banks in Retail Payments', above n 177, 8.

²⁶⁴ Federal Reserve Bank of Kansas City, above n 261, xlviii.

system.²⁶⁵ Conversely, the retail payment system with a larger numbers of participants generally employs a more moderate security system (having to adapt to the technology owned by the participants who are very diverse with not only domestic but also international participants).

While e-banking does not generate new types of risk compared to traditional banking products and services, nevertheless, because of the mixture of advanced and swift technology changes, third party service provider involvement in delivering e-banking products and services, lack knowledge in technology and e-banking risk issues among bank management and staff, and legal and regulatory ambiguity and uncertainty of the existing law on e-banking, and so on, e-banking has altered and sometimes amplified banking's traditional risks.²⁶⁶

Following the abundance of online fraud/crime, the United Nations²⁶⁷ concluded that fraud development could be attributed to several factors such as technological advances,²⁶⁸ lack of education,²⁶⁹ shortcomings in technology related laws,²⁷⁰ and fear of adverse publicity.²⁷¹

Many institutions and experts such as the Federal Financial Institution Examinations Council (FFIEC),²⁷² the United Nations Commission on International Trade Law (UNCITRAL),²⁷³ Roberds,²⁷⁴ Rusch,²⁷⁵ Pennathur,²⁷⁶ and Gates and Jacobs,²⁷⁷ concur

²⁶⁵ William Roberds, 'The Impact of Fraud on New Methods of Retail Payment' (1998) First Quarter *Federal Reserve Bank of Atlanta Economic Review* 43.

²⁶⁶ Electronic Banking Group, 'Electronic Banking Group Initiatives and White Papers' (Basel Committee on Banking Supervision, 2000) 12. See also Kondabagil, above n 194, 11, 15–16; FFIEC, 'E-Banking', above n 115, 18; Peter Grabosky, Russell G Smith and Gillian Dempsey, *Electronic Theft: Unlawful Acquisition in Cyberspace* (Cambridge University Press, 2001) 179.

²⁶⁷ United Nations, 'International Review of Criminal Policy' cited in Harry S K Tan, 'E-Fraud: Current Trends and International Developments' (2002) 9 *Journal of Financial Crime* 347, 347.

²⁶⁸ '[T]he easy availability of new technologies with high operational speeds, capacity and connectivity make [it easier for] unlawful activities ... to escape detection. Conversely, a majority of cybercrime victims are not technologically sophisticated or equipped enough to prevent, detect or deal with computer crime.': *ibid*

²⁶⁹ '[T]he lack of awareness of how to maintain a minimum level of security with regard to personal information or electronic property.': *ibid*.

²⁷⁰ '[M]ost law enforcement agencies lack the technical expertise as well as sufficient regulatory powers and equipment to investigate and prosecute fraudulent digital transactions.': *ibid*.

²⁷¹ '[I]n some cases when a crime is detected, business[es] have been reluctant to report criminal activity because of their concern as to how the publicity can cause embarrassment, loss of public confidence, investor loss or economic repercussion[s].': *ibid*.

²⁷² FFIEC, 'Retail Payment Systems', above n 180, 25.

²⁷³ UNCITRAL, 'UNCITRAL Legal Guide on Electronic Funds Transfers', above n 189, 11.

²⁷⁴ Roberds, above n 265, 1.

²⁷⁵ Rusch, above n 106, 566.

²⁷⁶ Pennathur, above n 54, 20.

on natural risks and vulnerabilities inherent in the operation of retail payment systems. As the CPSS asserts in its report:

From the moment of initiation of a non-cash payment until its settlement with finality, the participants in a transaction (payer, payee and one or more financial institutions) may be exposed to certain risks. These risks arise at the level of the individual payment, and where payments are netted at the aggregate level as well.²⁷⁸

The CPSS states in its report on ‘Clearing and Settlement Arrangements for Retail Payments in Selected Countries’, that (in general) risk in the retail payment system is comprised of fraud risk, operational risk, legal risk, and settlement risk (including liquidity and credit risks),²⁷⁹ and systemic risk. This view is consistent with that of the Basel Committee on Banking Supervision,²⁸⁰ Akindemowo,²⁸¹ Pennathur,²⁸² and Nsouli and Schaechter,²⁸³ who found in their studies that for e-banking activities, besides standard risks for traditional banking activities, particular risks are also applicable, namely operational risk, reputational risk,²⁸⁴ and legal risk.

Regarding concerns about security and fraud, Vrîncianu and Popa point out that ‘security is considered the central operational risk of e-Banking’, therefore security problems such as fraud risk cut across risk categories and can be classified not only as an operational risk,²⁸⁵ but also as a risk that would expose the bank to legal risk²⁸⁶ and reputational risk.²⁸⁷

²⁷⁷ Gates and Jacob, above n 258, 7.

²⁷⁸ CPSS, ‘Clearing and Settlement Arrangements for Retail Payments in Selected Countries’, above n 245, 11–12. See also FFIEC, ‘Retail Payment Systems’, above n 180, 24.

²⁷⁹ For risk definition, see CPSS, ‘A Glossary of Terms’, above n 5, 29, 45. *Settlement risk*: ‘general term used to designate the risk that settlement will not take place as expected. This risk comprises both credit and liquidity risk’. Liquidity risk: ‘the risk that a counterparty (or participant in a settlement system) will not settle an obligation for full value when due. Liquidity risk does not imply that a counterparty or participant is insolvent since it may be able to settle the required debit obligations at some unspecified time thereafter’. See also Michele Braun et al, ‘Understanding Risk Management in Emerging Retail Payments’ (2008) 14(2) *Economic Policy Review - Federal Reserve Bank of New York* 137, 140.

²⁸⁰ Basel Committee on Banking Supervision (BCBS), ‘Risk Management Principles for Electronic Banking’ (Bank for International Settlement, 2003) 5–9.

²⁸¹ Akindemowo, above n 95, 126–27.

²⁸² Pennathur, above n 54, 2111–13.

²⁸³ Nsouli and Schaechter, above n 10, 3–5.

²⁸⁴ *Reputational risk* is the risk of significant negative public opinion that results in a critical loss of funding or customers. Reputational risk may arise among other things from a significant breach of security, whether as a result of external or internal attacks on a bank’s system, including mistakes, malfeasance, and fraud by third parties. See BCBS, ‘Risk Management for Electronic Banking and Electronic Money Activities’, above n 3, 7.

²⁸⁵ Operational risk has an array of risks included in its definition, including security risk, fraud risk, and legal risk. For further explanation, see BCBS, ‘Risk Management for Electronic Banking and Electronic Money Activities’, above n 3, 5–8. See also FFIEC, ‘Retail Payment Systems’, above n 180, 27–9; CPSS, ‘Clearing and Settlement Arrangements for Retail Payments in Selected Countries’, above n 245, 10–11.

Kondabagil echoes Vrîncianu and Popa's view by stating that any kind of unauthorised disclosure or exploitation of consumer data will expose banks to both reputational and legal risks.²⁸⁸ Braun et al further highlight that it becomes more important to raise the question of legal risk if case law is less well developed or simply that the drafters of established laws may not have foreseen some of the ways in which payments are initiated, processed, and settled.²⁸⁹

3.3. Payment Card Fraud

When Willie Sutton,²⁹⁰ a prolific 19th Century bank robber was asked why he had robbed banks, he famously answered 'because that's where the money is'.²⁹¹ As banking products and services changed following the development of computer and telecommunication technology, Krebs, an information security expert, remakes the Sutton tale as follows: 'I'm quite certain that if the infamous Willie Sutton had his heyday in the present culture, Sutton's fabled answer to the question of why he robbed online banks would have been, "Because that's where the *easy* money is"'.²⁹²

Nowadays, payment cards have become an indispensable part of modern life and have spoiled their users with the broad range of services and capabilities that are used to support e-commerce and meet the need to have a fast and convenient way of payment.

²⁸⁶ FFIEC, 'Retail Payment Systems', above n 180, 28–9. See also Maxwell J Fry et al, *Payment Systems in Global Perspective* (Routledge, 2009) 5; BCBS, 'Risk Management Principles for Electronic Banking', above n 280, 11. See also CPSS, *Clearing and Settlement Arrangements for Retail Payments in Selected Countries*, above n 245, 10–11. As the BCBS asserts in its report, basically legal risk can occur if a party or the parties involved in the payment system do not abide by or conform with laws, rules, regulation, or prescribed practices. The FFIEC added that legal risk can arise if financial institutions fail to comply with 'the bylaws and contractual agreements established with the bankcard associations, clearinghouses, and other counter-parties with which it participates in processing, clearing, and settling retail payment transactions' or with 'existing consumer protection statutes, regulations, and case law governing retail payment transactions'. On the other hand, legal risk can also occur where the legal rights and obligations of the parties involved in e-banking transactions are not well established (either in the form of laws or agreement), or are obscure and/or uncertain.

²⁸⁷ Marinela Vrîncianu and Liana Anica Popa, 'Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests' (2010) *The AMFITEATRU Economic Journal* 388, 389. See also BCBS, 'Risk Management for Electronic Banking and Electronic Money Activities', above n 3, 5–8; FFIEC, 'Retail Payment Systems', above n 180, 27. According to BCBS, reputation risk is 'the risk of significant negative public that results in a critical loss of funding or customers.'

²⁸⁸ Kondabagil, above n 194, 15, 70.

²⁸⁹ Braun et al, above n 279, 140.

²⁹⁰ For brief information about Willie Sutton, see above n 1 and accompanying text.

²⁹¹ R Narasimhan, *Frauds in Banks* (ICFAI University Press, 2005) 7.

²⁹² Krebs, 'Cyber Crooks...', above n 2.

Unfortunately, payment cards like other type of payment instruments, are susceptible to fraud.²⁹³

A payment card itself as a means for authentication and authorisation of payment and held by the consumer is vulnerable to cardholder abuse or attack from external parties (such as those who use skimming, card trapping, and/or social engineering to access the card) as well as to the risk of simply being lost by the cardholder or stolen from them.²⁹⁴

Financial crime and fraud have occurred since the inception of trade.²⁹⁵ Gates and Jacob defined payment fraud broadly as ‘any activity that uses information from any type of payments transaction for unlawful gain. Such fraud can be perpetrated on any type of payments device, including credit and debit cards, cash, checks, online or mobile payments, and automated clearing house (ACH) transactions’.²⁹⁶

Pertaining to payment cards, Saville and Loomis noted that since the dawn of the use of credit and ATM/debit cards, the payment card industry has been subjected to fraud losses.²⁹⁷ All organisations regardless of their type and size are affected by the global problem of fraud.²⁹⁸ In spite of being one of the most accepted means of payment, the modern payment card has also been haunted in a manner similar to conventional fraud that commonly attacks cash payment, namely through the use of counterfeit or lost or stolen documentation (in this instance payment cards and PIN rather than cheque book and signature, and electronic theft rather than an armed robbery).²⁹⁹

²⁹³ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 101. See also Francis J Facciolo, ‘Unauthorized Payment Transactions and Who Should Bear the Losses’ (2009) 83(2) *Chicago-Kent Law Review* 605, 618–19.

²⁹⁴ Explanation regarding type and method of fraud on payment card will be discussed further in Chapter IV.

²⁹⁵ Jack Dorminey et al, ‘The Evolution of Fraud Theory’ (2012) 27 *Issues in Accounting Education* 555, 556.

²⁹⁶ Gates and Jacob, above n 258, 7.

²⁹⁷ See Julie Saville and Nancy Loomis, ‘Why Wait for EMV to Solve Your Fraud Problems? One-Time Use Card Numbers Can Reduce Debit Fraud Now’ (First Data Corporation, 2010) <<http://www.firstdata.com/downloads/thought-leadership/one-time-card-star-cert-wp.pdf>>, 4. See also Smart Card Alliance, ‘Fraud in the US Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud’ (2009) <http://www.smartcardalliance.org/resources/lib/Fraud_EMV_Contactless_20091007.pdf>, 5; Jan Devos and Igor Pipan, ‘The Role of IT/IS in Combating Fraud in the Payment Card Industry’ (2009) 14(3) *Journal of Internet Banking and Commerce* 1.

²⁹⁸ Hernan Murdock, ‘The Three Dimensions of Fraud’ (2008) 65 *The Internal Auditor* 81, 81.

²⁹⁹ M Krivko, ‘A Hybrid Model for Plastic Card Fraud Detection Systems’ (2010) 37(8) *Expert Systems with Applications* 6070, 6070.

There are many different definitions of payment fraud. In her 2010 article, Krivko defined plastic card fraud as ‘an unauthorized account activity committed by means of the debit/credit facilities of a legitimate account’.³⁰⁰ Sullivan asserts that ‘payment fraud occurs when someone gains financial or material advantage by using a payment instrument or information from a payment instrument, to complete a transaction that is not authorized by the legitimate account holder’.³⁰¹ Meanwhile, Mohamad canvasses plastic cards as fraud targets in payment card transactions. In this case, fraudsters using ‘plastic payment cards, such as ATM, debit, credit or store cards to take money without permission or prior to knowledge from a bank, building society or credit card account (or to charge money to credit/debit cards)’.³⁰² He further argues that the illegal gaining and/or use of payment card data and the PIN is the primary cause of payment/plastic card fraud.³⁰³ In addition, the lack of an account holder’s authorisation is the most important distinctive feature of payment card fraud.

Card issuing companies, merchants and customers worldwide have experienced great losses and inconvenience caused by plastic card fraud. The increasing volume of payment traffic, the advancement and expansion of modern technology, and the evolution of fraudulent tactics have increased plastic card fraud development.³⁰⁴ The payment system industry and regulators are keen to reduce and contain fraud incidents so that a robust, efficient and trusted payment system can be maintained.

According to the CPSS, risks such as fraud, operational and other risks ‘are generally addressed through technical features of various payment instruments and system control’.³⁰⁵ Roberds argues that it is possible with the use of technical feature or technology to eradicate fraud in electronic payments, as confirmed by the experience where costly security measures are used in wholesale funds transfer systems. However, this approach could not be applied to retail payment systems, since it would be too costly for banks and consumers alike, prolong consumers transactions (time

³⁰⁰ Ibid.

³⁰¹ Sullivan, *The Changing Nature of US Card Payment Fraud*, above n 262, 102–104.

³⁰² Hanna Mohamad, ‘Background Paper: Plastic Card Fraud’ (NSW Government, 2011) 5.

³⁰³ Ibid.

³⁰⁴ Krivko, above n 299, 6070.

³⁰⁵ CPSS, *Clearing and Settlement Arrangements for Retail Payments in Selected Countries*, above n 245, 1.

consuming), and is not appropriate for the retail payment system which is mostly used for high volumes of low value transfers.³⁰⁶

3.3.1. Why Are Payment Cards Always Vulnerable to Fraud?

Since its inception, the payment card industry has been targeted by fraudsters as an object for their activities.³⁰⁷ Unlike wholesale payment systems, a retail payment system (such as in a payment card system) is located in a more open environment, with relatively less comprehensive security features, and provides direct access to its end-users through its consumer activated terminals or electronic agents (such as ATMs and EFTPOS terminals). As a consequence, the payment card system is more exposed to fraud risk.

Pertaining to this, the Smart Card Alliance argues that ‘payments networks are vulnerable to fraud at any point in a payments chain, and fraudsters often attempt to exploit the weakest link in that chain’.³⁰⁸ Due to this fact, it is worth knowing what factors contribute to the proliferation of fraud in the payment card system (as shown below).

3.3.1.1. The Trade-off between Cost, Security and Consumer Convenience

Payment card systems require relatively huge investment to establish a viable electronic payment system. Most of the funds are spent on providing communications and computing facilities to optimise efficiency and convenience in consumer and merchant card transactions, and also to reduce fraud.³⁰⁹ In order to reduce fraud risk that always haunts payment card transactions, the creation and maintenance of a payment card system entails the introduction of costly infrastructure for consumer identification, authentication and authorisation.³¹⁰

In the development of an electronic banking system, banks always have concerns regarding processing costs and security. Commercial banks typically are very susceptible to the need for profitability in their payment products and services.³¹¹ The cost-effectiveness and technical efficiency of the electronic payment system cannot be

³⁰⁶ Roberds, above n 265, 43.

³⁰⁷ Smart Card Alliance, ‘Fraud in the US Payments Industry’, above n 297, 5.

³⁰⁸ Gates and Jacob, above n 258, 8.

³⁰⁹ Hunt, above n 182, 84–5. See also OECD Competition Committee, above n 178, 27.

³¹⁰ OECD Competition Committee, above n 178, 27.

³¹¹ Rambure and Nacamuli, above n 32, 21.

separated from the choice by the financial institution's management of payment system design and its associated risks.³¹² For the providers of the systems, technical or productive efficiency of the system refers to the ability to deliver a certain amount and quality of payment products and services at the minimum possible cost.³¹³ Banks are always eager to press processing costs of generic payment services to the lowest level so as to dedicate funds and other resources to value-added services, customer relations and profit.³¹⁴

Generally, banks are quite satisfied with the status quo because it serves banks relatively well, without any further investment involved and typically, consumers have no choice other than to use the offered services.³¹⁵

As Roberds argues,³¹⁶ from a technical and information security viewpoint, it is indeed possible to eradicate fraud in electronic payments by using state-of-the art encryption, private networks, public key infrastructure for authentication, smart cards (cards based on chips) and so on. However, some choices that are used in the wholesale payments system where the transactions normally involve relatively large amounts of money and greater transaction costs probably will not be appropriate for retail payment systems such as the payment card system.

If extensive safety features were applied in retail payment systems, this approach would be deemed very good from a fraud containment point of view. However, banks would have to allocate a high level of resources to achieve such a goal in this manner, and that would lessen the benefit to the bank in terms of profitability. Consumers might also find it difficult, complex, slow (as result of more complex authentication procedures) and too costly to use in their payment transactions, and that in turn could hinder its use and further development.³¹⁷ Conversely, a reduction in allocation of payment resources beyond a certain point in order to lower the cost of transactions may result in less

³¹² Summers, 'The Payment System in a Market Economy', above n 253, 4.

³¹³ CPSS, 'Clearing and Settlement Arrangements for Retail Payments in Selected Countries', above n 245, 13–15.

³¹⁴ Rambure and Nacamuli, above n 32, 24.

³¹⁵ Harry Leinonen, 'The Changing Retail Payments Landscape: An Overview' in *The Changing Retail Payments Landscape: What Role for Central Banks?* (Federal Reserve Bank of Kansas City, 2009) 25–6.

³¹⁶ Roberds, above n 265, 43.

³¹⁷ Committee on Payment and Settlement Systems (CPSS), 'Core Principles for Systemically Important Payment Systems' (Bank for International Settlements, 2001) 4.

accurate services and increase the possibility that risks will rise and feared frauds and other crimes occur.³¹⁸

The inter-connection with other bank and/or switching institution systems both in domestic and international networks also complicates the matter. Unlike network schemes such as Visa and MasterCard that have agreements, rules and administrative powers to enforce some level of technical standards among their members,³¹⁹ switching companies that connect ATMs/EFTPOS machines owned by proprietary banks are generally lax in terms of these capabilities. As Sullivan argues, security in network connections is not optimal because ‘one member of the network has no incentive to take account of the external benefits or costs of others’.³²⁰ As a result, this often makes one or more members reluctant to enhance their security features, leaving these members’ e-banking devices as the weakest link in the entire network.³²¹

In most cases, the need for higher security for e-banking products will always have a trade-off in terms of investment required and consumer convenience.³²² Besides that, the desire to improve security for one bank is sometimes difficult to achieve because of legacy infrastructure that is not easy to enhance. If it is able to be enhanced, it requires relatively large investment, administrative difficulties, and/or is time consuming to change.³²³

³¹⁸ CPSS, ‘Clearing and Settlement Arrangements for Retail Payments in Selected Countries’, above n 245, 13–15.

³¹⁹ For instance, in EMV shifting liability rules, every member that not comply with EMV standards after certain date will bear the fraud damages.

³²⁰ ‘Efforts to improve card payment security by one member of the network may benefit other members, just as one member’s security breach may harm others’. See Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 118–19.

³²¹ Ibid.

³²² See Gifford, above n 17, 11–12. See also CPSS, ‘Clearing and Settlement Arrangements for Retail Payments in Selected Countries’, above n 245, 13–15. Beside the trade-off between cost and security, there are also trade-offs between security and technological innovation, security and privacy, security and usability. See Glaessner, Kellermann, McNevin, above n 51, 21–2; Stallings and Brown, above n 221, 34.

³²³ Banks in the USA were reluctant to embrace EMV despite pressure from the card networks, mainly due to the massive cost of upgrading the national EFTPOS infrastructure, and the fact that fraud at ATM/EFTPOS is not at a high enough level to justify the massive investment required in hardware, training of retailers and re-education of customers. See Nigel Walsh, ‘ATM Fraud Prompts Card Rethink?’ (2005) 17(2) *Card Technology Today* 10, 10. See also Meyer and Matyas, above n 72, 449. However, after massive security breaches at Target and Neiman Marcus, a deadline for implementation was set for October 2015: Olga Kharif and Bianca Vázquez Toness, *Why US Retailers Are Still Vulnerable to Card Fraud* Bloomberg Business, 10 April 2014 <<http://www.bloomberg.com/bw/articles/2014-04-10/u-dot-s-dot-retailers-behind-schedule-for-card-payment-system-upgrade>>.

Hence, cost constraints will always affect payment system design, which will have consequences for the payments system's viability and safety.³²⁴ In regard to this, Claessens et al argue that there should be a proper balance between security and cost.³²⁵ Further, they argue that in reality, 'banks try to have a minimal level of security alleviating most of the risks, with maximum level of convenience'.³²⁶ Therefore, banks in a retail payments system typically only try to minimise fraud to an acceptable level, since it is impossible to make the retail payments system infallible in terms of fraud.³²⁷

Nonetheless, often this paradigm is transformed inadequately by management into bank security features.³²⁸ Gates and Jacob contend that as a consequence of those cost constraints mentioned above, the payment industry traditionally has been slow to update technology ('while fraudsters have quickly adapted to the new channels available').³²⁹ Hence, in practice reports regarding fraud in retail payment systems and its ramifications continue to occur and will always do so. Similar problems have actually also occurred in Indonesia, since Indonesia's retail payment system basically have no policy and development concept regarding the retail payment system that is any different to those of other countries (as earlier explained).

3.3.1.2. Incentives for Payment Card Fraud

Vulnerable environments will attract potential perpetrators to commit crime, as they will see these environments as potentially rewarding situations with little apparent risk

³²⁴ CPSS, 'Core Principles for Systemically Important Payment Systems', above n 317, 4.

³²⁵ Claessens et al, above n 196, 256; See also Glaessner, Kellermann and McNevin, above n 51, 2, 21–2; Richard A Epstein and Thomas P Brown, 'Cybersecurity in the Payment Card Industry' (2008) 75 *University of Chicago Law Review* 203, 211; Rambure and Nacamuli, above n 32, 54.

³²⁶ Claessens et al, above n 196, 256. Instances of this can be seen from Visa/MasterCard business policy. In order to increase consumer convenience, payment transaction speed and loyalty, Visa and MasterCard launched a 'zero liabilities' approach for consumers over fraud on their accounts, and low value card payment below certain limit without a consumer's signature (skips authentication process). See Visa, *Zero Liability* (2011)

<http://usa.visa.com/personal/security/visa_security_program/zero_liability.html?it%BCcj/personal/security/visa_security_program/index.htmljZero%20Liability*>; and MasterCard, above n 42.

³²⁷ See Bruce J Summers, 'Fraud Containment' (2009) 33(1) *Economic Perspectives* 17, 18–19; Glaessner, Kellermann and McNevin, above n 51, 29; Greenstein and Feinman, above n 206, 252–3; Robin Adams, 'Prevent, Protect, Pursue - a Paradigm for Fighting Fraud' (2010) *Computer Fraud & Security* 5, 5.

³²⁸ Mike Bond and Piotr Zielinski, 'Decimalisation Table Attacks for PIN Cracking' (University of Cambridge computer Laboratory Technical Report TR-560, 2003) <<http://www.cl.cam.ac.uk/~mkb23/research/PIN-Cracking.pdf>>.

³²⁹ Gates and Jacob, above n 258, 9. See also Rambure and Nacamuli, above n 32, 24; Gleason and Heimann, above n 87, 164. According to Gleason and Heimann, one of the reasons why banks are very slow to adopt new technology is because banks are always concerned with merchants' reluctance to accept additional cost in regard of enhancement if terminal security ('leaving banks/merchants [to] operate [with a] relatively low level of technology in the current system').

of being caught or punished.³³⁰ There are also security issues regarding the proliferation nonbank and third party service providers in the payment system industry.³³¹

Generally, a payment card system is a massive and complex system and involves many linked counterparts. Hence, any immediate upgrade of its security features could be a very difficult task. Banks' standardised infrastructure, their interoperability connection with other institutions, and cost constraints, are several factors that hinder banks from frequently and immediately upgrading their payment card systems, and are factors why any requirement for immediate action is somewhat unrealistic. In contrast, criminals have little or no difficulty in employing the latest technology to defraud the system and commit identity theft/fraud.³³²

Despite banks continually enhancing their security features, fraudsters are constantly adapting and developing new ways to collect and use identity information, and bank account and credit card details.³³³ As Casey observes, 'A criminal *modus operandi* is comprised of learned behaviours that can evolve and develop over time. It can be refined, as an offender becomes more experienced, sophisticated, and confident' and ultimately perpetrate fraud on a bigger scale and one that is more destructive in its extent.³³⁴

Litan, an analyst specialising in fraud detection and prevention at Gartner Research, has formulated a theory on the proliferation of ATM/debit card fraud that has become a concern for banks all over the world. According to him, ATM/debit card fraud is facilitated by the different nature of ATM/debit card transactions compared to those of a credit card.³³⁵ Other than that, Iannacci and Morris note that it is now very easy for criminals to commit payment card fraud, since anyone can procure the same technology

³³⁰ Sridhar Ramamoorti, 'The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component into Fraud and Forensic Accounting Curricula' (2008) 23(4) *Issues in Accounting Education* 521, 3.

³³¹ Gates and Jacob, above n 258, 7.

³³² Meyer and Matyas, above n 72, 449.

³³³ Rambure and Nacamuli, above n 32, 64.

³³⁴ Eoghan Casey, *Digital Evidence and Computer Crime* (Academic Press, 2000) 27; see also Javelin Strategy & Research, '2010 LexisNexis True Cost of Fraud Study' (LexisNexis, 2010) 17.

³³⁵ ConsumerReports.org, above n 44. With credit card fraud, unless fraudsters purchased goods on-line via card not present transactions (CNP), there is always a risk of being caught if the fraudsters fail to 'perfect' the counterfeit credit card (card appearance and consistency between data inside magnetic stripe and data printed on the surface of the card) or the card has already been placed on the 'red flag list'. In contrast, in ATM/debit card fraud, fraudsters simply create counterfeit cards and then withdraw or transfer money from unattended ATM terminals without the risk being noticed by other people.

and equipment to make counterfeit documents, because the same technology and equipment are used to prepare/make documents for legitimate purposes.³³⁶ As stated in the UNCITRAL Model Law on Electronic Signatures, the original of a message is indistinguishable from a copy in an electronic environment. Hence, most probably unauthorised transactions conducted by fraudsters will be treated by the payment card system or its management as genuine or valid transactions. The potential for fraud is therefore substantial due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions.³³⁷

The proliferation of the means of information sharing, such as chat rooms on the Internet and other electronic forums, has also facilitated e-banking and greater organisation on the part of payment card fraudsters. In these forums, criminals can trade stolen card and bank account data, hacking tools and other services anonymously; hence there is minimum risk of being detected by law enforcement agencies.³³⁸ The Internet also enables fraudsters around the world to exchange information regarding successful fraudulent schemes, thus new fraud techniques can move quickly to various fraudsters globally.³³⁹ For instance, to cite Symantec, the price of stolen credit card information is between USD0.85 and USD30 per card number, while bank account information is available on the ‘underground’ Internet market at a cost of USD15 to USD850 per account number. Disturbingly, there are also other data available for sale such as full identities, email accounts and passwords.³⁴⁰

Given the multiplicity of types of online fraud/crime and their frequency and existing evidence, the UN attributed ongoing fraud development to a combination of technological advances, a lack of consumer and industry education, inadequacies in the

³³⁶ Iannacci and Morris, above n 20, 7. In credit card fraud, fraudsters normally charge merchandise to the card at a merchant and then sell it to get the money. By contrast, fraudsters with access to a bank consumer’s ATM/debit card, once they have bank consumer data and PIN, then they can simply withdraw money from an ATM without the worry of finding a market and buyer for their illicitly obtained merchandise as would be the case in credit card fraud.

³³⁷ United Nations Commission on International Trade Law (UNCITRAL), ‘UNCITRAL Model Law on Electronic Signatures with Guide to Enactment’ (United Nations 2001) 20.

³³⁸ Ross Anderson et al, ‘Security Economics and the Internal Market’ (European Network and Information Security Agency, 2008) 9–10. See also Gifford, above n 17, 27–8; Steve Malphrus, ‘Perspectives on Retail Payments Fraud’ (2009) XXXIII *Economic Perspectives* 31, 31; Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 103. Sullivan asserts that some criminals who are involved in transnational fraud specialise in gathering payment related data by writing malicious software or creating fake websites, and trade on underground online markets to buy and sell services that aid in stealing data or perpetrating payment fraud.

³³⁹ Malphrus, above n 338, 31.

³⁴⁰ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 102–104.

relevant legislation and fear of adverse publicity (due to its economic implications).³⁴¹ This, together with a lack of resources, or the willingness to allocate resources to the task, appears to have impeded an adequate timely response and perversely acted as an incentive for fraud.

3.3.1.3. The ‘Balloon Effect’ in Payment Card Fraud

The regulator and the payment system industry go ‘hand in hand’ in combating fraud for the creation of a secure and efficient payment system. Regulations and various fraud prevention and detection tools continue to be implemented in the retail payment system in order to maintain public confidence and reduce fraud.

However, fraudsters have quickly adapted to the new channels available, and there is also a tendency to displace effort to the most vulnerable operators. As the Smart Card Alliance asserts:

Criminals are known to exploit the weakest link, moving from locations where stronger authentication is present to those where it is not, or from financial institutions and merchants who have more sophisticated fraud detection and prevention tools to those with less.³⁴²

Greene refers to this phenomenon as the ‘balloon effect’, that is, squeeze fraudsters in one area of operation and they move to another, or in terms of where ‘fraudsters are moving from one channel and technology to the next’. Thus, if banks have applied one particular fraud prevention method in their payment system services that begins to decrease the success rate of a particular fraud approach, fraudsters then naturally will divert their activities to focus on another part of payment system that is still vulnerable to exploitation.³⁴³

³⁴¹ United Nations, ‘International Review of Criminal Policy’, above n 267, 347.

³⁴² Smart Card Alliance, ‘Fraud in the US Payments Industry’, above n 297, 8. See also Krivko, above n 299, 6070.

³⁴³ Mark N Greene, ‘Divided We Fall: Fighting Payments Fraud Together’ (2009) 33(1) *Economic Perspectives* 37, 38. See also Gates and Jacob, above n 258, 9; Mercator Advisory Group, *Credit Card Fraud Update: Silos Versus The Balloon Effect* (2007) <http://www.mercatoradvisorygroup.com/index.php?doc=credit&action=view_item&id=171&catid=3>; Michael Levi and Jim Handley, *Criminal Justice and the Future of Payment Card Fraud* (Institute for Public Policy Research, 2002) However, it is also argued that fraudsters may sometimes stick to the banks that have already improved their system security, assuming that there is always a vulnerable point of the systems that can be infiltrated either by using new fraud methods or by modifying an old fraud method. Each bank has a different number of consumers. Generally fraudsters will attack banks with many consumers rather than those with fewer consumers, simply because more potential victims equal more profit.

As a payment card system consists of a wide range of activities and involves many institutions in its transactions, the weakest link can be anything along the pathway of card transactions. Among other things, this can be the consumers themselves, ATM/EFTPOS terminals, network connections, bank computers, switching company computers, as well as employees of merchants, switching companies, and banks.

The most obvious example of the balloon effect in payment card fraud is related to the implementation of the global EMV standard to the credit/debit card issued by banks that carry a scheme network brand such as Visa and MasterCard. The EMV standard increases security of payment cards by utilising chip technology for storing and executing payment card transactions.³⁴⁴

However, since all EMV standard cards still carry magnetic stripe technology to enable them to be used in countries where ATMs or EFTPOS terminals still are not EMV compliant (a 'fallback' policy), then the EMV card as a whole is not infallible from identity theft attack targeting consumer data inside the magnetic stripe.³⁴⁵ Today, many experts and institutions in payment card industries concur about the vulnerability of magnetic stripe technology in payment cards.³⁴⁶

As a result, the balloon effect in payments card fraud works in at least two directions regarding global implementation of EMV standards. First of all, criminals tend to attack the countries where their payment card technology still relies on the magnetic stripe alone. Typically, all ATM and EFTPOS terminals in these countries are only able to read magnetic stripe cards.³⁴⁷ Hence fraudsters can still easily target domestic banks'

³⁴⁴ See European Central Bank, 'Report on Card Fraud' (2012) 10–11. In the report, data for 2010 showed that there is an 11% decrease in counterfeit fraud. The use of counterfeit cards appears to have shifted from ATMs to POS terminals, due faster implementation of the EMV standard at ATMs.

³⁴⁵ Studies have shown that the EMV chip + PIN cards in a specific region or country vastly reduce domestic card present (CP) fraud, but there is a corresponding increase in fraud linked to stolen account information used outside that domestic market. However, the UK Payments Administration (formerly APACS) says the US reluctance to adopt EMV is impacting the UK market. According to APACS, domestic card fraud in the UK dropped 32% in 2007, while counterfeit card fraud increased by 46% the same year. APACS claimed the increase was 'due to fraudsters copying U.K. cards and using these stolen cards in countries which do not yet have chip + PIN'. See Saville and Loomis, above n 297, 2. See also Saar Drimer, Steven J Murdoch and Ross Anderson, 'Thinking inside the Box: System-Level Failures of Tamper Proofing' (Paper presented at the IEEE Symposium on Security and Privacy, Oakland, CA, 2008) <http://ieeexplore.ieee.org.ezproxy.uow.edu.au/xpls/abs_all.jsp?arnumber=4531159&tag=1>, 282.

³⁴⁶ Smart Card Alliance, 'Fraud in the US Payments Industry', above n 297, 18; Sullivan, 'The Changing Nature of US Card Payment Fraud', above n 262, 115; Financial Fraud Action UK, *Fraud The Fact 2012: The Definitive Overview of Payment Industry Fraud and Measures to Prevent It* (2012) <<http://www.financialfraudaction.org.uk/downloads.asp?genre=facts%20and%20figures>>

³⁴⁷ Sullivan, 'The Changing Nature of US Card Payment Fraud', above n 262, 115.

payment cards and/or others' payment cards issued by international financial organisations that conduct local transactions in these countries. The United States³⁴⁸ and Indonesia are notorious examples of this balloon effect in payment card fraud, since US payment cards and Indonesia's ATM/debit cards have until the present day continued to rely on magnetic stripe technology.

Secondly, criminals can still attack consumer data found inside the magnetic stripe in the countries that have implemented EMV standards, but then use it to withdraw money or conduct others transactions in the non-EMV standard countries (in cross-border fraud). An example of this concerns cross-border fraud that attacked EMV-compliant European countries. According to EAST's data, while overall ATM fraud losses dropped 14 per cent across 22 European states, 82 per cent of the losses sustained actually came from outside European borders where the magnetic stripe is still widely utilised.³⁴⁹

Evidence of these matters can be seen in the effect of EMV implementation in a number of European countries, where the incidence of skimming attacks is decreasing but the number of cash trapping attacks is on the rise.³⁵⁰ From a study undertaken by Diebold Incorporated, the increasing number of cash trapping frauds in Europe is quite staggering. During the first half of 2011, there were 6,756 incidents of cash trapping reported in Europe, up from just 150 incidents for the same time in 2010. Cash trapping resulted in reported losses of EUR495,782 for the period from January to June 2011.³⁵¹

Similar evidence of these phenomena has also been found in Indonesia. Following a deluge of ATM fraud using skimmers that rocked the country in the 2010, Bank Indonesia (the central bank) encouraged banks to toughen their security features in order to combat skimming attack. As result, banks have utilised various anti skimmer devices

³⁴⁸ See Smart Card Alliance, 'Fraud in the US Payments Industry', above n 297, 18; Drimer, Murdoch and Anderson, 'Thinking inside the Box,' above n 345, 281; Walsh, above n 323, 10; Diebold Incorporated, 'White Paper: ATM Fraud and Security' (2002) 2; Davis, Stroud and Paese, above n 217, 3; Sullivan, 'The Changing Nature of US Card Payment Fraud', above n 262, 115;

³⁴⁹ Tracy Kitten, *ATM Skimming Threats Evolve* (5 May 2011) Bank Info Security <http://www.bankinfosecurity.com/articles.php?art_id=3612&rf=2011-05-06-eb>.

³⁵⁰ In this attack method, fraudsters attempt to gain access to cash by attaching a fraudulent device to the cash-dispensing slot, causing notes to be stuck inside the ATM. The perpetrator then returns later to remove the cash from inside the dispenser. See Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 2.

³⁵¹ Ibid.

and ensured more diligent supervision of ATM booths.³⁵² Fraudsters consequently have difficulty in attaching their skimming devices without having first customised them. Thus, while the incidence of skimming fraud has tended to reduce, the incidence of card trapping has tended to rise, both in numbers and in the variation of the fraud devices used.³⁵³

Fraud tools are also affected by this balloon effect. Before banks enhanced their ATM security with anti ATM skimmer technologies,³⁵⁴ card-trapping fraudsters typically used fraud tools such as ribbon or camera film negative film and attached these with glue to the ATM mouth for trapping consumer's card. However, since banks have outfitted anti-skimming devices to the front of ATM card reader slot, which also makes traditional card-trapping methods such as the 'Lebanese Loop' difficult to apply, many fraudsters have utilised a matchstick to trap the card instead (which was unaffected by the instalment of anti-skimmer devices) and achieved a high rate of success.³⁵⁵

³⁵² Some improvements in the ATM security include among other things: anti-skimmer devices, jitter, ATM slot sensor, and so on.

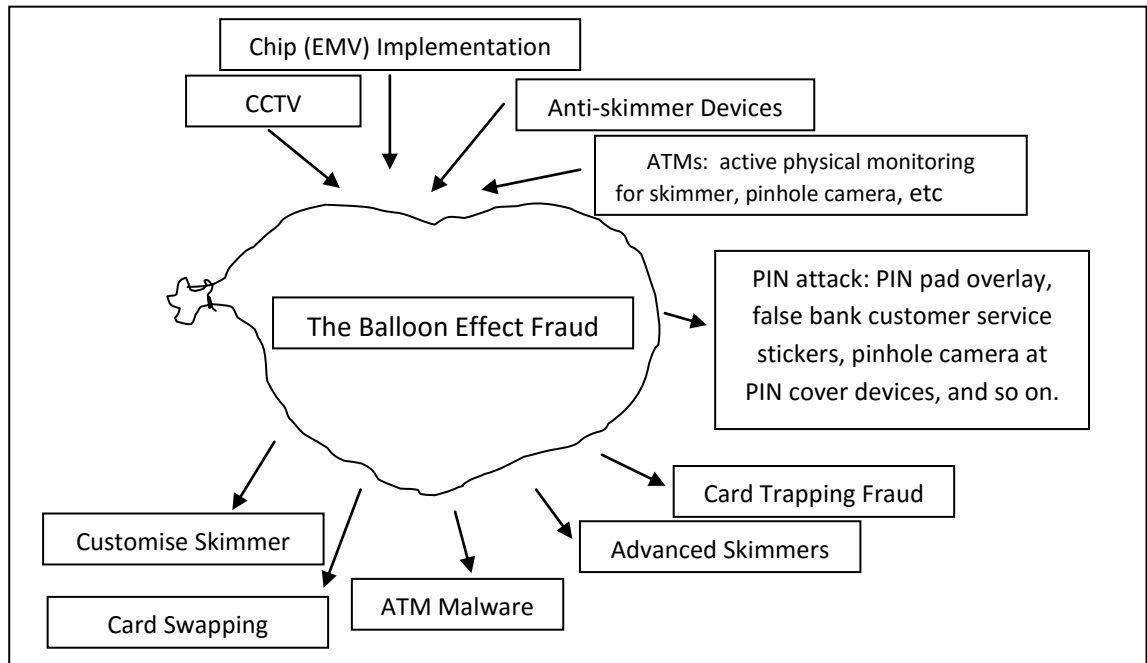
³⁵³ Stefanus Arief Setiaji, *Kejahatan Bank: Pembobolan Kartu ATM Naik Pada 2012* [Banking Fraud: ATM Card Theft Increased in 2012] (2013) Bisnis.com <<http://en.bisnis.com/articles/kejahatan-bank-pembobolan-kartu-atm-naik-pada-2012>>. See also Skynet Media Group, *Teknik & Modus Card Trapping* [Technique and Modus of Card Trapping] (2011) Mafia Kartu Kredit <<http://www.mafiakartukredit.com/2012/03/teknik-modus-card-trapping.html>>; 'Kejahatan Perbankan Kembali ke Tradisional' [Banking Fraud Returns to Traditional Way], *Kompas* (online), 26 September 2011

<<http://nasional.kompas.com/read/2011/09/26/07422898/Kejahatan.Perbankan.Kembali.ke.Tradisional>>.

³⁵⁴ See Brian Krebs, *Green Skimmers Skimming Green* (2011) <<http://krebsonsecurity.com/2011/03/green-skimmers-skimming-green/>>. In many cases, the anti-skimming tools take the shape of green or blue semi-transparent plastic casings that protrude from the card acceptance slot to prevent would-be thieves from easily attaching skimmers. In Indonesia, this anti-skimming tools are called: 'cocor bebek' or 'duck snout'.

³⁵⁵ *Kejahatan Card Trapping Memacetkan Mesin ATM Untuk Menguras Uang ATM* (Warning) [Card Trapping Crime Jammed ATM Machine to Drain ATM Cash (Warning)] (15 October 2012) Direktorat Reserse Kriminal Umum, Polda Metropolitan Jakarta Raya, <<http://reskrim.metro.polri.go.id/read/article/8203/19/Kejahatan-Card-Trapping-Memacetkan-Mesin-ATM-Untuk-Menguras-Uang-ATM-Warning>>.

Figure 3: The Balloon Effect in Payment Card Fraud



3.3.2. Inherent and Known Vulnerabilities in the Payment Card System

In information security, infrastructure and networks are generally huge systems that are not easy to manage and control due to their size. According to Pipkin, ‘upgrades are very expensive, so old systems stay in operation long after the security flaws are known’. Furthermore, he contends that misinterpretation of security policy and/or its implementation, and/or failure to address new issues created by new technology or new business processes, have become a source of security vulnerabilities and created many points of compromise.³⁵⁶

Payment cards are susceptible and vulnerable to fraud. Sullivan argues that ‘vulnerabilities exist in the card payment approval process, however, that enable criminals to make fraudulent card payments. These vulnerabilities are related to an information-intensive payment approval process’.³⁵⁷ Meyer and Matyas even suggest that, ‘it appears impossible to develop any type of payment system which completely eliminates all fraud risks’.³⁵⁸

³⁵⁶ Pipkin, above n 226, 69.

³⁵⁷ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 102–3.

³⁵⁸ Meyer and Matyas, above n 72, 4489.

All in all, the FFIEC asserts that vulnerabilities can be depicted as ‘weaknesses in a system, or control gaps that, if exploited, could result in the unauthorized disclosure, misuse, alteration, destruction of information or information systems’.³⁵⁹ However, Pipkin has argued that vulnerabilities are difficult to foresee and most of them are not exposed until they are misused.³⁶⁰ Furthermore, the FFIEC observes that there are commonly two types of vulnerabilities, ‘known’ and ‘expected’.³⁶¹

Regarding known vulnerabilities, Pipkin argues that these ‘account for the largest part of successful attack’. He further asserts that known vulnerabilities must be addressed, since by the time knowledge of a vulnerability has become widespread, malicious programs that could exploit that vulnerability are generally available for distribution and integration into larger, user-friendly toolkits. Hence, any fraudsters — even those without special skills — still have the ability to exploit all known vulnerabilities.³⁶²

It is argued that most payment card fraud methods such as skimming, card trapping, shoulder surfing, malware and so on, are known to exploit vulnerabilities in bank systems. Most of all, those who deal with identity theft methods have known that such methods have been around for years. Banks can be assumed to have known about all these identity theft methods for some time from the many avenues for information exchange, such as at banking forums and seminars, or from their own daily experiences.

Even though banks always claim that the authentication process between client (consumer-activated terminal) and the authenticated banks (host) is secure, Claessens contends that such claims are mostly not true in reality. According to him, client platforms are generally very vulnerable. Malicious programs, such as viruses, Trojan horses, worms, and other malicious programs can tamper with the installed root

³⁵⁹ FFIEC, ‘Information Security’, above n 202, 12–13.

Known vulnerabilities are discovered by testing or other reviews of the environment, knowledge of policy weaknesses, knowledge of inadequate implementations, and knowledge of personnel issues... Expected vulnerabilities to consider are those that can reasonably be anticipated to arise in the future. Examples may include unpatched software, new and unique attack methodologies that bypass current controls, employee and contractor failures to perform security duties satisfactorily, personnel turnover ..., new technology introduced with security flaws, and failure to comply with policies and procedures.

See also Stallings and Brown, above n 221, 16.

³⁶⁰ Pipkin, above n 226, 35.

³⁶¹ FFIEC, ‘Information Security’, above n n 202, 12–13. See also Pipkin, above n 226, 69.

³⁶² Pipkin, above n 226, 69.

certificates, and among other things can intercept and steal communication information before it is 'securely' sent to the bank.³⁶³

Claeessens's assertion is apparently absolutely right in terms of the reality of e-banking practices in Indonesia. Banks tend to declare repeatedly to the public that their systems are always secure and 'infallible'. For instance, even in the massive ATM cards skimming fraud that affected more than ten banks in Indonesia in early 2010, there was one affected bank that had proclaimed (and was quoted by the news media) that their bank was secure and had not been affected by the skimming fraud scheme that was sweeping the country.³⁶⁴ On the contrary, according to Bank Indonesia and Indonesia's Police report,³⁶⁵ the bank actually had also suffered from the skimming fraud. This misleading information also tends to be unfair to other banks that are fraud victims and that suffer damage to their reputation. It could also jeopardise the rights of consumer victims as this misinformation could mislead judgment for fraud liability disputes.³⁶⁶

³⁶³ Claessens et al, above n 196, 261–2.

³⁶⁴ Lukman Hakim Zuhdi, 'Pembobolan ATM, Salah Siapa? [ATM Theft, Who is at Fault?]', *Tabloid INDONESIA MONITOR* 27 January - 2 February 2010; see also Indra Subagja, *Bank Mandiri: 4 Nasabah yang Laporkan ke Polda Bukan Korban Skimming* [Mandiri Bank: 4 Consumers That Report to Police Station were not Skimming Victim] (25 January 2010) Detik.com <<http://news.detik.com/read/2010/01/25/183554/1285861/10/bank-mandiri-4-nasabah-yang-lapor-ke-polda-bukan-korban-skimming>>; Indah Septiyaning, *Dilengkapi Anti Skimmer, ATM Bank Mandiri Aman* [Equipped with Anti Skimmer, Mandiri Bank is Secure] (26 January 2010) Boyolalipos.com <<http://www.boyolalipos.com/2010/dilengkapi-anti-skimmer-atm-bank-mandiri-aman-12955>>. This dishonest information from the bank apparently aimed to avoid reputation risks and keep its consumers feeling secure, and loyal, and probably also to attract more consumers by depicting that bank's information security quality as superior to that of its competitors. However, such information tends to confuse and mislead stakeholders, especially the payment system authority and the bank's consumers and other banks that have fallen prey to skimming fraud.

³⁶⁵ *Bank Diminta Perbaiki Sistem Pengamanan* [Banks Asked to Improve Its Security System] (23 January 2010) Hukumonline.com <<http://www.hukumonline.com/berita/baca/lt4b5a35f0f1afb/bank-diminta-perbaiki-sistem-pengamanan>>. See also *Pembobolan ATM: BI Instruksikan Bank Evaluasi Sistem IT* [ATM Theft: BI Instructs Banks to Evaluate Their IT System] (2010) Indosiar.com <http://www.indosiar.com/fokus/bi-instruksikan-bank-evaluasi-sistem-it_84020.html>; Herdaru Purnomo, *BI: Pengguna ATM Tak Perlu Panik, Kerugian Ditanggung Bank* [BI: ATM Users do not Need to Panic, Banks Bear the Loss] (20 January 2010) Detik.com <<http://finance.detik.com/read/2010/01/20/181324/1282733/5/>>; Unpublished Bank Indonesia Internal Note from Payment System Oversight Team to Director of Payment System and Accounting Directorate Concerning *Kasus Pembobolan Dana Nasabah Melalui Mesin ATM di Industri Kartu ATM* [Consumers' Fund Theft Cases Through ATM Machines in ATM Card Industry]. From the latter document, it was reported that there were 11 issuing banks that were affected by skimming fraud in Bali (these 11 banks reflect 13% of the total 84 issuing banks for ATM card in Indonesia). ATMs owned by these 11 banks account for approximately 80% of the total ATMs machines in Indonesia.

³⁶⁶ See District Court of South Jakarta Verdict No 632/Pdt.G/2010/PN.Jkt.Sel dated 30 June 2011 (*Nasruddin v PT Bank Mandiri Tbk* (Card Trapping Case)). In this verdict, one of the reasons for the judges decision that in favor of defendant was the failure of the plaintiff to prove his allegation concerning numbers of complaints from bank's consumers regarding the 'fraudster's card trapping devices that had been present for quite some time' in the bank's ATMs. See the case description in Chapter Six / section 6.6.4.3.2.1.

It is argued that most payment system fraud in Indonesia can be depicted as exploiting known bank vulnerabilities. Banks generally have a fraud department or section that is responsible for fraud prevention and detection and the implementation of security features to circumvent fraud. They commonly update their identity theft and fraud information through several avenues. These include internal security audits, which may reveal several long existing key vulnerabilities.

According to one bank's internal audit review, consumers debit/credit card data for end-to-end internal card processing passed through the personal computers of several employees without encryption (even if some employees were able to access the data without any actual authorisation right to access the card data). There were also no controls or procedures for the management of data that was stored on the employees' PCs. To make things even worse, there was no audit trail in place regarding who had access to the data and for what purposes. Even more distressing, the vendor that maintained the card processing hardware/software could also access the data. Meanwhile, the bank's review of the bank's EFTPOS system revealed that consumer card data transactions which travel from an EFTPOS machine to the bank's host system were in the plain text form (unencrypted).

Similarly, in the switching or interoperability context where switching companies are involved in card transactions, every switching system activates their 'trace message' system and stores every consumer's card data that travels through their system (in the plain text format). By recording consumer card data, switching companies can easily resolve any disputes regarding consumer transactions that travel through their system. On the other hand, this practice also makes a switching company's data base server/computer a potential target for identity theft either from internal or external fraudsters.³⁶⁷

Avenues (other than internal audits) for banks to update their identity theft and fraud information also include bank information exchange forums, fraud conferences, or international organisations that focus on payment system fraud information (as banks normally are members or subscribers).

³⁶⁷ This example of a payment card vulnerability known to bank management is from the unpublished '2008 Debit/Credit Card Internal Audit Review Report' from a major bank in Indonesia.

Generally, all these vulnerabilities were not deliberately exposed by banks or even by the bank authority. To win consumer trust, banks commonly only picture their strengths and bury their weakness. Bank jargon such as ‘we use firewalls, encryption, anti skimmer, and so on’ always depict their security features information as ‘the best’. However, as to how good or how comprehensive all these features are or whether or not all of these features are ‘commercially reasonable’ to protect their system from identity fraud, it is difficult to gauge without having an acceptable benchmark as a standard, and without any professional and comprehensive ‘hands on’ audit. This unfortunate situation often leaves the consumer as the easiest and weakest target to be blamed both in technological and legal aspects if unauthorised ATM/debit card transactions do occur.

Hence, it is submitted that in fraud liability disputes between banks and consumers over unauthorised ATM/debit card transactions, the bank’s information security features and how they are implemented in practice become one of the important factors to be considered and assessed exhaustively as well as the consumer’s behaviour and a country’s liability regulations.

3.4. The Fraudsters

One of the most important factors in understanding fraud is related to the persons who perpetrate the fraud. In payment card fraud, anyone can commit the fraud. Payment card fraudsters typically are no different to most people in society, in terms of their demography and psychological characteristics.³⁶⁸ The perpetrators in payment cards fraud range from individual novices to major organised crime syndicate members.³⁶⁹ Cvrcek, Krhovjak and Matyas noted that the former class were largely comprised of an ‘individual or small group of loosely organised individuals that do not have any special hardware for card analysis, cloning, ...etc’; these were characteristically termed ‘opportunistic thieves’.³⁷⁰

In terms of the source of the threat, Adams argues that payment card fraudsters can come from external parties such as first-party, second party (‘friendly’ party), third-

³⁶⁸ W Steve Albrecht et al, *Fraud Examination* (South-Western, 2012) 33. See also Levi and Handley, above n 343. According to Levi and Handley, ‘those who successfully engage in plastic card fraud on any significant scale are generally bright, business actorial and innovative. They have demonstrated an ability to operate adaptively and respond to initiatives aimed at curtailing their activities.’: 23.

³⁶⁹ Albrecht et al, above n 368, 36.

³⁷⁰ Dan Cvrcek, Jan Krhovjak and Vashek Matyas, ‘PIN (and Chip) or Signature: Beating the Cheating?’ (Paper presented at the Security Protocols, Cambridge, UK, 2005) 69.

party, and be essentially opportunistic in nature, or be part of an organised group of criminals; or originate from insiders³⁷¹ or be an internal threat posed by persons such as a bank's own staff, such as dishonest bank employees at a call centre collecting password data for use by an accomplice.³⁷²

Iannacci and Morris stated that organised criminal groups have no concerns about borders in committing their crimes. Such groups of criminals travel from state to state and country to country looking for fraud prospects. As Iannacci and Morris observe, 'They do this in an often futile attempt to evade detection and/or prosecution'.³⁷³ The mobility of these international criminal organisations, also known as transnational criminal organisations, has become a major problem for law enforcement agencies at a local, national and international level.³⁷⁴

Nonetheless, Facciolo noted in his study that there has been a trend in identity theft where organised crime is more prevalent than individuals as the party responsible for unauthorised transactions in payment systems.³⁷⁵ A growing global economy and increasing interoperability between payment system infrastructures in different countries in systems such as the payment card system has provided opportunities for criminal behaviour and created a fertile environment for fraud that is more complex, organised and common than ever before, such as in cross-border fraud.³⁷⁶ More criminals engaged in card fraud now can be linked to serious organised crime, such as large scale organised theft, money laundering and tax evasion, and cybercrime and terrorism.³⁷⁷

³⁷¹ For instance, an insider such as an ATM technician or someone else with a key to the ATMs placed the malware on more than 20 ATMs in Russia and the Ukraine. See Kim Zetter, *New ATM Malware Captures PINs and Cash-Updated* (6 April 2009) [www.wired.com <http://www.wired.com/threatlevel/2009/06/new-atm-malware-captures-pins-and-cash>](http://www.wired.com/threatlevel/2009/06/new-atm-malware-captures-pins-and-cash).

³⁷² Adams, above n 327, 5. See Gates and Jacob, above n 258, 7. According to Gates and Jacob, 'payments fraud can be committed knowingly by a consumer (first-party fraud), or consumers can be victimized by fraudsters operating within financial institutions or as part of criminal enterprises (third-party fraud)'; bank employees with access to computer terminals could enter fraudulent instructions to transfer funds or alternatively change the software, leading to fraud. See also Arora, above n 197, 47–8; Anderson et al, above n 338, 9–10.

³⁷³ Iannacci and Morris, above n 20, 5

³⁷⁴ Ibid.

³⁷⁵ Facciolo, above n 293, 622.

³⁷⁶ Tedder, above n 44, 9.

³⁷⁷ Australian Crime Commission, *Card Fraud* (2011) [<http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/card-fraud>](http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/card-fraud). See also Mike Barwise and Daniel Bachfeld, *Attack of the Card Cloners* (2007) The H Security [<http://www.h-online.com/security/features/Manipulated-ATMs-746193.html>](http://www.h-online.com/security/features/Manipulated-ATMs-746193.html). Barwise and Bachfeld in their study

Interestingly, there is also the possibility of organised crime working in concert with individuals in payment card fraud. For instance, as revealed by Mohamad in her paper, there were occasions where organised crime groups also recruit financially vulnerable individuals to participate in ‘shopping holidays’ to Australia to use fraudulent or stolen credit cards.³⁷⁸

In Indonesia, information about who the fraudsters in the payment card system are is also far from clear. The ‘dark number/figure’ phenomenon (encompassing both unreported and, more obviously, undetected incidents of criminal activity) has occurred in Indonesia as elsewhere. Banks and other payment system providers tend to ‘bury’ fraud incidents for the sake of a company’s reputation and to avoid further ‘hassles’ in terms of a police investigation.

Unless the fraudsters were successfully apprehended or could be identified through CCTV footage, efforts to determine their identity in relation to proceeds of crime are very difficult.³⁷⁹ Nevertheless, many ATMs in Indonesia are still not equipped with CCTV cameras.³⁸⁰ Where they do exist at compromised ATMs, their evidence is often unreliable because the footage is blurred, or the record has been deleted, or sometimes the camera simply does not work. In many cases, even if the CCTV is working well, the fraudsters are still difficult to identify because they were wearing baseball caps or even full-face helmets to avoid facial recognition. The apprehension of payment card

revealed that payment card fraud conducted on a huge scale can be associated with terrorist organisations. In early 2007, the Tamil Tigers (LTTE) through Sri Lankan asylum seekers in the UK, purchased petrol station franchises and subsequently systematically skimmed the cards of UK motorists at least 200 petrol stations in the North and East of the UK. See also Dennis Lormel, ‘Terrorism and Credit Card Information Theft: Connecting the Dots’ (2008) <http://www.ipsaintl.com/2008_2/September-2008_3.html>, 14. This document can be retrieved from: <http://www.ipsaintl.com/2008_2/September-2008_3.html>. In his study, Lormel argues that payment cards (such as credit cards) are extremely vulnerable to fraud and have been used extensively by terrorists, such as Imam Samudera (the person that responsible for Bali bombing a decade ago). See also Anderson et al, above n 338, 10.

³⁷⁸ Mohamad, above n 302, 13–14. See also Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 104.

³⁷⁹ See Permana, above n 31. It is there related how the city of Yogyakarta’s police department (Indonesia) complained to the banks regarding the poor quality of the banks’ ATM CCTV records, which made investigation of ATM fraud and uncovering perpetrators very difficult. Mr Tiong (from Yogyakarta Police Watch) asked the police department to improve their performance, since ATM fraud occurrence was increasing; however, none of the fraudsters has been successfully apprehended.

³⁸⁰ Gede Suardana, *POLDA Bali akui Kesulitan Ungkap Kasus Pembobolan ATM* [Bali Local Police Department Admitted They Had Difficulties to Revealed ATM Theft Cases] (1 February 2010) <<http://news.detik.com/read/2010/02/01/144856/1290356/10/polda-bali-akui-kesulitan-ungkap-kasus-pembobolan-atm>>. In this news-story, Bali Police Chief, Police Inspector General Sutisna, admitted that police have difficulty in discovering the perpetrators of ATM theft due to a lack of evidence and clues at the crime scene. One of the major causes of these difficulties was the absence of CCTV cameras at many banks’ ATMs which had (it was suspected) been compromised.

fraudsters also remains very difficult (especially for ATM fraud) since the gap between the identity theft/identity fraud and fraud reports from consumers are relatively long and records may be taped over. Nevertheless, the Indonesian police have successfully apprehended some fraudsters. Some were local,³⁸¹ while others came from overseas.³⁸² There was also an instance where overseas fraudsters became fraud masterminds in Indonesia and were working in concert with Indonesian culprits who executed ATM/debit card fraud in the field.³⁸³

3.5. Conclusion

The general nature of ATM/debit card payments as a part of a retail payment system with its large number of participants, less exhaustive security features, its more open and increased access points including the all-pervasive unattended consumer activated terminals, and greater bank interoperability and the increased involvement of third party service providers — has magnified and complicated some of banking's traditional risks. Security problems associated with ATM/debit card transactions exist from the moment of initiation of an ATM/debit card transaction until its settlement — namely fraud risk — cut across risk categories and expose banks to legal and reputational risk.

Nowadays, fraudsters that target ATM/debit cards have more efficient and quicker ways to perpetrate identity theft that could lead to identity fraud, such as by unauthorised ATM/debit card transactions. They are also more motivated to target banks and their consumers as the opportunities and incentives to commit ATM/debit card fraud have

³⁸¹ See, eg, Gede Suardana, *Pembobol ATM Diancam 15 Tahun Penjara [ATM Fraudsters Threatened 15 Years in Prison]* (23 June 2010) Detik.com <<http://news.detik.com/read/2010/06/23/180654/1385062/10/pembobol-atm-diancam-15-tahun-penjara>>.

³⁸² Gede Suardana, *WN Malaysia Pembobol ATM di Kuta Dibekuk [Malaysian Citizen ATM Theft in Kuta was Arrested]* (2 August 2011) Detik.com <<http://news.detik.com/read/2011/08/02/123639/1694686/10/wn-malaysia-pembobol-atm-di-kuta-dibekuk>>. See also: *Pembobol ATM Asal Srilanka Dicidaduk [ATM Thief from Sri Lanka Apprehended]* (24 June 2012) Kompas.com <<http://lipsus.kompas.com/topikpilihanlist/2133/1/100.hari.jokowi-basuki/read/xml/2008/06/24/11101760/Pembobol.ATM.Asal.Sri.Lanka.Dicidaduk>>; *'Napi Asal Malaysia Otak Pembobol ATM [Recidivist From Malaysia Became Mastermind of ATM Theft]*', *Kompas* (online), 19 September 2008 <<http://health.kompas.com/read/2008/09/19/03593524/Napi.Asal.Malaysia.Otak.Pembobol.ATM>>.

³⁸³ Rachman and Fitri, above n 36. See also Didi Tri Kertapati, *Pembobolan Dana Nasabah: Pelaku Diduga Masuk Sindikat Internasional [Consumers' Fund Theft: Alleged Perpetrators' Suspected as a Member of International Syndicate]* (26 January 2010) Detik.com <<http://news.detik.com/read/2010/01/26/173650/1286539/10/pelaku-diduga-masuk-sindikat-internasional>>; Wahyu Satriani Ari Wulan, *'BCA Blokir Penarikan dari Toronto dan Australia [BCA Blocked Withdrawal from Toronto and Australia]*', *Kompas* (online), 26 January 2010 <<http://news.detik.com/read/2010/01/26/173650/1286539/10/pelaku-diduga-masuk-sindikat-internasional>>.

increased, due to the increased uptake of the online methods for transactions and communication of ATM/EFTPOS transactions, the proliferation of information available in the online environment in terms of an abundance fraudulent methods and tools shared on the Internet, remote and anonymous access, high-quality graphics and printing, and multipurpose fraudulent tools that can be obtained more easily and less expensively than previously. The banks' inability to prevent and/or detect payment fraud, or take action if they do, makes payment card fraud all the more appealing. Apprehension of risk of detection and prosecution by law enforcement agencies is also very minimal, while the rewards for fraud can be highly significant. Fraudsters themselves can be anyone, from individual beginners to the transnational crime organisations, insiders, or outsiders.

Regarding the nature of the payment card system along with fraudsters' motives and the incentives to commit ATM/debit card fraud, payment system stakeholders should understand that payment card transactions would always be susceptible to fraud. Fraudsters view payment card fraud as victimless, easy and most rewarding, since the gains in terms of illicit money and the opportunity to elude identification in relation to the fraud are great. The possibility of easy money almost always is a driver for the fraud.

Hence, in order to minimise ATM/debit card risks, banking industries (including consumers), law enforcement agencies and the regulator must work together to improve security awareness and develop fraud prevention and detection methods to circumvent fraud. Payment card regulation should also be established comprehensively, including fraud liability rules. The regulations could be expected to create incentives for every party involved in the banking industry to increase their vigilance and ensure best security standard practice. Severe and effective punishment of fraudsters is also needed to create a deterrent effect and prevent payment card fraud.

CHAPTER 4 – IDENTITY THEFT/IDENTITY FRAUD METHODS IN ATM/DEBIT CARD TRANSACTIONS IN INDONESIA: OPPORTUNITIES AND INCENTIVES

4.1. Introduction

The payment card system — just like other electronic payment systems — relies on identification, authentication and authorisation processes to ensure that the system will only process authorised transactions. In Indonesia, the ATM/debit card systems still utilise a magnetic stripe as a means of recording and storing consumer data. All those processes still rely on the existence of correct comparative data between magnetic stripe card data and its associated PIN recorded in the bank's system.

Unfortunately, identification, authorisation and authentication technology using magnetic stripe data and PIN are notoriously vulnerable and susceptible to various fraud attacks. Identity theft that later can be transformed into identity fraud can be conducted actively or passively. The fraud perpetrator can be anyone from inside a bank and/or its agent, an outsider/third party, and/or consumers themselves.

Therefore, it is argued that one way to understand more about identity theft/fraud attack and its prevention/mitigation is to determine the point where the attack was committed (the point of compromise). If the point of compromise can be determined, then the party that should be responsible for safeguarding the payment transaction and therefore any consequent fraud liability where such a breach occurs can be more easily drawn. Hence, even though not exhaustive, this chapter tries to enumerate all types of fraudulent activities along with the points of compromise and their associated fraud methods/devices that target consumers and/or banks.

4.2. Concept of Identity Theft and Identity Fraud in Payment Cards

In this thesis, 'identity' refers to 'the distinguishing character or personality of an individual'. In accordance with this definition, 'identity theft' can be described as a

conduct that ‘involves the theft of elements of a person’s identifying characteristics (items in the list such as name, address, credit card number).’³⁸⁴

In addition to defining identity theft, it is also common to define another form of theft, which is identity fraud. Identity theft and identity fraud are two terminologies that are sometimes used interchangeably in the various literature resources. However, it is argued that identity theft and identity fraud should be distinguished. They are different terms with different implementation phases in practice. Schreft argues that a precise definition of identity theft is important, in regard to efforts to measure and combat identity theft.³⁸⁵

Although some define identity theft as occurring ‘when one individual misuses another individual’s personal information to commit fraud’,³⁸⁶ others, such as Rachel Kim of Javelin Strategy & Research, argue that ‘identity theft occurs when someone gains your personal data without your permission’, while identity fraud occurs when ‘the criminal takes that personal information and misuses it for financial gain’.³⁸⁷ Therefore, often identity fraud is the subsequent action of identity theft.³⁸⁸ Fraud is generally the end goal of identity theft.³⁸⁹

In payment card fraud, identity theft that leads to payment fraud starts with the fraudsters having successfully gained either a genuine consumer’s ATM/debit cards (lost/stolen cards) or a consumer’s payment card information, and their PIN. Payment card fraud then occurs when fraudsters conduct unauthorised ATM/debit card transactions to obtain cash or goods using consumers’ lost/stolen cards or counterfeit cards that have been manufactured using that stolen information.³⁹⁰

³⁸⁴ Stacey L Schreft, ‘Risks of Identity Theft: Can the Market Protect the Payment System?’ (2007) 92(4) *Economic Review - Federal Bank of Kansas* 5, 7. See also Rachel Kim, ‘2007 Identity Fraud Report - Consumer Version: How Consumers Can Protect Themselves’ (Javelin Strategy & Research, 2007) 2.

³⁸⁵ Kim, above n 384.

³⁸⁶ Sullivan, ‘Can Smart Cards Reduce Payments Fraud and Identity Theft?’, above n 33, 39 [emphasis added], citing President’s Task Force on Identity Theft, ‘Combating Identity Theft: A Strategic Plan’.

³⁸⁷ Kim, above n 384, 2. See also Malphrus, above n 338, 32; Douglass, above n 122, 43–4.

³⁸⁸ Sullivan, ‘Can Smart Cards Reduce Payments Fraud and Identity Theft?’, above n 33, 36.

³⁸⁹ Kim, above n 384, 6.

³⁹⁰ Sullivan, ‘Can Smart Cards Reduce Payments Fraud and Identity Theft?’, above n 33, 39–40.

4.2.1. Identity Theft: Types of ATM/Debit Card Attack

In the payment card system, the objective of payment card security is to guarantee that only payments transactions authorised by cardholder are permitted.³⁹¹ To filter out the occurrence of fraud in the payment card transactions, ‘a card payment approval system authenticates the card, identifies the cardholder, and determines whether the transaction satisfies certain limits set by the card issuer or merchant’.³⁹²

Unfortunately, as the FFIEC admits, all authentication methodologies have weaknesses, both of a technical and non-technical nature.³⁹³ The payment card data and PIN information is relatively vulnerable and easy to attack using various fraud methods.³⁹⁴ Fraudsters know that if they obtain both data (card number data and PIN) (identity theft), then they can undertake unauthorised payment card transactions and drain a consumer’s account (identity fraud).³⁹⁵ In all payment card fraud, unauthorised ATM/debit card transactions always cause a latent risk of loss.³⁹⁶

Rachel Kim of Javelin Strategy & Research explains various ways in which consumers’ financial information can be stolen:

- Through a lost or stolen wallet, check book or credit card
- From a criminal changing the address on an account
- Through information stolen in your own home, including by friends, relatives, and in-home employees
- By someone who e-mails, calls, or text messages you, pretending to be a bank or other trusted source to get you to divulge private information
- By hacking, viruses, and spyware on a computer or ATM machine
- By a data breach at a retailer, school, bank, hospital or any agency that maintains access to your private information
- By a corrupt business employee who has access to your records
- Through eavesdropping by a criminal while you conduct a public transaction (“shoulder surfing”)
- Through mail theft from an unlocked mailbox
- From a trash can, a method known as “dumpster diving”
- Through new and different methods those criminals are continually developing.³⁹⁷

In addition, many organisations and experts have identified frequent types of payment card fraud,³⁹⁸ as follows: account application fraud;³⁹⁹ account takeover;⁴⁰⁰ use of lost/

³⁹¹ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 103.

³⁹² Ibid 102–104.

³⁹³ FFIEC, *Information Security*, above n 202, 33.

³⁹⁴ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 102–104.

³⁹⁵ Smart Card Alliance, ‘Fraud in the US Payments Industry’, above n 297, 11.

³⁹⁶ Diebold incorporated, ‘White Paper: Battling Card Fraud through Chip and PIN Technology,’ above n 209, 5.

³⁹⁷ Kim, above n 384, 2.

stolen,⁴⁰¹ altered⁴⁰² or counterfeit cards;⁴⁰³ or criminal activity involving ‘card not present’ (CNP) transactions,⁴⁰⁴ merchant collusion,⁴⁰⁵ and cardholder fraud.⁴⁰⁶

Based on the attack method or technique, two types of attacks on the payment card system can be distinguished: first, the ‘active attack: an attempt to alter system resources or affect their operation’; and secondly, the ‘passive attack: an attempt to learn or make use of information from the system that does not affect system resources’.⁴⁰⁷ Meyer and Matyas argue that the ‘passive attack is most probably to enable the subsequent use of lost or stolen cards, or the production and use of counterfeit cards’.⁴⁰⁸

Furthermore, attacks can be distinguished according to the origin of the attack: first, ‘the ‘inside attack: initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization’. Therefore, e-banking systems should also be protected against unauthorised activities by current and former employees.⁴⁰⁹ Secondly,

³⁹⁸ See INTERPOL, *Payment Cards*, above n 21; Iannacci and Morris, above n 20, 30; Devos and Pipan, above n 297, 6–7; Oracle Corporation, *US Card Fraud* (2010) Bank Gateway.com <<http://www.banking-gateway.com/microsites/oracle/US%20Card%20Fraud.pdf>>, 3–5; Financial Fraud Action UK, above n 346, 7.

³⁹⁹ A type of ID theft crime in which payment cards are obtained through a fraudulent application process using stolen or counterfeit documents.

⁴⁰⁰ Another type of ID theft crime, usually involving deception of a financial institution, re-issue of a payment card and its redirection to a different address.

⁴⁰¹ This type of fraud involves misuse of actual cards that have been either lost by or stolen from the genuine cardholder.

⁴⁰² Any access device that is changed in any way to change the appearance or electronic information contained within the device is said to be ‘altered’. Criminals often use stolen, valid card numbers on stolen devices to create the appearance of a valid card.

⁴⁰³ Fraud undertaken using plastic cards that have been specifically produced or existing cards that have been altered. These cards are encoded with illegally obtained payment card account data in order to pay for goods and services or to withdraw cash.

⁴⁰⁴ Fraud committed using payment card account data to undertake transactions where there is no face-to-face contact between the seller and purchaser. Typically, this type of fraud is committed over the Internet, by mail order or telephone. CNP fraud is currently the fastest growing payment card related type of fraud in many areas of the world. However, since this thesis only focuses on ATM/debit card fraud where the transactions require the physical presence of a payment card, the fraud method discussion will not include CNP fraud such as account application fraud, account take over, and the like.

⁴⁰⁵ Sometimes a merchant will work in concert with the criminal to perpetrate the fraud. Not only do employees working for merchants get involved in these schemes, but the company owners do as well, and this happens in greater numbers.

⁴⁰⁶ Cardholder fraud occurs when a credit card customer receives a credit card under his own identity but with the intent to defraud the issuer.

⁴⁰⁷ Stallings and Brown, above n 221, 17. See also Meyer and Matyas, above n 72, 445–6.

⁴⁰⁸ Meyer and Matyas, above n 72, 445–6.

⁴⁰⁹ Kondabagil, above n 194, 95.

the ‘outside attack: initiated from outside the perimeter, by an unauthorized or illegitimate user of the bank’s system (an “outsider”)’.⁴¹⁰

However, for the purpose of this thesis, attacks will be distinguished according to where the point of compromise exists (that is, the point where the fraudster attacked the payment card system). This information security approach will be deemed very important, because by knowing the location of the point of compromise, the typology of the fraud method and the fraudsters can be more easily depicted. The party that is supposed to be in the best position to safeguard the payment card system at the point of compromise can also be determined and should most likely also be responsible for the loss of money from the consumer account (fraud liability).

In accordance with this idea, it is deemed necessary that in order to accurately appoint the party that should be responsible for fraud liability, the point of compromise should be demarcated into three target areas of crime/fraud: (1) attack on consumers/cardholder (outside consumer activated terminal perimeter/bank system); (2) attack on consumers and banks (mixed perimeter); or (3) attack on bank/bank’s third party system (inside bank system perimeter, including banks’ counterpart/third party provider/network).⁴¹¹

4.2.1.1. Cardholder as Point of Compromise

4.2.1.1.1. Third Party Fraud

Some fraudsters, usually low skill fraudsters, prefer to steal the ATM/debit card and/or its PIN directly from the cardholders. They use various methods, such as:

1. Lost and Stolen Card Fraud

The most common and conventional card fraud is theft. Lost/stolen card fraud is where the card is lost or stolen and then attempts are made by an unauthorised individual to use it.⁴¹²

⁴¹⁰ Stallings and Brown, above n 221, 17.

⁴¹¹ The fraud classification is similar to those of Devos and Pipan. In their work, they split the fraud method according to the target of the data theft: 1) theft of original card and cardholder information directly from the card, 2) theft of original card and cardholder information directly from the system, and 3) theft of original card and cardholder information directly from the cardholder. However, in practice these three classifications can be intermingled so it would complicate the analysis of related parties regarding who should be responsible for losses incurred. See Devos and Pipan, above n 297.

⁴¹² Devos and Pipan, above n 297, 6–7. See also Financial Fraud Action UK, above n 346, 28.

When an ATM/Debit card is stolen, the fraudster, who currently holds the card, could use it at a merchant where a PIN or signature is not required. However, if the fraudster could retrieve the PIN of the lost or stolen card, greater damage can be expected to occur because now the card can be used to withdraw money at an ATM or used as a means of payment at PIN-enabled merchants.⁴¹³

Lost and stolen card fraud covers fraud that is derived from consumers' genuine payment cards being abused where such cards have been reported as lost or stolen by the original cardholder.⁴¹⁴ In accordance with this definition, Oracle Corporation argues that this fraud may not apparently be the work of 'card gangs'.⁴¹⁵ By contrast, Hole et al assert that a card gang might be behind card stolen fraud, where it is believed that the encrypted PIN value inside the magnetic stripe card can be cracked using a 'two-step attack strategy'. However, Hole et al's assertion could not be generalised to every ATM/Debit card system, since other bank systems might not include PIN information inside the magnetic stripe. For instance, in Indonesia, all five bank employees who have been interviewed in Jakarta between July and August 2012 said that in their payment card system, PIN information or PIN information values are not stored inside the magnetic stripe card.⁴¹⁶

From this above list of fraud threats that target consumers, typically the exposure to this type of fraud is limited, since the window of opportunity for card utilisation by fraudsters is quite narrow, just the time between the loss of a card and the time of the reporting of that loss by the cardholder.⁴¹⁷

2. Card Swapping and Social Engineering Fraud

Some fraudsters target bank cardholders in order to get their payment card and PIN. Among methods that are recorded are the fraudster swapping consumers ATM/debit card (especially ATM/debit card without printed consumer name (anonymous card or also known as an 'instant card') with other genuine ATM/debit card by trickery, such

⁴¹³ Financial Fraud Action UK, above n 346. Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud prevention, presenting a united front against financial fraud and its effects.

⁴¹⁴ Oracle Corporation, above n 398, 3–5.

⁴¹⁵ Ibid.

⁴¹⁶ Kjell J Hole et al, 'Lessons from the Norwegian ATM System' (2007) 5 *IEEE Security & Privacy Magazine* 25, 25–9. See also interviews: BO-1; BO-2; BO-3; BO-4; and BO-6.

⁴¹⁷ Meyer and Matyas, above n 72, 445–6.

as: swapping consumer card at the legitimate point of sale outlet (employee fraud); put a matchstick inside the ATM slot to block the ATM/debit card with the con-artist subsequently offering to help solve the problem, and swapping the card immediately; swapping the consumer's card when the card has fallen from the consumer's hand due to a deliberate nudge or body impact from the fraudster (normally this happens when consumers have just withdrawn money from an ATM); or by deceit and stories fabricated by the fraudster who urges consumers to agree to hand over their card for 'fund checking' purposes as a prerequisite for a particular offer, such as for a cheap Rolex watch or fund transfer destination for other fictitious purposes. Fraudsters typically obtain the PIN by using the shoulder surfing method.

To deceive bank consumers, most of the fraud methods employ 'social engineering techniques' and can be classified as an active attack. The FFIEC described social engineering as follows:

Social engineering involves an attacker obtaining authenticators by simply asking for them. For instance, the attacker may masquerade as a legitimate user who needs a password reset or as a contractor who must have immediate access to correct a system performance problem. By using persuasion, being aggressive, or using other interpersonal skills, the attackers encourage a legitimate user or other authorized person to give them authentication credentials.⁴¹⁸

The enabling factor for the use of social engineering techniques was and is the asymmetry of information that exists between the banks and their consumers. It is a reality that in practice, especially in Indonesia, banks tend to promote only the advantages of electronic banking, including payment card system, and remain reluctant to educate consumers regarding the various risks that threaten the payment card system (and pose a risk to the consumer). The reason for this reluctance, as a prominent Indonesian banker revealed when interviewed, is that the bank is afraid that consumers will have a false perception that the bank has weak security if it educates consumers about the various existing fraud methods.⁴¹⁹

⁴¹⁸ FFIEC, *Information Security*, above n 202, 35–6. See also Pipkin, above n 226, 69, 78. Pipkin argues that social engineering methods have many different facets, but the most frequent include 'sympathy (I cannot get this to work, can you help?), empathy (I understand. Tell me your problems and maybe I can help), admiration (You are so good at this, can you show me how?), and intimidation (if you do not get me that information, you will be in big trouble!)'.

⁴¹⁹ Interview: Siti Sekarwati, Division Head ATM Operation, PT Bank Mandiri, Tbk (Persero) (Jakarta, 5 August 2012); See also Interview with Wani Sabu, Division Head Halo BCA, PT Bank Central Asia, Tbk (Jakarta, 14 August 2012).

This lack of knowledge of fraud and other vulnerabilities in the system gives criminals an advantage so that they are able to more easily defraud the consumers who are uninformed about their payment cards.⁴²⁰

4.2.1.1.2. Second Party Fraud

Included in this type of fraud are any fraudulent activities that are committed by the family, friends or acquaintances of consumers themselves. In many instances, consumers either deliberately or inadvertently fail to safeguard consumer payment cards and PINs, thus enabling ‘the people around them’, such as wife/husband, spouse, partner, colleagues, office boy, child, or the like to access the card and PIN information, which later can be used to conduct unauthorised ATM/debit card transactions.

4.2.1.1.3. First Party Fraud

The absence of adequate non-repudiation authentication method to verify the validity of consumer transactions may also facilitate dishonest consumers’ misuse of the payment card information to repudiate transactions and make claims for restitution for ‘damages’.⁴²¹ In relation to ATM/debit card, first party fraud involves cardholders who make fraudulent claims knowing that they themselves withdrew the disputed funds.⁴²² First party fraud commonly increases when there is harsh economic conditions that force some consumers to defraud their own bank.⁴²³

4.2.1.2. Consumer-Activated Terminal and Cardholder as Point of Compromise: Card Trapping

In the previous sub-section, fraudsters are seen to target cardholders alone in order to get their genuine ATM/debit card and PIN. Lost and stolen cards, card swapping, social engineering and the like have been employed to obtain a cardholder’s genuine card. In committing their illegal action, fraudsters do not jeopardise any payment card system within the bank perimeter (even though the crime itself can occur in close proximity to one part of the payment card system infrastructure, such as a bank ATM location).

⁴²⁰ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 102–104. See also Kondabagil, above n 194, 95.

⁴²¹ Kondabagil, above n 194, 95.

⁴²² Meyer and Matyas, above n 72, 445–6.

⁴²³ Oracle Corporation, above n 398, 3–5.

Nevertheless, there is also a payment card fraud method that converges consumers or cardholders and the payment card system infrastructure as the fraud target in order to get a consumer's ATM/debit card and PIN — this is card-trapping fraud.⁴²⁴ The card-trapping method has many variants, such as the 'Lebanese loop' and 'Algerian V'.⁴²⁵ Card trapping constitutes a major attack on ATMs.⁴²⁶

This method targets the ATM, where the fraudster or an associate places a malicious device directly onto or into the ATM card reader slot to steal the cardholder's genuine card.⁴²⁷ It aims to 'prevent the card being returned to the consumer and also stop the ATM from retracting it'.⁴²⁸ According to Diebold Incorporated, the card trapping or card theft mechanism operates as follows:

In an effort to obtain actual cards, criminals have used a variety of card trapping devices comprised of slim mechanical devices, often encased in a plastic transparent film, inserted into the card reader throat. Hooks are attached to the probes preventing the card from being returned to the consumer at the end of the transaction. When the ATM terminal user shows concern due to the captured card, the criminal, usually in close proximity of the ATM, will offer support, suggesting the user enter the PIN again, so that he or she is able to view the entry and remember the PIN. After the consumer leaves the area, believing their card to have been captured by the ATM, the criminal will then use a probe (fishing device) to extract the card. Having viewed the customers PIN and now having the card in hand, the criminal can easily withdraw money from the unsuspecting user's account.⁴²⁹

From the nature of the attack, card trapping can be categorised as an active attack. Active attacks are more obvious than passive attacks such as skimming fraud. Unlike a skimming fraud that could capture hundreds of examples of magnetic stripe card data in just one (passive) attack, card-trapping fraud usually only causes one card to be lost in each attack.⁴³⁰

A wide variety of devices have been used as in card trapping. As mentioned above, Diebold Incorporated asserts that criminals have utilised plastic transparent film, plates,

⁴²⁴ Mohamad, above n 302, 10. See also Mohammed, above n 195, 216–17.

⁴²⁵ Mohammed, above n 195, 216–17.

⁴²⁶ Pooja Mali et al, 'Multilevel ATM Security Based on Two Factor Biometrics' (2012) 1(8) *International Journal of Engineering Research and Technology (IJERT)* 1.

⁴²⁷ Mohammed, above n 195, 216–17.

⁴²⁸ Brian Krebs, *Beware Card - and Cash Trapping at the ATM* (20 November 2012) <<http://krebsonsecurity.com/tag/card-trap/>>.

⁴²⁹ Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7. See also Financial Fraud Action UK, above n 346, 28; Mohammed, above n 195, 216–17.

⁴³⁰ Mohammed, above n 195, 216–17.

wires, probes, and hooks (among other things) as card-trapping devices.⁴³¹ In addition, Mohammed explained that a loop of tape, wire, or strong thread over an ATM card reader is also commonly used.⁴³² A few ATM maintenance officers in Indonesia (who refuse to be named) confirm that all these fraudulent devices are utilised in card-trapping fraud in Indonesia. Moreover, they also add that matchbox sticks, parts of card payment material or even paper are often found inside the ATM slot, placed to facilitate card trapping.

In conjunction with this activity, fraudsters generally will deceive cardholders into revealing their PIN with various social engineering techniques, such as:

- a) direct observation by the perpetrator;⁴³³
- b) putting an overlay device on the keypad PIN;⁴³⁴ or
- c) attaching a spurious bank call centre sticker onto the front of the ATM and convincing the consumer to reveal their PIN when they eventually call the person posing as a bank officer.⁴³⁵

Recently, there has been an increase in the card-trapping pattern fraud globally, apparently as a result of the widespread installation of anti-skimming devices that

⁴³¹ Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 2–5.

⁴³² Mohammed, above n 195, 216–17. See also NCR, *Is ATM Security a Challenge in Kenya and All Over the World?* (2011) <http://aitec.usp.net/Banking%20&%20Mobile%20Money%20COMESA,%202-3%20March%202011,%20Nairobi/TopDare_NCR_BankingMobileMoneyCOMESA2-3Mar2011.pdf> 12–30.

⁴³³ See Nicholas J Johnson, *Lebanese Loops* (2013) Australia's Honest Con Man: Encyclopedia of Scams <<http://scams.wikispaces.com/Lebanese+Loops>>. See *ATM Scam Warning* (26 February 2003) About.com: Urban Legends <<http://urbanlegends.about.com/library/blatm-scam.htm>>. See also the series of pictures in presentation slides concerning card-trapping sequences at NCR, *Is ATM Security a Challenge in Kenya and All Over the World?*, above n 432, 10–31; Mohammed, above n 195, 216–17. In Indonesia, hile cardholders panic due to their cards having been trapped in the ATM slot, the criminal, who is usually in close proximity to the ATM, pretends to be a 'Good Samaritan', and comes to offer support to the distressed consumer. One of the most common methods is that the good Samaritan claims that he has had similar experiences, suggesting that the cardholder enter their PIN and then cancel the transaction in order to force the ATM spew out the card. The criminal obtains the PIN by watching the panicked, unaware and distracted cardholders when they enter their PIN on the ATM's PIN pad.

⁴³⁴ Jeremy Kirk, *Criminals Turn to 'Card-Trapping' at ATM Machines to Get Cash* (19 October 2011) CIO <http://www.cio.com.au/article/404671/criminals_turn_card-trapping_atm_machines_get_cash/>.

⁴³⁵ *Kejahatan Card Trapping Memacetkan Mesin ATM Untuk Menguras Uang ATM (Warning)* [Card Trapping Crime Jammed ATM Machine to Drain ATM Cash (Warning)] (15 October 2012) Direktorat Reserse Kriminal Umum, Polda Metropolitan Jakarta Raya, <<http://reskrim.metro.polri.go.id/read/article/8203/19/Kejahatan-Card-Trapping-Memacetkan-Mesin-ATM-Untuk-Menguras-Uang-ATM-Warning>>; Moksa Hutasoit, *Awas, Penipuan Lewat ATM Marak di Depok!* [Beware, Many ATM frauds in Depok!] (19 June 2010) Detik.com <<http://news.detik.com/read/2010/06/19/180214/1381958/10/awas-penipuan-lewat-atm-marak-di-depok?nd992203605>>; Mohammed, above n 195, 216–17; Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7.

caused the skimming method becoming more difficult to use. This observation was shared by the European ATM Security Team and the author's Indonesian bank interviewees alike.⁴³⁶ Other than that, the card-trapping method is deemed to be simpler, more efficient, and does not require particular skills or expensive devices (such as is the case with skimming or wire/computer tapping). Even though card trapping can be categorised as a 'low technology' fraud method, nonetheless it is a very effective method to steal consumers' cards. Although chip card technology may be impregnable to skimming fraud method, it is still susceptible to this type of fraud.

Figure 4: Card Trapping (Lebanese Loop)



Figure 5: Examples of Fake Bank Call Centre Details Affixed to ATMs in Indonesia



⁴³⁶ According to the European ATM Security Team (EAST) 2011 survey, cash trapping fraud surged in 11 European Countries and contributed to a near doubling of recorded ATM fraud attacks, from just 6,649 attacks for the first six months in 2010 to 11,220 attacks for the same period in 2011. See Kirk, 'Criminals Turn to 'Card Trapping'', above n 434. See also Interview with Wani Sabu, Division Head Halo BCA, PT Bank Central Asia, Tbk (Jakarta, 14 August 2012). According to her, since anti-skimmer devices have been mounted at most Bank BCA ATMs, skimming fraud incidents have reduced quite significantly. However, other types of fraud such as card-trapping and SMS incidents have significantly increased (balloon effect).



Source: mafiakartukredit.com

Even though banks have made efforts to tighten security against fraudulent activities at ATMs, bank officials admit that card-trapping fraud is still a problem despite anti-ATM skimmer technology having been installed, a fact attested to by maintenance officers. Bank maintenance officer interviewees noted that they were still busy removing card-trapping devices from various compromised ATMs in Jakarta on a daily basis. To mitigate card-trapping fraud, some banks in Indonesia have replaced old ATMs with ones that are able to send an 'error' message and halt services if an ATM's slot is infiltrated by foreign materials. However, older ATMs are still used widely in Indonesia, and hence they are still highly susceptible to various fraud risks.⁴³⁷ Fraudsters try new methods to steal consumers' ATM/debit card data at ATMs. If they cannot defeat the new security technology, they come up with new ways to work around the technology. Sometimes, a low-tech method can be just as effective and lucrative for criminals as actual attacks on ATMs.⁴³⁸

4.2.1.3. Consumer-Activated Terminal as a Point of Compromise

Nowadays, there is a significant increase in the use of ATMs and EFTPOS terminals by banking consumers around the globe. Unlike the bank branches that are limited in terms of their numbers and in the hours during which they are open, the consumer activated terminal is available 24 hours a day at most locations, from the busy streets in central business districts, to transport terminals, malls, and so on, to a quiet corner in a suburb.

⁴³⁷ Interviews: BMO-1 and BMO-2. This phenomenon has been recognised by some bank officials at a meeting with Bank Indonesia in the Payment System Department on 5 November 2010, where the Author was also involved.

⁴³⁸ Kitten, *ATM Skimming Threats Evolve*, above n 349.

However, the great benefit offered consumers by consumer activated terminals that are located beyond the inside of a banking institution building is accompanied by an increased possibility of fraud attack. The relatively unguarded consumer activated terminals open the door of opportunity to the commission of crime.⁴³⁹

ATM/debit card consumers confidently conduct remote payment card transactions because they believe that the banks will protect their transactions. Indeed, in general banks are always keen to protect their systems and consumers. However, regardless of bank efforts to secure ATM/debit card transactions, Diebold Inc states that there are seven (inherent) points of compromise along the ‘chain of trust’ in the bank system that can be attacked by fraudsters and each attracts its own attack method/s.

1. Access control reader — these types of skimming attacks were diminishing, but are on the rise again. [Author’s note: An inside camera can be used to steal PINs.⁴⁴⁰]
2. External skimmer — a camera or keypad overlay is used to capture PINs.
3. Internal skimmer — attacks have been increasing, especially at gas pumps where criminals open the pump and attach an internal skimmer. These attacks are impossible for consumers to detect and difficult for gas stations to detect.
4. USB “sniffing” — criminals intercept and store card information, coupled with a PIN camera.
5. Malware — placed on a PC and ATM; most criminals use a USB drive to steal data.
6. TCP/IP theft — not all FIs have encrypted data, leaving them vulnerable to brute-force attacks.⁴⁴¹
7. Back-end infrastructure infiltration — theft from where card information is stored.⁴⁴²

4.2.1.3.1. Swallowed ATM/Debit Card Theft at ATM’s ‘Retain Pocket’

UNCITRAL has canvassed that current models cash dispensers — ATMs and EFTPOS terminals — ‘require the convergence of two items to authorise the transaction. i.e. a plastic card with magnetic stripe containing certain information and the entry by the bank customer of a personal identification number (PIN)’.⁴⁴³

⁴³⁹ Diebold Incorporated, *Playing Defense: Trends in ATM Attacks* (2007) <http://www.diebold.com/atmsecurity/files/DBD_WhitePaper_Island.pdf>.

⁴⁴⁰ Dong-Tsan Lee, ‘Re-examining the Security Issues of ATM Systems’ (2004) 2004(2) *Computer Fraud & Security* 13, 13.

⁴⁴¹ Note: In a definition posted by Cory Janssen, ‘[a] brute force attack is a “trial and error” method used to obtain information, such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organisation’s network security’: Cory Janssen, *Brute Force Attack* (2013) technopedia <<http://www.technopedia.com/definition/18091/brute-force-attack>>.

⁴⁴² Diebold Incorporated, ‘*White Paper: ATM Fraud and Security*’, above n 348, 5.

⁴⁴³ UNCITRAL, ‘UNCITRAL Legal Guide on Electronic Funds Transfers’, above n 189, 50–1.

The natural location of ATMs and EFTPOS machines outside the bank perimeter with most of them unattended (also known as ‘island ATMs’) eliminates the necessity for ‘round the clock’ human involvement and makes ATMs a relatively easy target for various crimes.⁴⁴⁴ Unrestricted physical access to ATM components outside the safety of the bank — such as to a card reader and PIN pad on the front of the ATM — are vulnerable to compromise by fraudulent devices such as skimmers, false keypads, and so on.⁴⁴⁵

The involvement of many different people or organisations in the establishment or life cycle activities related to these machines (such as cash or paper-print replenishment, maintenance, booth cleaning, and so on) also makes ATMs and EFTPOS machines more vulnerable to abuse. However, fraudsters have recently not only targeted island ATMs (such as standalone ATMs located in stores or other buildings) as well as ‘through the wall’ ATMs, but also non-island ATMs (that is, ATMs that located in the bank branch).⁴⁴⁶

There have also been many reports where besides an ATM attack to obtain a consumer’s personal information such as their card number and PIN (which has become the most prevalent and notorious ATM crime),⁴⁴⁷ criminals are also stealing entire ATMs laden with cash.⁴⁴⁸ Nonetheless, the latter type of activity is beyond the scope of

⁴⁴⁴ See Bell, above n 44. See also Diebold Incorporated, ‘*White Paper: ATM Fraud and Security*’, above n 348, 1.

⁴⁴⁵ Pat Telford and Peter Kulik, *Ten Immutable Laws of ATM Security* (2011) ATM Industry Association (ATMIA)

<<https://www.atmia.com/clientuploads/directory/whitepaper/TenImmutableLawsofATMSecurity2011.pdf>>.. See also Bond and Zielinski, above n 328.

⁴⁴⁶ Diebold Incorporated, ‘*White Paper: ATM Fraud and Security*’, above n 348, 2–5.

⁴⁴⁷ Ibid.

⁴⁴⁸ Russell G Smith and Peter Grabosky, ‘Plastic Card Fraud’ (Paper presented at the Conference Crime against Business, Melbourne, 1998) 6. See also Diebold Incorporated, ‘*White Paper: ATM Fraud and Security*’, above n 348, 2–5. In the white paper, Diebold Incorporated stated that physical attacks on an ATM ‘include any type of assault that physically damages the components of the ATM in an attempt to obtain cash’. Targets include: (a) The ATM’s safe’ (by cutting/grinding/drilling/prying the locks, handles and hinges of the safe door, or using a blowtorch or similar device, or explosives); (b) The ATM ‘top hat’ in an attempt to steal ATM components such as the hard drive, or to attach an internet skimmer or download malware (by prying open the door or side panels of the top hat, prying open the fascia, damaging the lock to gain access, picking the lock in order to covertly attach an internal skimmer; (c) ‘The ATM ‘presenter and depositor’ in an effort to gain access to the ATM’s cash sources, which include the deposit storage area and the divert bin (by ‘cutting, prying, drilling, torching, and smashing’); (d) ‘The entire ATM, when attempting’ to remove it from its existing location and move it to a location where its safe or vault can be laboriously penetrated and its contents removed (‘by ramming or ram raid — attempting to ram the ATM with a car, truck or heavy machinery; pulling — placing a chain or rope around an ATM and attaching the other end to a vehicle to pull the ATM from its foundation[s]...; lifting — using a forklift or similar equipment to try to lift the ATM from its foundation[s]’).

this thesis since it is not fraud and the loss, if any, is not associated with any consumer accounts, and hence will only be borne by the bank.

As most of the ATMs throughout the world share many similarities and standards, ‘ATM fraud is also not confined to particular regions of the world’. Probably the most complex factor is that the fraudsters and victims are ‘often on different continents, and the problems of one region can quickly become the problems of another’.⁴⁴⁹ Diebold Incorporated concluded several factors that attract ATM fraud globally:

ATM fraud is growing because it produces cash and is considered to be fairly low risk relative to other crimes. The necessary equipment for criminal activity is inexpensive, readily available and expendable. ATM fraud also lends itself to organized crime. The fraud is repeatable, profitable and does not appear likely to end.⁴⁵⁰

Generally, fraudsters physically attack the ATM in an effort to get cash, whether it is in the safe/vault or in the cash dispenser/depositor slot.⁴⁵¹ However, the safe itself is difficult to compromise because it is made with very strong metal with a special key that makes it difficult for a criminal to penetrate.⁴⁵² Therefore, instead of targeting cash stored in the safe, according to bank officers interviewed, some fraudsters in Indonesia prefer to target consumer cards that have been ‘swallowed’ by the ATM and retained inside it.⁴⁵³ Apparently, this *modus operandi* is derived from fraudsters considering it far easier to access consumer cards that have been swallowed and also less likely to attract the attention of bystanders or passers-by. Fraudsters have noticed that there will always be instances where this legitimately occurs, for example, a consumer entering a wrong PIN entry above the bank threshold limit (the number of times the bank permits the consumer to attempt to access their card using an incorrect PIN — consumers typically are only given three consecutive trials to enter the right PIN, otherwise their card will be automatically swallowed by the ATM). Such experiences also make consumers far less likely to suspect a card’s disappearance is due to other than machine malfunction (or their own error), so facilitating other methods of identity theft.

⁴⁴⁹ Diebold Incorporated, ‘*White Paper: ATM Fraud and Security*’, above n 348, 1.

⁴⁵⁰ Ibid 8. See also Mohamad, above n 302, 11. See also Telford and Kulik, above n 445.

⁴⁵¹ Diebold Incorporated, ‘*White Paper: ATM Fraud and Security*’, above n 348, 2–5.

⁴⁵² Attacks on safes normally require a quite a bit of effort and special tools, with methods including drilling, prying, pulling, or using explosive materials. These kinds of efforts — besides being time consuming — also involve greater risk for the fraudster in terms of increased risk of apprehension because of the noise and complications that occur during such operations.

⁴⁵³ Interviews: BO-1; BO-2; BO-3 and BO-4 who handle bank ATM operations.

In this method, however, fraudsters need to just open the ‘top hat’ of the ATM using a counterfeit key (many ‘top hat’ keys use a universal key, so it can be accessed by different vendors) or by forcing it open.⁴⁵⁴ As for the universal key, fraudsters can even purchase one on eBay.⁴⁵⁵ If the top hat is also equipped with an additional padlock, then fraudsters have to break the padlock to gain entry. Once the ATM top hat has been opened, the fraudsters take genuine consumer cards that have been swallowed and reside in a special compartment and use them for purchasing things in shops that do not require a consumer’s PIN.⁴⁵⁶ There is also a possibility that the fraudster can withdraw cash from an ATM, if they can guess what a card’s PIN is.⁴⁵⁷

Interestingly, this type of fraud method is still not widely known. The dearth of information concerning this type of fraud probably indicates that this method is either new or less attractive to fraudsters.⁴⁵⁸ The usage of genuine ATM/debit cards without PIN information will only provide limited financial gain for fraudsters. Apprehension risk is also greater, since fraudsters perform face-to-face transactions at EFTPOS locations. Other than that, consumers also tend to inform their banks regarding their ‘swallowed’ cards immediately, making the period in which perform unauthorised transactions relatively short.

4.2.1.3.2. Magnetic Stripe Card Data Theft at ATMs

1. Card Skimming

One of the most popular ways to access a consumer’s account information is to skim the information from the card. ‘Card skimming’ is the most frequently used method of

⁴⁵⁴ Ibid.

⁴⁵⁵ Robert Siciliano, *Flash Attacks: Big Money for Payment Card Scammers* (2011) Infosec Island <<http://www.infosecisland.com/blogview/10006-Flash-Attacks-Big-Money-for-Payment-Card-Scammers.html>>.

⁴⁵⁶ There are some banking practices in Indonesia where merchant transactions can be concluded without PIN or signature requirement. See Ramson Daniel, *Low Security Kartu ATM Mandiri [Low Security of Mandiri’s ATM]* (22 March 2012) Myzone: Ruang Jurnalisme Anda <<http://myzone.okezone.com/content/read/2012/03/22/6883/low-security-kartu-atm-mandiri>>.

⁴⁵⁷ For PIN guessing information, see Chapter Four / section 4.2.2.1 below and accompanying text.

⁴⁵⁸ There are a growing number of allegations from the banking industry that this fraud method is perpetrated or masterminded by someone who is familiar with ATM components. However, the suspect list can be quite long since many different parties might be involved in the ATM life cycle, such as the person in charge of maintenance, replenishment, bank staff, and so on. Some ATM top hats are actually doors can be accessed from behind or from the side, which renders efforts to identify the perpetrators using CCTV cameras useless.

illegally obtaining card track data on the magnetic stripe.⁴⁵⁹ To capture the data stored in the card's magnetic stripe, criminals use a device called a 'skimmer'.⁴⁶⁰ Even though payment card fraud methods vary, ATM skimming remains one of the payment card industry's greatest threat. According to one theft expert, Robert Siciliano, around USD350,000 was being lost worldwide daily to instances of ATM skimming in 2011, an amount that can only have increased.⁴⁶¹

Fraudsters still target ATMs as their primary target, simply because they offer the greatest monetary reward.⁴⁶² Unrestricted physical access to ATM components introduces risk. The most obvious risks are related to the card reader and PIN pad on the front of the ATM, which can be compromised by fraudsters.⁴⁶³ With ATM skimming method, fraudsters set up a card reader or skimmer and attach it to the ATM on bank premises (or elsewhere such as at a petrol pump, restaurant or retailer). This electronically captures magnetic stripe information when consumers conduct transactions.⁴⁶⁴

Diebold Incorporated asserts that 'criminals place a hard-to-detect, small overlay device on top of the card slot of ATMs or POS equipment'.⁴⁶⁵ Because a skimmer is relatively small, it can be sophisticated and disguised to fit over a legitimate slot (a factory installed card reader) on ATMs and designed to look like a normal part of the ATM (or other payment terminal).⁴⁶⁶ Further, Diebold Incorporated explains how skimming process take place:

⁴⁵⁹ Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 2–5. In the Indonesian context, see Herdaru Purnomo, *Pembobolan Via Alat Pembayaran Kartu Sudah Capai Rp. 12 Miliar* [Payment Card Theft Damaged Reached Rp12 billion] (8 June 2011) Detik.com <<http://finance.detik.com/read/2011/06/08/080958/1655426/5/pembobolan-via-alat-pembayaran-kartu-sudah-capai-rp-12-miliar>>.

⁴⁶⁰ Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7. See also Barwise and Bachfeld, above n 377.

⁴⁶¹ Kitten, *ATM Skimming Threats Evolve*, above n 349. Note: This figure was cited in 2011. US commentators have noted that the rate continues to escalate, even in the US: Robin Sidel, 'Theft of Debit-Card Data from ATMS Soars: Thieves are stealing information to make counterfeit plastic', *Wall Street Journal*, 19 May 2015, <<http://www.wsj.com/articles/theft-of-debit-card-data-from-atms-soars-1432078912>>. Debit card compromises at ATMs on bank premises rose 174%, while those at non-bank machines rose 317%, and are not expected to fall until new technology is more widely in place.

⁴⁶² Kitten, *ATM Skimming Threats Evolve*, above n 349.

⁴⁶³ Telford and Kulik, above n 445.

⁴⁶⁴ ConsumerReports.org, above n 44. See also Mohammed, above n 195, 216–7; Levi and Handley, above n 343.

⁴⁶⁵ Diebold Incorporated, *White Paper: Battling Card Fraud through Chip and PIN Technology*, above n 209, 2. See also Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 2–5.

⁴⁶⁶ Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, 'Final Report Model Criminal Code on Chapter 3 - Credit Card Skimming Offences' (2006)

When the consumer inserts his card into the card reader, the skimmer captures the card information before it passes into the ATMs card reader to initiate the transaction. The transaction continues in a normal fashion. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used the ATM. An inexpensive, commercially available skimmer can capture and retain account numbers and PINs for more than 200 ATM cards. Typically, criminals design skimming devices to be undetectable by consumers.⁴⁶⁷

Skimmer devices vary in size, shape and capabilities. As Masters and Turner have explained, they vary from ‘standalone pocket devices to devices that are incorporated into [the] keyboard’. Some skimmers are extensively used for legal purposes but some others are used for extravagant fraudulent activities. Masters and Turner further distinguished skimmer devices into three types, namely, basic skimmers,⁴⁶⁸ magnetic stripe card reader encoders,⁴⁶⁹ and re-packaged skimmers.⁴⁷⁰ Magnetic stripe card readers or skimmer devices are abundant in the marketplace, both in the brick-and-mortar and on-line world. Originally, skimmers were marketed for legitimate business retail purposes; however, because of their relatively small size, mobility/portability and user-friendly operation, they also have become increasingly used for fraudulent activities.⁴⁷¹

<[http://www.lawlink.nsw.gov.au/lawlink/SCAG/ll_scag.nsf/vwFiles/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf/\\$file/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf](http://www.lawlink.nsw.gov.au/lawlink/SCAG/ll_scag.nsf/vwFiles/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf/$file/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf)> 3; See also Mohammed, above n 195, 216–17.; Barwise and Bachfeld, above n 377.

⁴⁶⁷ Diebold Incorporated, ‘*White Paper: ATM Fraud and Security*’, above n 348, 2–5. According to Diebold Incorporated, there are three kinds of card skimming attacks that can occur:

- External card skimming – placing a device over the card reader slot (motorized or dip) to capture consumer data from the magnetic stripe on the card during a transaction. This is the most common form of card skimming.
- Internal card skimming – gaining access to the top hat of the ATM to modify the card reader or replace the original card reader with an already modified one for the purpose of obtaining consumer card data during a transaction.
- Vestibule card skimming – in locations where the ATM is located within a vestibule, skimmers are placed on the vestibule door card access reader to capture cardholder data from the *magstripe* where the card is read so an unwary consumer inserts their card into the vestibule instead of on the ATM.

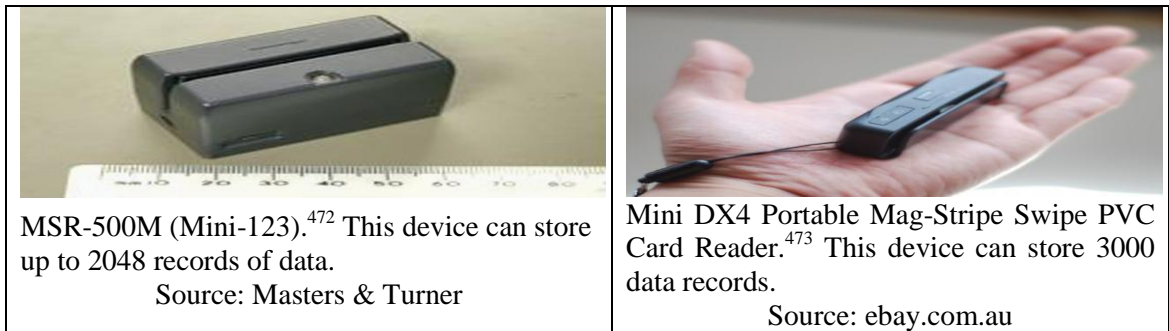
⁴⁶⁸ These basic skimmers are normally used by fraudsters to secretly capture consumer cards in restaurants or shops, by hiding them behind the desk or inside a pocket. When a consumer is distracted, the fraudster swiftly swipes the card in the skimmer. This mini skimmer generally only has the capability to capture and store magnetic card information. It does not have capability to encode or write the data onto a magnetic stripe card.

⁴⁶⁹ Unlike the basic skimmer that is normally only capable of reading and storing magnetic stripe information, magnetic swipe card encoders generally have greater capabilities, such as being able to read and write magnetic stripe data.

⁴⁷⁰ Masters and Turner, above n 216, 18.

⁴⁷¹ Ibid.

Figure 6: Mini Magnetic Stripe Card Reader



Magnetic swipe card encoders — besides being used to create magnetic stripe card for legitimate businesses, such as for hotel cards, retail shops and so on — are also usually used to create clone cards for unauthorised payment card transactions. This type of skimmer is able to write card skimming information onto new or used magnetic stripe card. Many variants of this kind of skimmer are available on the market.⁴⁷⁴

Figure 7: MSR206 Magnetic Swipe Encoder



Source: Masters and Turner⁴⁷⁵

Masters and Turner explain that repackaged skimmers are where fraudsters typically dismantle the skimmers from their standard manufactured packages and incorporate them into false ATM fascias and ATM slot adaptors.⁴⁷⁶ Further, they note that usually the fake fascias are of such quality that they exactly resemble a genuine part of the ATMs (especially on the user interface side). Only the reverse side of the fascias shows ‘the haphazard build quality’ (see Figures 8 and 9 below).⁴⁷⁷

⁴⁷² Ibid.

⁴⁷³ *Mini00 DX4 Portable Magnetic Stripe Swipe PVC Card Reader* (23 February 2013) ebay <http://www.ebay.com.au/itm/Mini00-DX4-Portable-Magnetic-Stripe-Swipe-PVC-Card-Reader-/251003524960?pt=AU_CashRegisterAccessories&hash=item3a70f9d760>. This mini DX4 can be bought online for around AUD200.00.

⁴⁷⁴ Ibid.

⁴⁷⁵ Masters and Turner, above n 216, 18.

⁴⁷⁶ Ibid.

⁴⁷⁷ Ibid.

Figure 8: The Extracted Components of a Mini-123 Card Reader Removed from its Manufactured Packaging and Repackaged for Use in a Fake ATM Fascia



Source: Masters & Turner⁴⁷⁸

Figure 9: Imitation ATM Fascia – Front and Rear View



Source: Masters & Turner⁴⁷⁹

Figure 10: Various ATM Skimmers on the ATM



Source: Brian Krebs⁴⁸⁰

Some skimmers are so advanced that they incorporate features such as the ability to send an SMS text message to the fraudster's mobile phone whenever a new card is

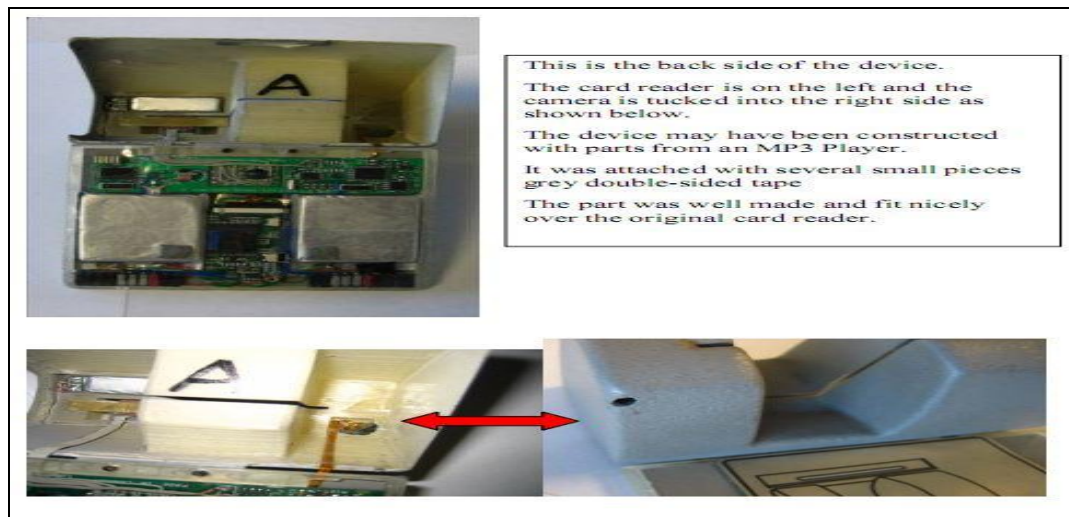
⁴⁷⁸ Ibid.

⁴⁷⁹ Ibid.

⁴⁸⁰ Brian Krebs, *ATM Skimmers, Part II* (2 February 2010) www.krebsonsecurity.com <<http://krebsonsecurity.com/2010/02/atm-skimmers-part-ii/>>. See also *Thieves Create More Sophisticated ATM Card Skimmers* (27 April 2012) Mashable <http://www.youtube.com/watch?v=_2H-_zAudn8>.

swiped,⁴⁸¹ so the fraudsters do not even have to dismantle the skimmer from the ATM in order to download the stolen data. Even now, many sellers offer tiny card readers (for example, the MSCR710) for purchase online. This tiny card reader, if used by fraudsters as a skimmer, will be of great benefit to them. Due to its tiny shape, it is easy to fit to any kind of case, has low power consumption, and greatly increased storage capability (data for up to 32,000 cards).⁴⁸² Even the seller acknowledges that the device can be used for illegal purposes and warns the potential buyers in its disclaimer (in red font) that the card reader is sold only for legal purposes and not for use as a card payment skimmer.⁴⁸³

Figure 11: Rear of an ATM Skimmer with SMS Capability



Source: Brian Krebs⁴⁸⁴

When the skimmer is installed in an ATM, the device then records and stores the electronic information from the magnetic stripe of the authentic payment cards as they

⁴⁸¹ Brian Krebs, *Would You Have Spotted the Fraud?* (15 January 2010) [www.krebsonsecurity.com <http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/>](http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/).

⁴⁸² For instance, mycardreader.com sells magnetic stripe card reader with interrupted swiping support with the size just width: 2mm, length: 6mm and height: 11mm, and costs 'only' USD1,500 each. See *MSCR710* (MyCardReader.com <<http://mycardreader.com/18-mscr710.html>>).

⁴⁸³ Ibid. See the disclaimer wording:

Disclaimer: Our magnetic card readers are intended for legal use only. Even though our magnetic card readers can be used as a debit or credit card reader and can read any type of magnetic stripe bank cards, we will not sell them to be used for skimming as debit or credit card skimmers.

The buyer understands that the *magstripe* card reader being purchased is not for illegal use. That he/she will safeguard the use and distribution of this device and make an effort to prevent illegal use from occurring.

We are not and will not commercialise this product if we know or suspect that it will be used for unlawful purposes.

⁴⁸⁴ Krebs, 'Would You Have Spotted the Fraud?', above n 481.

are inserted into the ATM slot.⁴⁸⁵ The data skimmed from a number of swiped cards is then stored in the skimmer device to be accessed or reproduced on a counterfeit card later.⁴⁸⁶ This data is then downloaded to a computer when the skimmer is dismantled, or the data can be sent to the fraudsters that reside near the ATM via a wireless network.⁴⁸⁷ Skimming of magnetic stripe information is a significant problem because it provides criminals with so much readily usable information for conducting unauthorised transactions.⁴⁸⁸

To combat the proliferation of ATM fraud using skimmer devices, most banks throughout the world (including in Indonesia at the encouragement of its central bank)⁴⁸⁹ choose to equip their ATMs' card reader slot with an anti-skimmer device. Generally, ATM anti-skimming devices take the shape of 'green or blue semi-transparent plastic casings that protrude from the card acceptance slot to prevent would-be thieves from easily attaching skimmers'.⁴⁹⁰

Figure 12: Anti-Skimming/‘Duck Snout’ at a Bank ATM in Sumatra (Indonesia)



Source: Sriwijaya Post/Syahrul Hidayat⁴⁹¹

⁴⁸⁵ Sullivan, 'The Changing Nature of US Card Payment Fraud', above n 262, 102–4. See also: Financial Fraud Action UK, above n 346, 28; Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 3; Diebold Incorporated, *White Paper: Battling Card Fraud through Chip and PIN Technology*, above n 209, 2.

⁴⁸⁶ Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 4–5.

⁴⁸⁷ Barwise and Bachfeld, above n 377.

⁴⁸⁸ Iannacci and Morris, above n 20, 61.

⁴⁸⁹ After the ATM skimming deluge in Indonesia in 2010 (described previously), Bank Indonesia encouraged all banks to enhance their ATM security to cope with the associated fraud and to compensate all bank consumers who lost their funds. Following BI's direction to improve ATM operational security, all the banks that were victims of recent ATM fraud became committed to implement a variety of increased security features, including (among others) the installation of PIN covers at ATMs, installation of anti-skimmer and 'jitter', as well as fitting CCTV cameras to ATM booths that did not already have CCTV in place.

⁴⁹⁰ Krebs, 'Green Skimmers Skimming Green', above n 354.

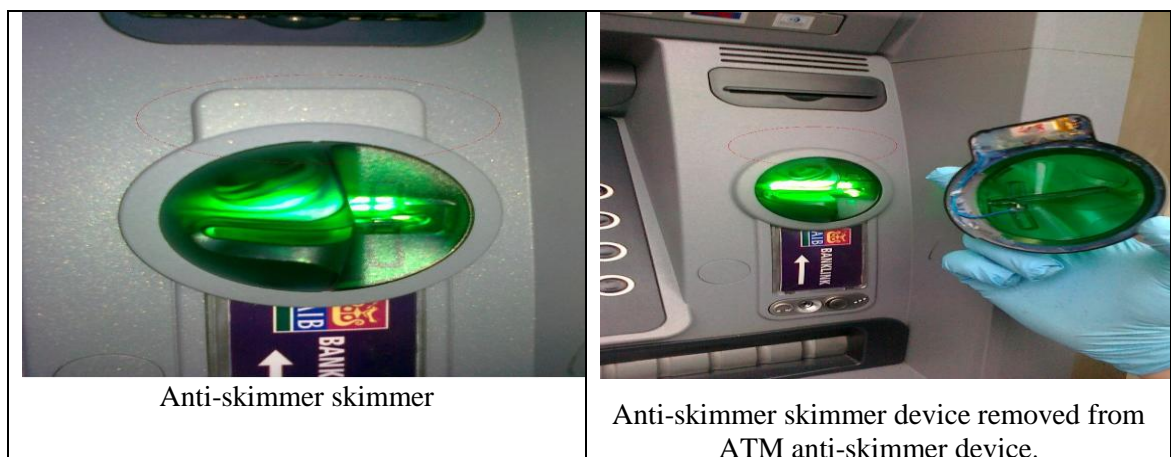
⁴⁹¹ Wahyu Satriani Ari Wulan, 'Inilah Ciri ATM Anti-'Skimming' [This is Typical ATM Anti-'Skimming']', *Kompas* (online), 22 January 2010 <<http://nasional.kompas.com/read/2010/01/22/12220871/Inilah.Ciri.ATM.Antiskimming>> .

However, the implementation of anti-skimming devices has not been without controversy. When banks first introduced anti-skimmer devices, the implementation was not accompanied by any consumer education. To make things even worse, a bank can have multiple brands of ATMs. As a result, the shape and colour of anti-ATM skimmers on the ATMs also vary.

Bank consumers are finally learning from the mass media or by ‘word of mouth’ that the ‘coloured plastic thing’ installed at an ATM card reader slot is actually an anti-skimmer device. However, fraudsters continually improve and modify their fraud techniques. In the case of ATM anti-skimming devices fraudsters have in no time circumvented them by devising ‘anti-skimmer skimmer’ devices (see Figure 13 below).

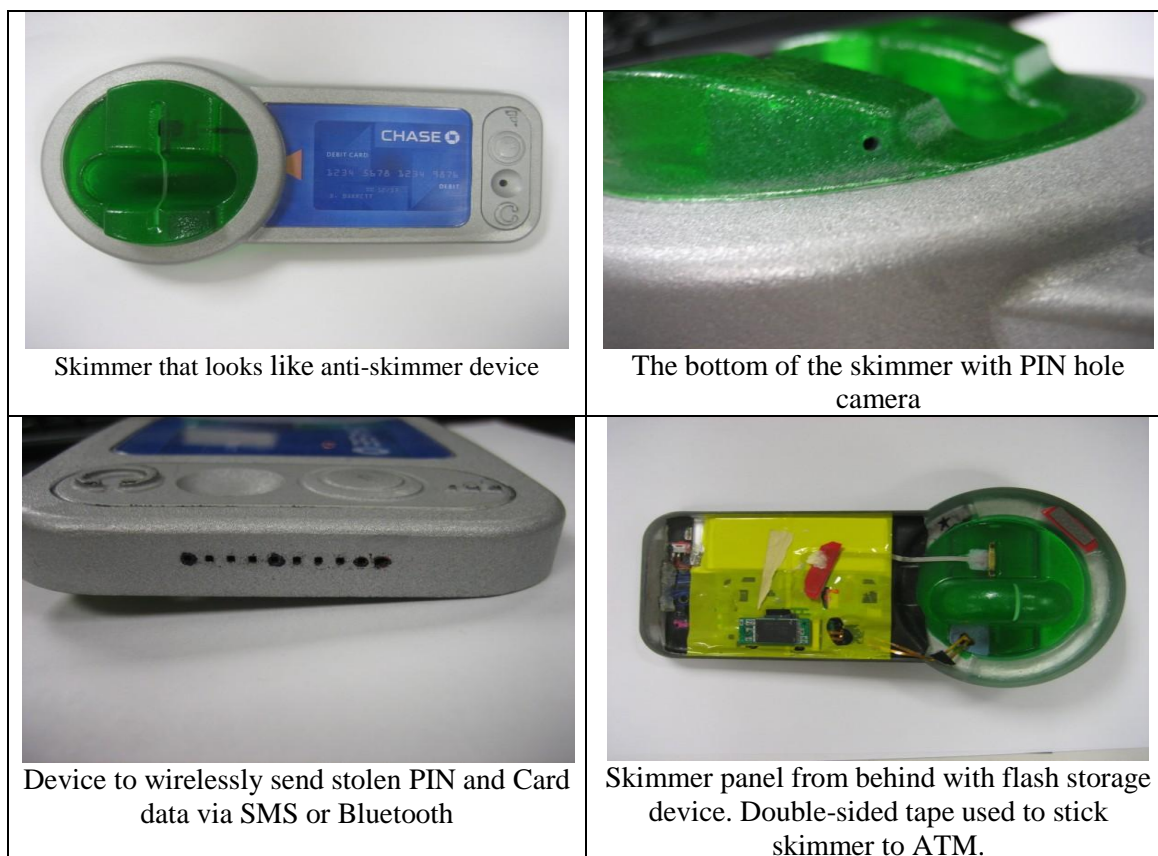
Now many fraudsters ‘simply [craft] their skimmers to look exactly like the anti-skimming devices’.⁴⁹² A skimmer found in a Chase Bank branch in West Hills (California), for example, was an ‘all in one’ skimmer (a skimmer that includes a magnetic stripe skimmer and also a pinhole camera device) designed to fit over the card acceptance slot. Authorities believe that this type of sophisticated, professional-grade ATM skimmer was made with the help of a 3D printer.⁴⁹³ Therefore, more consumers might be deceived by this new skimmer fraud since they believe that they have deliberately performed their ATM transactions at a secure ATM, just as was being encouraged by banks.

Figure 13: ATM Anti-Skimmer Skimmer and Skimmer



⁴⁹² Krebs, ‘Green Skimmers Skimming Green’, above n 354.

⁴⁹³ Brian Krebs, *Pro Grade (3D Printer-Made?) ATM Skimmer* (2011) <https://krebsonsecurity.com/2011/12/pro-grade-3d-printer-made-atm-skimmer/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+KrebsOnSecurity+%28Krebs+on+Security%29>.



Source: Brian Krebs⁴⁹⁴

In most cases, cardholders are frequently unaware that there is a skimming device on the consumer-activated terminal and their data has been stolen at the time of transaction. If a cardholder victim fails to check their bank statements frequently, a criminal can repeatedly withdraw money to the maximum limit every day until the account is drained or cancelled.⁴⁹⁵ When the consumer finally becomes aware, they have difficulty in pinpointing the timing and location of this skimming attack.⁴⁹⁶

Even though some banks have urged consumers to take precautions when conducting ATM transactions, nonetheless ‘customers are not sure what they are looking for when it comes to compromised machines, and a lot of the externally attached equipment is high quality and extremely subtle’.⁴⁹⁷

Furthermore, consumer vigilance is ineffective because there is also a wide variety of ATMs and anti-skimmer models, which make it impossible for consumers either to

⁴⁹⁴ Krebs, ‘Green Skimmers Skimming Green’, above n 354. See also Krebs, ‘Pro Grade (3D Printer-Made?) ATM Skimmer’, above n 493.

⁴⁹⁵ Kirk, ‘Criminals Turn to ‘Card Trapping’, above n 434.

⁴⁹⁶ Diebold Incorporated, *White Paper: Battling Card Fraud through Chip and PIN Technology*, above n 209, 2.

⁴⁹⁷ Walsh, above n 323, 10.

memorise the details for every ATM model or to immediately notice when there is a fraudster's device attached. As Barwise and Bachfeld argued, 'the untrained eye will hardly notice this mini-scanner, which is adapted to the ATM's design. Sometimes, the criminals even put a completely new front panel on the ATM.'⁴⁹⁸

2. Malware

An ATM basically is just an ordinary computer inside a custom-built case.⁴⁹⁹ Therefore, any attack that happens to an ordinary computer might also occur to an ATM computer. Unrestricted physical access to ATMs makes every ATM component — both outside and inside the ATM case — vulnerable to attack. Specifically about the vulnerabilities of ATM components inside the ATM cabinet, Telford and Kulik observe that:

The components inside the locked ATM cabinet, but outside the safe, are also vulnerable to compromise from both hardware and software attacks such as plugging in a USB or even a DVD drive, replacing components inside the ATM — even removing the ATM computer and replacing it with an attacker's computer. Physical access allows any software or hardware component to be replaced; protecting physical access to ATMs starts with security of the site and use of unique keys for ATM cabinets.⁵⁰⁰

Fraudsters now have infected ATMs with malware in an attempt to steal consumer payment card data and PIN.⁵⁰¹ For some fraudsters, planting malware in the ATMs seems to be more rewarding with less risk compared to ATM skimming that has been very popular among fraudsters.⁵⁰² An instance of ATM malware was found on 20 machines in Russia and the Ukraine that were all running Microsoft Windows XP operating system.⁵⁰³

Trustwave's SpiderLabs that was ordered to analyse malware found in Eastern European ATMs, revealed that:

⁴⁹⁸ Barwise and Bachfeld, above n 406.

⁴⁹⁹ *How ATM Machines Work* (2013) eHow tech <http://www.ehow.com/how-does_4564295_do-atm-machines-work_.html>; Kylene Arnold, *Parts of an Automatic Teller Machine* (2013) eHow Money <http://www.ehow.com/info_8322362_parts-automatic-teller-machine.html>. See also Arnold, above n 499.

⁵⁰⁰ Telford and Kulik, above n 445.

⁵⁰¹ Danny Bradbury, 'A Hole in the Security Wall: ATM Hacking' (2010) 2010(6) *Network Security*, 13. See also Jeremy Kirk, *ATM Malware Spreading Around the World* (2009) <http://www.cio.com/article/494341/ATM_Malware_Spreading_Around_the_World>.

⁵⁰² Kim-Kwang Raymond Choo, 'The Cyber Threat Landscape: Challenges and Future Research Directions' (2011) 30(8) *Computer & Security* 719, 722.

⁵⁰³ Zetter, above n 371. See also Bradbury, above n 501, 13. The malware was compiled using the Delphi Programming language developed by Borland. It installs itself as a Windows service, then injects itself into Windows system messaging process. It looks for transactions taking place in the machine, and checks for track two data, collects it and stores in a Windows directory for later retrieval.

The malware captures magnetic stripe data and PIN codes from the private memory space of transaction-processing applications installed on a compromised ATM. The malware contains advanced management functionality allowing the attacker to fully control the compromised ATM through a customized user interface built into the malware. This interface is accessible by inserting controller cards into the ATM's card reader. SpiderLabs analysts do not believe the malware includes networking functionality that would allow it to send harvested data to other, remote locations via the Internet. The malware does, however, allow for the output of harvested card data via the ATM's receipt printer or by writing the data to an electronic storage device (possibly using the ATM's card reader). Analysts also discovered a code indicating that the malware could eject the cash-dispensing cassette.⁵⁰⁴

Recently, ATMs have often used publicly available operating systems such as Microsoft Windows XP operating system and 'off the shelf' hardware. As a consequence, besides their benefits of efficiency and interoperability, ATM computers are susceptible to being infected with malware. The malware can be injected into an ATM via network or through other infected devices (such as a USB attack). Once installed on the ATM, the malware can collect card information and PINs.⁵⁰⁵

According to the FFIEC, malicious codes or programs (malware) are 'any program that acts in unexpected and potentially damaging ways'. Common types of malware are 'viruses, worms, Trojan horses, monitoring programs such as spyware, and cross-site scripts'.⁵⁰⁶ Malware has constantly been ranked as one of the key cyber risks to business, governments and individuals.⁵⁰⁷ Evidence of the increasing malware threat are statistics cited by Symantec, which reported that malware numbers skyrocketed from just under 2.9 million in 2009 (a 71 per cent increase over 2008) to 286 million new malware variants detected by Symantec in 2010.⁵⁰⁸

⁵⁰⁴ Trustwave, *Automated Teller Machine (ATM) Malware Analysis Briefing* (28 May 2009) [www.wired.com <http://www.wired.com/images_blogs/threatlevel/2009/06/trustwave-security-alert-atm-malware-analysis-briefing.pdf>](http://www.wired.com/images_blogs/threatlevel/2009/06/trustwave-security-alert-atm-malware-analysis-briefing.pdf)

⁵⁰⁵ Mohammed, above n 195, 221–2. See also Telford and Kulik, above n 445. Bradbury, above n 501, 13.

⁵⁰⁶ FFIEC, *Information Security*, above n 202, 61. FFIEC further asserts that some of the effects of malware are that it can:

- Replicate itself within a computer and transmit itself between computers.
- Change, delete, or insert data, transmit data outside the institution, and insert backdoors into institution systems.
- Attack institutions at either the server or the client level.
- Attack routers, switches, and other parts of the institution infrastructure.

Malicious code can also monitor users in many ways, such as logging keystrokes and transmitting screenshots to the attacker.

⁵⁰⁷ Choo, above n 502, 721.

⁵⁰⁸ Ibid.

Malware (such as root kits) is software that is able to access a computer without being noticed by the computer administrator by subverting the computer's standard operating system functionality. Malicious code attacks are a growing problem because they are deeply hidden and thus very difficult to detect and remove. Malware can steal and collect personal information about users without their consent.⁵⁰⁹ Banks, as electronic banking providers, can prevent or detect and remove malicious codes on their computer (at host and network level) only by implementing appropriate centralised anti-virus software.⁵¹⁰

The perpetrator that uses malware to infect systems can be anyone, ranging from outside intruders that have forced access to the computer, or authorised users.⁵¹¹ Zetter argues that typically a malware attack needs a collaborator from among authorised ATM personnel, such as an ATM technician or anyone else with an access key to the ATM, so that fraudsters are able to place the malware on the ATM.⁵¹² In terms of where the malware are installed, Bradbury contends that the installation of such malware could happen at the factory when the device was programmed, or at the premises where it is used. There is also the possibility that malware could also be installed remotely.⁵¹³

Further, Telford and Kulik note that every ATM has an administrator.⁵¹⁴ Often, the ATM administrator's job is accomplished either by physical service interface at the ATM, or, as is the most recent development, through remote management tools. Aside from this, the developers of the ATM software itself also have a big opportunity to 'control the operation of an ATM, and could write software to change screen flow or

⁵⁰⁹ Symantec, 'Internet Security Threat Report : 2011 Trend' (www.symantec.com, 2012) <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf> 32. According to Symantec, the current front runners in the rootkit arena are Tidserv, Mebratix, and Mebroot. These all modify the master boot record (MBR) on Windows computers in order to gain control of the computer before the operating system is loaded. Variants of Downadup (aka Conficker), Zbot (aka Zeus), as well as Stuxnet all use rootkit techniques to varying degrees.

⁵¹⁰ Kondabagil, above n 194, 110–11. See also Anderson et al, above n 338, 9–11. According to Anderson et al, 'most malware tools are not initially detected by the common antivirus products, as their authors test them against these products; and when the antivirus vendors do catch up, the *crimeware* authors issue updates'.

⁵¹¹ Kondabagil, above n 194, 110–11. See also Anderson et al, above n 338, 9–11.

⁵¹² Zetter, above n 371. See also Bradbury, above n 501, 13; Choo, above n 502, 723.

⁵¹³ Bradbury, above n 501, 13.

⁵¹⁴ Administrators are trusted people who can install software, configure devices, manage accounts and establish security policies, and handle the other management tasks associated with keeping the ATM operational. See Telford and Kulik, above n 445.

content, capture PINs, or access other confidential information’.⁵¹⁵ As a result, fraudulent ATM administrators or developers of ATM software can circumvent every security measure aimed to prevent uploading of malicious code/software, or could compromise encryption processes and introduce a ‘back door’ for remote access to ATM system files.⁵¹⁶

Concerning the huge impact of malware on ATMs, Trustwave strongly recommends that all financial institutions with ATMs perform an analysis of their ATMs to identify whether or not malware is present.⁵¹⁷ The finding that the malware was moving to machines in the United States and elsewhere also triggered this recommendation. They also believed that fraudsters tend to use a fraud method in one country as a trial. If it is successful and the perpetrators realise that it can also be executed in other countries, it will spread quickly.⁵¹⁸

However, despite massive reports of malware on ATMs, many financial institutions and banks in many countries have been reluctant to invest in proper actions to cope with this threat. There is even an allegation that some financial institutions and banks have a tendency to install illegal and insecure software, which might further increase security risk.⁵¹⁹

In a recent development, malware not only was used to attack ATMs but also EFTPOS terminals. Fraudsters are attacking payment processors and merchants with enhanced malware to compromise payment card data. Much of the latest malware has the capability to evade anti-virus systems. An example of this malware is ‘Dexter’, a 2012 Trojan that infected hundreds of POS systems, mainly in the United States and United Kingdom. This malware looked for card data while lying in the memory of the EFTPOS terminals.⁵²⁰

⁵¹⁵ Ibid.

⁵¹⁶ Ibid.

⁵¹⁷ Trustwave, above n 504, 6.

⁵¹⁸ Zetter, above n 371.

⁵¹⁹ Tracy Kitten, *Illegal ATM Software to Blame for Most ATM Hacks, Solution Provider Says* (28 July 2009) ATM Marketplace <<http://www.atmmarketplace.com/article/128364/Illegal-ATM-software-to-blame-for-most-ATM-hacks-solutions-provider-says>>.

⁵²⁰ Tracy Kitten, *Enhanced Malware Targets Retailers: Stored Card Data on Networks, POS Systems Primary Target* (2013) Bank Info Security <<http://www.bankinfosecurity.com/enhanced-malware-targets-retailers-a-5604?rf=2013-03-13-eb&elq=fe6911eb340477d8853befa86ada91c&elqCampaignId=6124>>. Securelet, an online security firm, is quoted explaining how Dexter works, as follows:

Based on interviews with some of Indonesia's bank officials responsible for the development of ATMs, banks so far have no anti-malware software. As a result, they lack the ability to prevent the installation of or detect malware on ATMs. It was quite surprising that some officers admitted that they 'did not even know' about the possibility of malware attack on ATMs. If these interview results are accurate, it reflects the banks' poor risk management efforts in relation to keeping abreast with fraud risk developments. As a result, banks may fail to realise that there are many possibilities of phantom withdrawals caused by malware on ATMs, and blame consumers whenever phantom withdrawals occur.⁵²¹ The *Body Shop* case fraud that occurred in 2013 is evidence that malware attack on ATM/debit card operations has arrived in Indonesia.⁵²²

4.2.1.3.3. Magnetic Stripe Card Data Theft at EFTPOS Terminals

1. Card Skimming and EFTPOS Terminal Tampering

Consumer data breach at merchants comprises a huge problem for financial institutions, because merchants or their employees are outside the bank's 'perimeter' and relatively unsupervised by banks (that is, the banks do not directly monitor them). Hence, according to Grabosky, Smith and Dempsey, 'merchants or their employees are ideally placed to permit access to computer networks and to alter transaction details'.⁵²³

EFTPOS terminals at merchants are relatively protected from outsiders who are not authorised to have access (protected by the building, locked doors, and oversight by employees of the merchant). However, recently, skimmers have been found to break into shops more frequently and add skimming devices to legitimate EFTPOS terminals.⁵²⁴ Although relatively insulated from outside attack, EFTPOS terminals do not have protection from insiders (such as the retailers themselves, clerks, cashiers, sales personnel, and so on) who are authorised to have access to the terminals but have turned into fraudsters.

Dexter was targeting retailers, hotels and restaurants. Dexter exploited remote-access controls to infiltrate POS systems and capture screenshots of POS displays Once a terminal was infected, the malware stole transactional processing lists and parsed the memory for Track 1 and Track 2 data stored on payment cards' magnetic stripes. [at 2].

⁵²¹ Interviews with various bank officers responsible for ATM operations: BO-1; BO-2; BO-3; and BO-4.

⁵²² Edward Pangabea, *Modus yang Dipakai si Pembobol Kartu Kredit di Gerai Body Shop* [Modus Operandi Employed by Credit Card Theft Perpetrator in Body Shop Merchant] (31 May 2013) Liputan6.com <<http://bisnis.liputan6.com/read/601128/modus-yang-dipakai-si-pembobol-kartu-kredit-di-gerai-body-shop>>.

⁵²³ Grabosky, Smith and Dempsey, above n 266, 24.

⁵²⁴ Barwise and Bachfeld, above n 377.

However, there are also many reports where an outsider could compromise merchants' EFTPOS terminals by covertly replacing the merchants' EFTPOS terminals with ones that have been tampered with either by 'break and entry' when the business is closed, or by fraudsters tricking the owner or staff into allowing the installation of the fraudsters' bogus 'replacement' or 'upgraded terminal' by pretending to be a bank's or relevant third party's maintenance service officers.⁵²⁵

In recent years, merchants and acquirers/processors have become a point of compromise for hundreds of millions of payment card accounts.⁵²⁶ According to Javelin Strategy and Research, counterfeit payment cards have become one of the fastest growing card frauds. Fraudsters are breaking into payment card information from insecure and compromised merchant terminals (hacking into terminals at hotels, restaurants, petrol stations and other merchants, and obtaining consumer data).⁵²⁷

Merchants often become the perfect place to commit a crime such as accessing computer networks, altering transaction details,⁵²⁸ and skimming or intercepting payment card details from EFTPOS terminals.⁵²⁹ EFTPOS terminals are frequently abused in this manner, with or without the involvement of the merchant owner. In general, cardholders also do not realise when their cards are being attacked.⁵³⁰

In order to obtain consumer payment card information, fraudsters can install fake equipment to steal card information from the entry process. For instance, fraudsters can

⁵²⁵ See, e.g. Australian Crime Commission, *Banks, Law Enforcement and Retailers Warn Merchants to Secure EFTPOS terminals to Prevent Skimming* (2010) <<http://www.crimecommission.gov.au/media/banks-law-enforcement-and-retailers-warn-merchants-to-secure-eftpos-terminals-to-prevent-skimm>>; Andrew Koubaridis, 'EFTPOS Skimmers: 4 Arrests in Scam', *New Zealand Herald* (online), 10 April 2012 <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10797766>.

⁵²⁶ Saville and Loomis, above n 297, 5. See also Grabosky, Smith and Dempsey, above n 266, 24.

⁵²⁷ Javelin Strategy & Research, '2010 LexisNexis True Cost of Fraud Study', above n 334, 21. See also Sullivan, 'The Changing Nature of US Card Payment Fraud', above n 262, 102–104; Bell, above n 44; Drimer, Murdoch and Anderson, 'Thinking inside the Box', above n 345; Tedder, above n 44, 9.

⁵²⁸ Grabosky, Smith and Dempsey, above n 266, 24. See also Hidayatul Fajri, 'Kasir Restoran Bobol ATM, Rp 123 Juta Raib [Cashiers Restaurant Stole ATM, Rp123 Million Drained]', *Kompas* (online), 8 May 2012 <<http://megapolitan.kompas.com/read/2012/05/08/17564064/Kasir.Restoran.Bobol.ATM..Rp.123.Juta.Raib>>; Gede Suardana, *Pembobolan Rekening Nasabah: Mesin Pembayaran BCA di Hard Rock Hotel Bali Diganti [Consumers' Account Theft: BCA EFTPOS Machine at Hard Rock Hotel Bali Replaced]* (2010) Detik.com <<http://news.detik.com/read/2010/01/20/230403/1282860/10/mesin-pembayaran-bca-di-hard-rock-hotel-bali-diganti?nd771104bcj>>.

⁵²⁹ Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 1. See also the Smart Card Alliance, 'Fraud in the US Payments Industry', above n 297, 14.

⁵³⁰ Barwise and Bachfeld, above n 377. See also the Smart Card Alliance, 'Fraud in the US Payments Industry', above n 297, 14.

replace the PIN pad and terminal with devices that will display, print and/or record the entered values.⁵³¹ An example of this EFTPOS device-tampering scheme befell Michaels Stores Inc in Chicago (United States).⁵³² In this fraud incident, the fraudsters replaced legitimate EFTPOS PIN pads with ones that had been tampered with. The breach affected 90 Michaels stores in 20 states, stretching from Rhode Island to Washington, and opened the debate about which party should be liable for the fraud loss.⁵³³ As a precautionary measure, Michaels have removed some 7,200 PIN pads from most of its 964 US stores.⁵³⁴

Another interesting example, still in the United States, was an EFTPOS skimming attack on Save Mart, the Modesto (California) based grocery chain. Save Mart admitted that the skimming attacks that targeted the self-service checkout terminals at 24 Save Mart and Lucky Supermarkets in the San Francisco Bay area were believed to have exposed hundreds of consumer accounts to debit and credit card fraud. For security purposes, Save Mart has replaced or inspected all of its 2,557 EFTPOS terminals, which include self-checkout and staffed checkout lanes.⁵³⁵

However, unlike the Michaels EFTPOS breaches, which were detected by card issuer neural networks systems, the Save Mart breach was uncovered during a routine maintenance check.⁵³⁶ This demonstrates the important fact that only trained maintenance officers are able to distinguish a 'good' EFTPOS terminal from one that has been tampered with. Neither staff nor consumers could do so; the terminals were indistinguishable. Hence, it can be assumed that even the most vigilant consumers will

⁵³¹ See Mohamad, above n 302, 11.

⁵³² Tracy Kitten, *3 Tips to Foil POS Attacks* (2011) Bank Info Security <<http://www.bankinfosecurity.com/3-tips-to-foil-pos-attacks-a-3617>>.

⁵³³ Tracy Kitten, *Michaels Breach: Who's Liable?* (22 May 2011) Bank Info Security <<http://www.bankinfosecurity.com/michaels-breach-whos-liable-a-3668>>.

⁵³⁴ Tracy Kitten, *Michaels Breach Bigger than Reported* (12 May 2011) Bank Info Security <http://www.bankinfosecurity.com/articles.php?art_id=3628&rf=2011-05-14-eb>. Another example is from Perth (Australia), where in 2009 POS devices were replaced by skimmers at McDonalds franchises in a POS swap that defrauded 3500 customers of over AUD5 million: Joseph Sapienza, 'Police Arrest Two in EFTPOS Skimming Fraud' *Brisbane Times* [WA News section], 22 December 2009 <<http://www.brisbanetimes.com.au/wa-news/police-arrest-two-in-eftpos-skimming-fraud-20091222-lbcz.html>>. Although the EFTPOS swap was conducted in Perth, monies were withdrawn in the eastern states and overseas.

⁵³⁵ Tracy Kitten, *Grocer Confirms POS Skimming Attack: Customers, Card Issuers Watch for Fraudulent Activity* (4 January 2012) Bank Info Security <http://www.bankinfosecurity.com/articles.php?art_id=4376&rf=2012-01-04-eb&elq=6f859884d23941cab391ff197d886b3c&elqCampaignId=1109>.

⁵³⁶ Ibid.

not be able to notice the possibility of fraud, since the passive skimming attack at EFTPOS terminals will not compromise the smooth operation of EFTPOS transactions.

Interestingly, even for countries that have already migrated to EMV chip and a PIN standard, this does not mean that the EFTPOS terminals will be free from fraud. Using PIN pad swap or POS swipe schemes, fraudsters can disable the part of the EFTPOS terminals that read the chip on consumer cards, so the consumer is then forced to swipe the magnetic stripe into the EFTPOS terminal to make a transaction. This is where the consumer's card data is then stolen by the tampered with EFTPOS terminal.⁵³⁷ In some cases, magnetic stripe data is transmitted wirelessly to criminals who are waiting nearby.⁵³⁸

In ATM/debit card fraud, a merchant owner can independently operate as a point of compromise, or conspire with criminal organisations to orchestrate a fraud attack. If they operate independently, merchants can mount 'waiter attacks' in face-to-face transactions or abuse consumer magnetic stripe data during merchant transactions.⁵³⁹ Mobile handheld skimmers can be hidden inside a waiter's pocket, or mounted underneath a cashier's desk.⁵⁴⁰ This fraud method is also called 'wedge skimming'.⁵⁴¹ If colluding with strong criminal organisations, merchants can facilitate attacks using fake or modified EFTPOS terminals and tapping both cardholder magnetic stripe card data and PIN.⁵⁴²

There are also many occasions where a merchant's cashiers are involved in the fraudulent skimming process. Generally, cashiers (who get paid for working with the skimmers) first swipe the consumer's card into the EFTPOS terminal, and while the

⁵³⁷ Kitten, *3 Tips to Foil POS Attacks*, above n 532. See also Linda McGlasson, *Top 4 Skimming Threats: From Hand-Held POS Devices to Dummy ATMs* (2010) Bank Info Security <<http://www.bankinfosecurity.com/top-4-skimming-threats-a-3054>>.

⁵³⁸ Tracy Kitten, *POS Skimming Scam Stopped* (2 May 2011) Bank Info Security <<http://www.bankinfosecurity.com/pos-skimming-scam-stopped-a-3592>>.

⁵³⁹ 'Waiter attack' is one type of eavesdropping attack that is common at points of sale such as restaurants, petrol stations, shops and so on, where the waiter or other staff member, while taking the consumer's card for use for payment at an EFTPOS terminal, writes down the financial data embossed on the front of the card, such as the card's brand and issuer, cardholder's name, PAN, and expiration date. Instead of taking notes, the staff member also can copy a consumer's card data using a handheld skimmer.

⁵⁴⁰ Levi and Handley, above n 343. There can be a problem of merchants who are involved in fraudulent activities, the risk of which is increased by the soaring turnover rate of staff. Some may be serial fraudsters who are connected to criminal organisations. See also Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 5.

⁵⁴¹ Siciliano, above n 455.

⁵⁴² Radu, above n 210, 33.

consumer is distracted and not paying attention to the cashier or their card, the cashier swipes the card for a second time but on the fraudsters' skimmer.⁵⁴³ The cashier also registers the consumer's PIN, for example by asking the consumers to repeat the entry on the skimming device.⁵⁴⁴ Another method is simply one where cashiers just observe the consumer entering their PIN at the PIN pad ('shoulder surfing').

2. Card 'Double Swiping': Merchant's Cash Register/Computer Abuse

In Indonesia, most EFTPOS terminals do not have a PIN pad shield. Instead of being mounted on the bar and facing the consumer's side in front of cashier's desk, EFTPOS terminals generally are lying on the counter and the persons who swipe the card into the EFTPOS terminal are the cashiers themselves instead of the consumers. Even worse, sometimes an EFTPOS terminal is located under the cashier's table, hence, out of sight of consumers. These practices are very different to those of other countries such as Australia.⁵⁴⁵

The practices in Indonesia (as mentioned above) are particularly vulnerable to fraud committed by merchant cashiers. By holding the consumer's card for some time, rogue employees can use a covert and mini hand-held skimmer hidden behind the counter to steal the consumer's card data ('wedge skimming'). The unshielded PIN pad and the positioning of the EFTPOS terminal on the counter make it easy for a rogue employee or cashier to steal customer PINs by shoulder surfing. This unfortunate situation is also exacerbated by consumers' behaviour as they often do not even attempt to cover the PIN pad when they enter their PIN.⁵⁴⁶

⁵⁴³ See *Bobol Data ATM, Dua Kasir Mall Ditangkap* [ATM Data Theft, Two Mall Cashiers Busted] (24 November 2011) [Beritadewata.com <http://beritadewata.com/Hukum_dan_Kriminal/Kriminal/Bobol_Data_ATM,_Dua_Kasir_Mall_Ditangkap.html>](http://beritadewata.com/Hukum_dan_Kriminal/Kriminal/Bobol_Data_ATM,_Dua_Kasir_Mall_Ditangkap.html).

⁵⁴⁴ Barwise and Bachfeld, above n 377. See also Albrecht et al, above n 368, 535–6;

⁵⁴⁵ In many countries, including Australia, generally after consumers hand over the purchased goods to a cashier, that person then scans or enters the price of the goods and asks the customer to independently swipe or insert their payment card into the merchant's EFTPOS terminal to enable a payment transaction to occur. Most of the EFTPOS terminals are equipped with a PIN pad shield and mounted on a stick or pole facing the consumers almost vertically, making it nigh impossible for the cashier to 'shoulder surf' to obtain the consumer's PIN. Double swiping the consumer's card into a cash register computer is not common in these countries. From the information security viewpoint, these practices are highly regarded because they can reduce the likelihood of the occurrence of waiter or cashier attack using a hand-held skimmer (because card has never left consumer's hand in the Australian scenario above), and of PIN theft using the shoulder surfing method or a pinhole camera (due to the orientation and protection of the key pad from the cashier's line of sight).

⁵⁴⁶ See Smart Card Alliance, 'Fraud in the US Payments Industry', above n 297, 14.

To further complicate matters, after swiping a consumer's card in the merchant's EFTPOS terminal, most merchant cashiers in Indonesia 'double-swipe' the payment card into merchant's card reader in their cash register computer.⁵⁴⁷ One of the reasons for this insecure but 'legitimate' practice is to speed up reconciliation between payment transaction data in EFTPOS and the merchant record in their cash register system.⁵⁴⁸

From the information security perspective, swiping consumer cards into merchant cash register computers is very dangerous.⁵⁴⁹ Consumer debit card data stored in the merchant computer is vulnerable to data breach, especially due to internal fraud. Devos and Pipan note that in relation to administration, fund transfer information and further reference, most of the parties involved in the payment card system keep track of and store the cardholder transaction data. Indeed, according to them, 'this data is vulnerable and if stolen the data can be used to conduct fraudulent transactions or to produce fake cards'.⁵⁵⁰ There have been cases in big cafes in Bali where clerks or cashiers, using a mobile phone camera 'snap' an image of the consumer's card data as it appeared on the cash register's monitor when the card was swiped at the merchant's cash register computer.⁵⁵¹

Based on an interview with Sabu (Halo BCA Division Head, Bank Central Asia, who was also involved in the investigation and apprehension of fraudsters), one manner in which fraudsters capture consumer ATM/debit card information from a merchant's cash register monitor is as follows: when a consumer's card is swiped in a merchant's cash register computer, the magnetic stripe information (in all tracks) that appear in cash

⁵⁴⁷ 'Double swiping' here does not refer to the conduct of merchant cashiers that swipe consumers payment card twice in the EFTPOS machine for one transaction. Instead, 'double' in this sub-section refers to the common practice in almost all merchants in Indonesia where merchant cashiers after dipping or swiping a consumer's card in the EFTPOS machine to enable payment transactions, also then swipe it again to the merchant's cash registers to deliberately capture consumers' payment card magnetic stripe data for merchant reconciliation purposes

⁵⁴⁸ Rezkiana Nisaputra, *Visa Siap Amankan Transaksi Kartu Kredit di Indonesia* [Visa Ready to Safeguard Credit Card Transactions in Indonesia] (24 May 2013) Okezone.com <<http://economy.okezone.com/read/2013/04/03/457/785755/visa-siap-amankan-transaksi-kartu-kredit-di-indonesia>>.

⁵⁴⁹ 'Waspada Data Skimming Pada Cash Register [Allert on Data Skimming on Cash Register]' on BANKINFOSECURITY: SEC_RITY is not complete without 'U' <<http://bankinfosecurity.wordpress.com/2012/06/23/wasapadai-data-skimming-pada-cash-register/>>.

⁵⁵⁰ Devos and Pipan, above n 297, 3–4.

⁵⁵¹ See Gede Suardana, *Kasir Mall di Bali Terlibat Jaringan Pembobol ATM* [Mall Cashier in Bali Involved in ATM Fraudster's Network] (24 September 2011) detiknews <<http://news.detik.com/read/2011/11/24/172907/1775045/10/kasir-mall-di-bali-terlibat-jaringan-pembobol-atm>>; *Empat Pembobol ATM Diadili* [Four ATM Thieves Prosecuted] (27 Agustus 2012) Natanews: Dimensi Baru Informasi <<http://www.natanews.com/521/empat-pembobol-atm-diadili/>>.

register monitor are captured by a fraudster cashier using a mobile phone camera. The consumer's PIN is obtained by the corrupt cashier 'shoulder surfing' and memorising the number entered when the consumer enters their PIN in the EDC PIN pad located at the cashier's desk. Later, fraudsters use this data to create a counterfeit card and withdraw consumer's money from ATMs.⁵⁵²

A more sophisticated and massive payment card fraud involving a merchant's cash register has more recently occurred in Indonesia. In early March 2013, payment card data theft (identity theft) occurred at several Body Shop merchants in Jakarta and Padang (Indonesia) and compromised hundreds of bank consumers' payment cards (such as credit cards and debit cards) from Mandiri Bank and BCA. Most probably, this breach happened because Body Shop merchants implemented the common practice of 'double swiping' for payment card transactions — one swipe to the EFTPOS machine, and another swipe to the merchant's cash register.⁵⁵³

According to the Indonesian Credit Card Association, around 200 payment cards were counterfeited and more than 10,000 cards blocked and replaced by the affected banks due to this breach.⁵⁵⁴ The subsequent identity fraud in the form of unauthorised transactions occurred in foreign countries such as the United States, Mexico, the Philippines, Turkey and Malaysia.⁵⁵⁵ Again, this shows that international actors were also involved in the Indonesian Body Shop case.

However, it is believed that fraud like the Body Shop case has not only happened recently. Many fraud incidents have been left unsettled, or settled privately between the parties involved, where the incident was never reported to the authorities or in the media.

Long before the Body Shop case occurred, in 2007, the author raised this concern informally with several high ranking officers at Bank Indonesia and at the author's issuing bank (which is also an acquiring bank), and via one fraud discussion group

⁵⁵² Interview with Nathalya Wani Sabu, Division Head Halo BCA, PT Bank Central Asia, Tbk (Jakarta, 14 August 2012).

⁵⁵³ Martha Thertina and R R Ariyani, 'YLKI: *Regulasi Kerahasiaan Data Pribadi Mendesak* [YLKI: Privacy Regulation is Urgent]', *Koran Tempo* 5 April 2013, B2.

⁵⁵⁴ Martha Tertina and Rhama T W, '*Merchant Dilarang Double Swipe Kartu Pembayaran* [Store Prohibited Double Swipe Payment Cards]', *Koran Tempo* 15 April 2013, B2.

⁵⁵⁵ Maftuhah, *Pencurian Data Body Shop Terjadi di Jakarta & Padang*, above n 37.

mailing list.⁵⁵⁶ However, no attention was paid to this by either the regulator or the bank. Specific reasons for this inaction came from the bank when the author inquired: firstly, the bank needed merchants for their business; and secondly, to some extent, the merchants (especially big merchants) have more bargaining power than the bank in determining the terms and conditions of their relationship.

Even though double swipe to the merchant's cash register has occurred for quite some time in Indonesia, so far there has been no regulation by the payment system authority in Indonesia to ban merchants from double swiping consumer cards in their cash register computers. The Body Shop case was 'a blessing in disguise' because it opened the eyes of many policy makers in the Indonesian payment industry to the need to eliminate the 'clear and present danger' of double swiping practices.

The Indonesian Credit Card Association (AKKI) has proposed that Bank Indonesia as the payment system regulator should enact regulation in regard to the practice.⁵⁵⁷ Although the legal relationship between the store and the acquirer bank is created in the merchant agreement, there is no clause in the agreement that prohibits this practice. In general, even the bank does not perform an audit of the store's computer system nor are there any requirements regarding the merchant's treatment of bank consumers' data, leaving the consumers' data and their funds in jeopardy.

However, following the Body Shop case, Bank Indonesia as Indonesia's payment system authority, sent a letter on 8 April 2013 to all credit card and ATM/debit card issuers and acquirers entitled 'Security Enhancement on Credit Card/Debit Card Transactions'. The thrust of the letter was to urge banks and other financial institutions to improve their supervision of merchants by forbidding them to practise double swiping. Merchants who infringe such a ruling would be put on a black list of merchants.⁵⁵⁸

⁵⁵⁶ See evidence of the author's concern regarding 'double swiping' in email messages that can be retrieved from: Iwan Setiawan, *Data Fraud Kartu Pembayaran Perbankan* [Banking Payment Card Fraud Data] (2007) Yahoo!Groups <<http://groups.yahoo.com/group/BI-Cyclist/message/235>>.

⁵⁵⁷ Gina Nur Maftuhah, *Salahi Aturan, Pencurian Data di Body Shop Langsung di Stop* [Violates the Rules, Data Theft in the Body Shop was Stopped Immediately] (25 March 2013) Okezone.com <<http://economy.okezone.com/read/2013/03/25/457/780892/salahi-aturan-pencurian-data-di-body-shop-langsung-di-stop>>.

⁵⁵⁸ Bank Indonesia unpublished letter No 15/224/DASP on 8 April 2013. Unlike Bank Indonesia regulations that have 'enforcing power' especially on the bank, in contrast, Bank Indonesia 'letters' only have the effect of 'moral suasion' and hence there is no sanction if banks do not abide by it. The

Bank Indonesia's letter was not a regulatory measure. It was meant only to have the force of moral persuasion from the payment system authority to the banking industry. Therefore, there was to be no legal sanction to be imposed on banks or merchants who did not comply with the ruling contained in the letter. Steve Martha, AKKI General Manager, was a little sceptical about Bank Indonesia's letter on double swiping. There have also been concerns in the industry, that if the central bank's ruling is implemented, the stores/merchants may be unwilling to accept card payments.⁵⁵⁹ Thus, even though there is bank support for Bank Indonesia's policy on double swiping, in practice both banks and merchants are reluctant to adhere to it. This is an example of a trade-off between security and business policy, which would ultimately improve the residual risk for consumers, who are the weakest party in the payment system link.

As evidence of the lack of change on the practice of double swiping, the author still sees a great deal of double swiping while merchants are conducting card payment transactions in Indonesia. One such transaction, which had been successfully recorded with the approval of the restaurant cashiers, is depicted below:

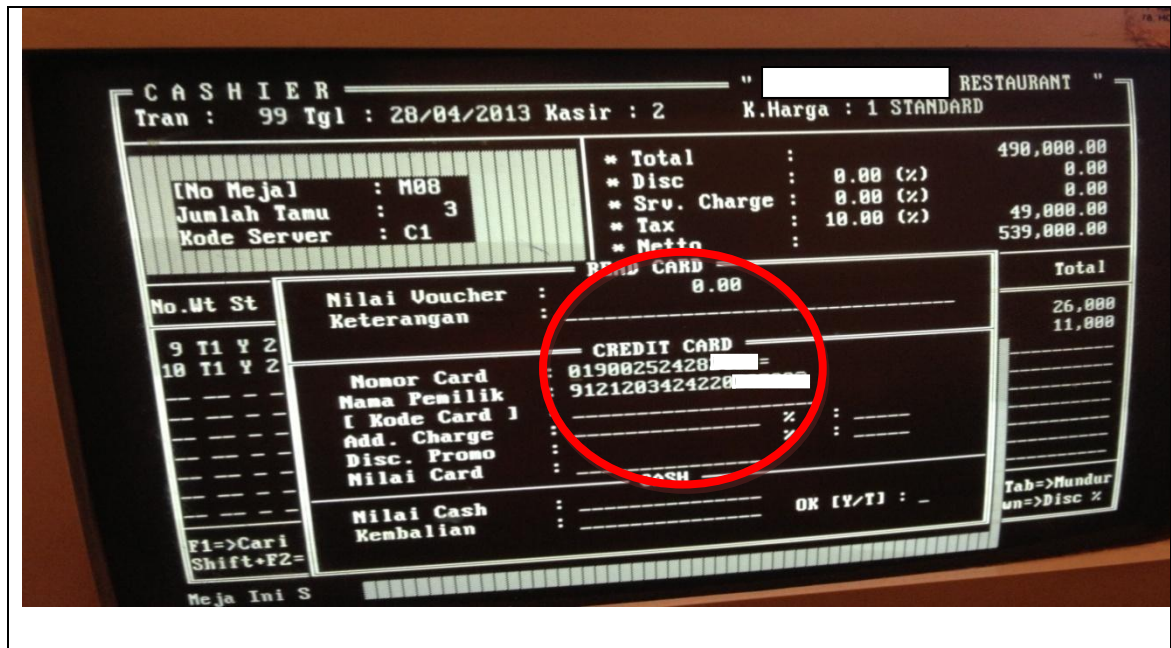
Figure 14: Bank EFTPOS Machine (blue) and Merchant's Card Skimmer (in Red Circle)



Merchant Black List is a list of the names of merchants proven not to have abided by bank or Bank Indonesia regulation, or involved in fraudulent activity.

⁵⁵⁹ Thertina and T W, above n 554.

Figure 15: Author Payment Card Tracks 1 and 2 Data on Merchant Cashier's Monitor (inside Red Circle)



From a technical point of view, any person who can obtain consumer payment card data (tracks 1 and 2) as shown in the Figure 15 — by writing down the data manually, capturing it with mobile phone camera, hacking computer storage, tapping it in the communication line, or using other fraudulent methods — can then easily and perfectly create counterfeit cards by encoding the data using a card writer encoder onto another magnetic stripe card. If the fraudsters also have obtained the consumer PIN, by means of shoulder surfing, spy camera, or key logging techniques, they would have the two authentication factors required by the system (that is, card data and PIN) to satisfy the identification and authentication requirements. In terms of the payment card information system, unauthorised transactions conducted by the fraudsters will be deemed valid, since it is now difficult for the payment system to distinguish between the data from a genuine card and that from a counterfeit card.

Therefore, in order to create sensible bank payment card practice using ATM/debit card and to protect a consumer's payment card credentials from identity theft, the author strongly recommends that Bank Indonesia enact a regulation that urges the merchant's acquirer bank to forbid its merchants conducting double swiping practice. Any violation of this regulation by a merchant will cause its acquiring bank to incur severe administrative sanctions from Bank Indonesia and/or bear full liability for consumer losses due to the double swiping practices.

4.2.1.4. ATM/EFTPOS Communication Network as Point of Compromise

Another venue that provides an opportunity for payment card fraud is skimming data from card use that is processed through the telephone or data cables connecting financial institutions and large commercial customers or ATM/EFTPOS terminals themselves. Payment card data such as credit card and debit card details including PINs that flow from merchant EFTPOS terminals to their bank, can be intercepted, copied, and sent to the skimmer for downloading onto counterfeit cards.⁵⁶⁰

Meyer and Matyas have argued that ‘communication links are highly vulnerable to the interception of message by a number of techniques which permit passive (listening), and/or active (data alteration/substitution) attacks’.⁵⁶¹ In this regard, Stallings and Brown note that ‘a passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.’⁵⁶²

A most prominent example of passive attack is ‘eavesdropping’. Eavesdropping aims to obtain information that is being transmitted, and does not entail any modification of the data. Hence it is very hard to detect, because the message traffic is sent and received without any obstruction, delay and alteration. Every transmission process is done in the perfectly normal manner.⁵⁶³ In the payment card system, an example of this passive attack is the use of a malicious code for bugging or tapping consumers’ ATM/debit card data and PINs that are transmitted from consumer activated terminals to the host system.

Wiretapping by ‘bugging’ an ATM or EFTPOS terminal or by tapping or intercepting the flow of data via a communication network is very hard to detect as a skimming device is planted *inside* the terminals and the entire skimming process is intangible, happening during legitimate transactions and without irregularities in the use of the card. Even the most observant consumer as a sender of information will not detect the

⁵⁶⁰ Australian Crime Commission, ‘Card Fraud’, above n 377. See also StGeorge, *Types of Fraud* (2012) <<http://www.stgeorge.com.au/online-services/security-centre/protect-yourself/types-of-fraud>>; Commonwealth Bank, *EFTPOS Skimming* (2013) <<http://www.commbank.com.au/business/merchant-services/other-services/protecting-you-and-your-customers.html#EFTPOS>>.

⁵⁶¹ Meyer and Matyas, above n 72, 478. See also Stallings and Brown, above n 221, 22.

⁵⁶² Stallings and Brown, above n 221, 22.

⁵⁶³ Ibid. See also Meyer and Matyas, above n 72, 22.

skimmer in this instance.⁵⁶⁴ Interestingly, most issuer/acquiring banks as a receiver of the transmission data are neither equipped with appropriate tools such as anti malware software, nor aware of the existence of malware within their system.⁵⁶⁵

An example of network hacking of EFTPOS systems is ‘war driving’, a hacking method that involves remotely scanning for open or vulnerable Internet connections to EFTPOS systems. Once a weak system is detected, a hacker hacks internal computers and installs key logging software onto the EFTPOS system. Hackers also install Trojans, which allow them ongoing access to the system, giving them the ability to install and re-install malware over time.⁵⁶⁶ Siciliano argues that remote hacking is not difficult since many people such as coders, programmers and criminal hackers have the ‘know-how’ to utilise tools to crack a Windows remote desktop and access dedicated ports used for remote servicing.⁵⁶⁷

In regard to this problem, Stallings and Brown contend that prevention in the form of data encryption is better than detection in dealing with eavesdropping attacks. Nonetheless, it is very unfortunate that ATM/debit card systems do not employ the most sophisticated encryption technology, such as is present in electronic money/stored-value cards technology.⁵⁶⁸ Mann argues that the maintenance of the status quo in ATM/debit card technology is caused by merchant and bank reluctance to upgrade their systems due to their consideration of the cost of such an investment.⁵⁶⁹

All forms of data communication can be intercepted regardless of whether that information is transmitted via communication lines, radio, or microwave.⁵⁷⁰ If fraudsters attack information transmitted through fixed lines, they have to place eavesdropping

⁵⁶⁴ Model Criminal Code Officers’ Committee of the Standing Committee of Attorneys-General, above n 466, 3. See also Meyer and Matyas, above n 72, 448–9.

⁵⁶⁵ Stallings and Brown, above n 221, 22.

⁵⁶⁶ Tracy Kitten, *POS Fraud: How Hackers Strike* (14 December 2011) Bank Info Security <http://www.bankinfosecurity.com/articles.php?art_id=4324&rf=2011-12-14-eb&elq=d0d8cc583b6b4e5b868f84ef253808b6&elqCampaignId=977>.

⁵⁶⁷ Ibid.

⁵⁶⁸ Stallings and Brown, above n 221, 22.

⁵⁶⁹ Mann, *Payment Systems and Other Financial Transaction*, above n 185, 164. According to Mann: [B]anks have resisted upgrading the technology for quite some time, based on concerns about the costs of requiring all merchants to purchase replacement terminals that would operate with more sophisticated encryption systems. Banks are particularly sensitive to those costs because merchants’ concerns about high equipment costs have been one of the main obstacles to growth of debit-card networks.

⁵⁷⁰ Meyer and Matyas, above n 72, 2.

tools (either hardware or software) within the system infrastructure, such as inside an ATM computer, EFTPOS terminal or communication line hub.

However, in recent years, wireless computing has been widely adopted due to its flexibility and cost saving efficiency. With satellite or microwave transmission, a physical connection is not required.⁵⁷¹ Unfortunately, a wireless communication protocol also has become a target for fraudulent exploitation.⁵⁷² Sensitive data communicated via wireless networks can be ‘sniffed’ by hackers with various tools. With interception tools and technology that is becoming more common and inexpensive, fraudsters can have the same level of access to information by eavesdropping on wireless communication without the need to physically tap into the communication line.⁵⁷³ Gifford further canvasses that wireless communication is vulnerable to straightforward attacks, unless system providers equip the communication data with appropriate security measures.⁵⁷⁴

The *Heartland Case* in the United States is one of several landmark decisions examples of how dangerous eavesdropping attacks on consumer payment data can be. This case involved identity theft from more than 130 million consumers’ credit and debit card records.⁵⁷⁵ In the other case, the TJX case caused US\$150–200 million in fraud losses, and most of that was debited directly from consumers’ bank accounts and in this instance the writer of the program used was issued restitution orders for USD\$171.5 million.⁵⁷⁶ This case called attention to the importance of security in payment card

⁵⁷¹ Ibid 478.

⁵⁷² Gifford, above n 17, 64.

⁵⁷³ Pipkin, above n 226, 223–4.

⁵⁷⁴ Gifford, above n 17, 36.

⁵⁷⁵ A 2009 landmark case in the US concerned a third party breach in EFTPOS system (the *Heartland Case*), the largest reported incident to date. See Tracy Kitten, *Heartland Breach: Legal Update* (6 April 2011) Bank Info Security <http://www.bankinfosecurity.com/articles.php?art_id=3510&rf=2011-04-07-eb>. A ‘mastermind’, in this instance was eventually prosecuted (together with 11 others) and he was sentenced to two 20 consecutive terms of imprisonment. Litigation was again underway in 2013–2014 with seven issuing banks suing the data processing company (Heartland): see Tracey Kitten, *More Litigation Tied to Heartland Breach* (21 February 2013) <<http://www.bankinfosecurity.com/more-litigation-tied-to-heartland-breach-a-5528/op-1>>. See also Frank Hayes, *Heartland Lawsuit Revived by Appeals Court* (6 September 2013) <<http://www.fierceretail.com/retailit/story/heartland-lawsuit-revived-by-appeals-court>>.

⁵⁷⁶ For lower value estimate, see Bell, above n 44. For upper value estimate and other details see further below. The person involved in writing the ‘sniffer’ was sentenced to two years jail and ordered to pay restitution of USD\$171.5 million: Dennis Fisher, *Convicted TJX Hacker Regrets Taking ‘Easy Way Out’ with Plea Deal*, Threat Post, 3 March 2015 <<https://threatpost.com/convicted-tjx-hacker-regrets-taking-easy-way-out-plea-deal-041213/77726/>>. As observers noted, given the low level of his assets, this was impossible. The hacking group-leader involved in this instance (Albert Gonzalvez), however, received a 20 year prison sentence: Kim Zetter Security, *TJX Hacker gets 20 Years Prison*, Wired, 25 March 2010

communication transmissions and to the question of what party or parties should be deemed legally responsible for fraud loss.⁵⁷⁷

<<http://www.wired.com/2010/03/tjx-sentencing/>> . He had already been fined of USD25,000, forfeited over USD2.7 million, surrendered his apartment, car and other items: Grant Gross, *Hacker Gonzalez Pleads Guilty to 20 Charges*, CSO, 11 September 2009 <<http://www.csoonline.com/article/2124329/identity-theft-prevention/hacker-gonzalez-pleads-guilty-to-20-charges.html>> . Neither could fully compensate the losses sustained. The involvement of overseas-based co-conspirators (Turkey, Russia) further complicated the case as it does in many instances.

⁵⁷⁷ See also Gifford, above n 17, 64–7; Morse and Raval, above n 44, 544; Richard J Sullivan, 'Risk Management and Nonbank Participation in the US Retail Payments System' (2008) 92 *Economic Review-Federal Reserve Bank of Kansas City* 5, 13; Schreft, above n 384, 14–15; Epstein and Brown, above n 325, 216–18; Morse and Raval, above n 44, 547. Gifford summarised the processes involved in the TJX attack and its ramifications as follows:

TJDX is a major North American retail chain with more than 3,500 stores. In December 2006, TJX disclosed that hackers had gained unauthorised access to its computer system and that numerous customer credit and debit card records had been compromised. The full scale of the incident then emerged. ... [H]ackers had first gained access to TJX's systems in July 2005, and that the intrusions had been going undetected for close on 18 months. During that period, ... a minimum of 45 million credit and debit card records had been stolen (some estimates put the true figure closer to 200 million). The initial attack exploited a weak wireless security protocol that was being used to transfer data between hand-held price checking devices, cash registers and the company's main computer system. Sitting in a car park close to a TJX store in St. Paul Minnesota and armed with a readily available wireless antenna, the hackers "eavesdropped" on wireless transmissions, downloaded them to a laptop and rapidly cracked the weak encryption protocol in use.

Having cracked the encryption protocol, the hackers were then able to eavesdrop on further email traffic and gather log on credentials for legitimate users. ... [They] used this access to set up their own user account on the TJX corporate computing systems in Framlingham, Massachusetts and used these to copy files and folders containing customer credit and debit card information.

Their ability to access confidential customer data was also reportedly compound by weak firewall rules and a failure by TJX IT staff to properly implement additional security software already purchased.

The hackers then sold the stolen information on the internet. ...[T]he stolen credit card and debit card details were purchased and used by online fraudsters from around the world, in countries including Sweden, Ukraine, Turkey, Australia, Hong Kong and Mexico.

Within days of the [TJX] disclosure ..., a number of lawsuits were filed. These were eventually consolidated into two class actions. One was a class action brought by consumers whose cards (and in some cases, identities) had been compromised.... The other was a class action brought by a number of "issuing banks" who had issued the cards that had been compromised.

Following the TJX intrusion, numerous fraudulent transactions were committed by fraudsters who had acquired the stolen credit and debit card details. The issuing banks (who ... had no idea that they were fraudulent transactions) paid out on these transactions but were then unable to recover the funds in the normal way from their cardholding customers because their customers had not made the purchases.

In addition to ... the losses associated with the fraudulent transactions, the issuing banks also collectively incurred millions of dollars of administration costs in replacing the compromised cards and in providing enhanced security monitoring of the compromised customer accounts.

...[T]he issuing banks looked for a means to recover these losses. There was little or no realistic possibility of targeting the fraudster himself or herself. There were thousands of them, ... scattered all over the world, ... difficult to identify, and even if ... traced, were likely to prove impecunious. Similarly, the original hackers were never found and, if they had been, it would have been highly unlikely that they would have had the financial wherewithal to compensate the issuing banks.

4.2.1.5. Bank and/or Its Counterpart's Data Centre Computer as Point of Compromise

While low-skilled criminals busily set physical-type traps (such as skimmers at ATMs) or virtual (online) traps for customers who are less cautious and lack information regarding fraud, a minority of criminals with a relatively good computer knowledge, choose to hack directly into the bank data centres, either within the bank's computer system, or in a bank's counterpart data processing system and/or its network. Such criminal activities are generally not preferred by criminals, as they require specific knowledge to overcome the bank's or its counterpart's security system. However, if they are successful, the data obtained is huge, so it is potentially very profitable. They can either use the data directly to perpetrate identity fraud, or sell it on the underground market for bank consumer data.

Sullivan's study on data breach in the United States revealed that, with the arrival of the Internet, the majority of data breaches are perpetrated by outsider fraudsters rather than insider fraudsters. Most data breach incidents result from the use of a stolen bank laptop or desktop, followed by bank information leaking through Internet, email or by hacking.⁵⁷⁸

One landmark example of data breach by hackers in the US payment card system occurred in November 2008, when computer hackers infiltrated RBS Worldpay, a US payment-processing subsidiary of the Royal Bank of Scotland, and gained access to data on 1.5 million cardholders. The hackers then extracted PIN numbers associated with some payment cards, created counterfeit payment cards, and modified computer system at RBS Worldpay to increase the available funds on the cards and the limits on the cash that could be withdrawn at ATMs. All this information was distributed to a global network of confederates. As result, over the course of just 12 hours, the fraudsters went on a cash withdrawal spree, obtaining USD9 million from 2100 ATMs in some 280 cities.⁵⁷⁹

For fraud liability issues between financial institution and consumer in U.S., see chapter 5.5.1. of this thesis. However, liability rules regarding allocation between financial institution, merchant and/or third party infrastructures providers are beyond the scope of this thesis discussion.

⁵⁷⁸ Sullivan, 'The Changing Nature of US Card Payment Fraud', above n 262, 105–6.

⁵⁷⁹ Ibid.

4.2.2. Methods of PIN Theft

If criminals can obtain skimmed information from the magnetic stripe of a bank customer's card,⁵⁸⁰ they have enough information to access an account. However, if the use of the card requires a PIN, they will have to get that number from a different source. The actual PIN number is not encoded on the card magnetic stripe since the stripe can be easily read with a very cheap device.⁵⁸¹

In ATM or debit card transactions at EFTPOS terminals, a PIN is indeed necessary.⁵⁸² The ATM/debit card system requires cardholders to enter a PIN in order to verify their identity. Therefore, after the criminals have successfully retrieved a consumer's magnetic stripe data from their ATM/debit cards, the next step is to get the consumer's PIN.⁵⁸³ The PIN is one of the most significant factors required to steal bank consumers' money. Even though probably not exhaustive, listed below are the most common methods for consumer PIN theft (related to consumer ATM/debit cards) that have also been identified in Indonesia.⁵⁸⁴

4.2.2.1. PIN Guessing

Nowadays, payment card systems world-wide have employed a 'two factor' authentication method. This method of authenticating the validity of the system user is based on 'something you have', which is ATM/debit card in the consumer's hand, and 'something you know', which is a PIN that should be remembered by the consumer.⁵⁸⁵

Consumers with an ATM/debit card basically have to memorise its PIN and are required not to record it in a manner that another person could ascertain what it is. The purpose of this is so that, if the ATM/debit card is lost or stolen, trapped in an ATM, or

⁵⁸⁰ See Geva, *The Law of Electronic Funds Transfers*, above n 83, 6–8. The magnetic strip is a technological device by which pre-recorded information is stored on a card. When magnetic-stripe card is passed ('swiped') at an ATM or EFT-POS terminal, the information stored in the magnetic stripe is 'read' and communicated directly to the issuer bank. See Mary Pat Flaherty, 'Bank Expert Discusses ATM Skimming - and how to detect it', *The Washington Post* (online), 6 April 2010 <<http://voices.washingtonpost.com/crime-scene/alexandria/atm-skimming-how-would-you-kno.html>>.

⁵⁸¹ Geva, *The Law of Electronic Funds Transfers*, above n 83, 6–11.

⁵⁸² Of course, there are also debit cards that require a signature as a method of authentication; however, these types of cards are beyond of the scope of this thesis.

⁵⁸³ Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7. See also Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 3; Smith and Grabosky, above n 448, 3–7.

⁵⁸⁴ See also Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7.

⁵⁸⁵ See Nigel Reavley, 'Flexibility, Fraud and Two-Factor Authentication' (2007) 19 *Card Technology Today* 12.

skimmed, whoever finds the card would be unable to use the card, because they do not know the associated PIN.

However, passwords or PINs, as a knowledge-based authentication mechanism, depend on human memory. With the increasing complexity and quantity of passwords, it is very difficult for all users to remember all of their passwords/PINs.⁵⁸⁶ Many people even forget their four-digit PIN, particularly if they have numerous cards with diverse PINs.⁵⁸⁷

Hence, some banks consumers inadvertently write the password or PIN down because the PIN may be too complex,⁵⁸⁸ or they have many cards so that ‘remembering many PINs may prove to be a problem’.⁵⁸⁹ As result, ‘many bank customers feel the need to carry the number with them whenever they intend to use their plastic card, thereby seriously compromising the security of the PIN’.⁵⁹⁰ Besides consumers’ writing their password/PIN down, Zhang et al argue that consumer malpractice regarding PIN also relates to their choice of weak rather than strong passwords, and using a common password for multiple accounts.⁵⁹¹

Concerning consumer choice of PIN, banks tend to give consumers flexibility in determining their own PIN. Generally, consumers frequently will choose a number for a PIN based on their own birthday or birthday of their closest person (such as their spouse), street address, telephone number or another number that is familiar to them.

While this gives consumers the opportunity not to write their PIN down, its disadvantage is that the practice makes it far easier for the PIN to be guessed, especially if the card is lost or stolen.⁵⁹² Radu asserts that the probability of ‘cracking’ the PIN is higher if ‘the number of digits in the PIN is small, the number of permitted wrong

⁵⁸⁶ Zhang et al, above n 233, 165–6. See also Hendry, above n 203, 76.

⁵⁸⁷ Zhang et al, above n 233, 165.

⁵⁸⁸ FFIEC, *Information Security*, above n 202, 27–9. See also Mohammad Mannan and P C van Oorschot, 'Reducing Threats from Flawed Security APIs: The Banking PIN Case' (2009) 28(6) *Computers & Security* 412. See also UNCITRAL, *UNCITRAL Legal Guide on Electronic Funds Transfers*, above n 189, 50–1; Arora, above n 197, 129–30.

⁵⁸⁹ Levi and Handley, above n 343.

⁵⁹⁰ See UNCITRAL, *UNCITRAL Legal Guide on Electronic Funds Transfers*, above n 189, 50–1.

⁵⁹¹ Zhang et al, above n 233, 165–6.

⁵⁹² See UNCITRAL, *UNCITRAL Legal Guide on Electronic Funds Transfers*, above n 189, 50–1.

attempts is high, and the number of wrong attempts is not stored from one ATM session to another'.⁵⁹³

For a four digit PIN, fraudsters normally only have three guesses to 10,000 probability.⁵⁹⁴ If the fraudsters have to guess the correct PIN and have three tries as normally allowed by an ATM system, they have one in 3,333 possibilities.⁵⁹⁵ However, from 3.4 million stolen passwords that have been made public over the years, researchers at Data Genetics come out with staggering summary of the actual probabilities. According to Data Genetics, the three most popular combinations are '1234' (10.713 per cent), '1111' (6.016 per cent), and '0000' (1.881 per cent) account for nearly to 20 per cent of all four-digit passwords.⁵⁹⁶

In addition, the research also found that many consumers use a year of birth as their PIN. Although the use of this makes a PIN easy to remember, the predictability of the consumer's PIN also increases. For instance, a four digit PIN starting with number 19 is quite popular. Month/year combinations were also found to be quite common. Therefore, choosing a birthday date or year as a PIN definitely makes the PIN easier to guess.⁵⁹⁷

There is also a possibility that a fraudster guesses an easily memorable way to enter PIN, such as entering four numbers in the single column from top to bottom on the ATM keypad (for example, number 2580).⁵⁹⁸ Apparently, fraudsters noticed that some consumers do not want the worry of memorising a complex PIN entry and prefer to use one row of the series of ATM PIN pad numbers.

⁵⁹³ Radu, above n 210, 31–2.

⁵⁹⁴ Bond and Zielinski, above n 328. See also Nick Berry, 'PIN Analysis' on Nick Berry, *DataGenetics* <<http://www.datagenetics.com/blog/september32012/index.html>>.

⁵⁹⁵ Will Oremus, 'The World's Least-Popular Four-Digit PIN: 8068' on Will Oremus, *Slate* (19 September 2012) <http://www.slate.com/blogs/future_tense/2012/09/19/how_to_choose_a_pin_code_avoid_birthday_date_1234_or_8068.html>.

⁵⁹⁶ Ibid. See also Berry, above n 594; Meredith Bennett-Smith, 'Safest ATM PINs: Analysis Reveals Four-Digit Combinations Almost No One Is Using', *The Huffington Post* (online), 20 September 2012 <http://www.huffingtonpost.com/2012/09/20/the-worlds-safest-atm-pin-four-digit-combination_n_1901430.html>.

⁵⁹⁷ Berry, above n 594.

⁵⁹⁸ Ibid.

Figure 16: ATM PIN Pad



From a criminal's perspective, since both of these authentication components are in the consumer's hands' (the card inside the wallet/bag and written PINs somewhere inside the wallet, and sometimes a driver's licence with the cardholder's date of birth on it),⁵⁹⁹ naturally that consumer might become the first listed by fraudsters as a target. It is well known that one of the weakest links in the payment system infrastructure is the people themselves.⁶⁰⁰

If a cardholder payment card along with its PIN information falls into the hands of fraudsters before the cardholder notices or has the chance to inform the issuing bank to block further transactions, most probably it will be the cause of unauthorised ATM/debit card transactions. With genuine payment card and information in the hands of fraudsters, they will easily withdraw money from any ATM or conduct transactions in any shops, both in the brick-mortar-world or on the Internet.⁶⁰¹

4.2.2.2. Shoulder Surfing

Shoulder surfing is the criminal act of stealing a consumer PIN by the perpetrators positioning themselves in close but not direct proximity to the ATM (so they are looking over the consumer's shoulder) to covertly observe what number a consumer taps into the keypad when entering the PIN.⁶⁰² However, someone using binoculars or a

⁵⁹⁹ See Financial Fraud Action UK, above n 346, 28.

⁶⁰⁰ Levi and Handley, above n 343.

⁶⁰¹ See also Financial Fraud Action UK, above n 346, 18.

⁶⁰² Diebold Incorporated, '*White Paper: ATM Fraud and Security*', above n 348, 4–7. See also Financial Fraud Action UK, above n 346, 28; Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 3; Mohamad, above n 302, 10.

telephoto lens can also observe the cardholder entering a PIN on the keypad from a distance.⁶⁰³

In practice, shoulder surfing is not the only way to steal a consumer's PIN. Being next to or at the consumer's side to observe the entry of the PIN (such as commonly happens in the ATM card-trapping method) or observing the consumer entering their PIN from the opposite direction (such as typically happens at EFTPOS terminals in merchant transactions) has also proved to be quite effective.

Nowadays, it is easier for a fraudster merchant's cashier to observe consumers entering their PINs, since PINs are used more regularly, often in overcrowded stores. From one experiment in a merchant-like environment regarding 'whether PIN-entry spying is easier than signature falsification', Matyas et al concluded that 'the risk of PIN compromise is high', especially in the case of merchants that do not have EFTPOS terminals with PIN pad security shields.⁶⁰⁴

In Indonesia, based on observations at several merchants in various cities, most EFTPOS terminals do not have PIN pad security shields. All EFTPOS machines are located at the cashiers' desks, which makes observation of consumer PIN entry very easy. In some cases, there were EFTPOS terminals that were even located underneath the cashier's desk, hidden from the sight of consumers. The author himself even had an experience where a cashier at a major hospital in Jakarta had to take the card to be swiped to an EFTPOS machine located in a different room that was out of sight of the card owner. At the moment (up until early 2016), there are no regulations in Indonesia that regulate EFTPOS machine use at merchants (positioning and so on).

4.2.2.3. PIN Pad Overlay

A PIN pad is a small handheld device, the purpose of which is to allow the cardholder to enter a PIN secretly on consumer-activated terminals without having to reveal that PIN to the shop cashier or to anyone else. A fake PIN pad overlay is a fake keyboard that looks exactly like the ATM PIN pad and is placed on top of the genuine ATM keyboard. It allows the cardholder to enter the PIN normally to activate the transaction,

⁶⁰³ Smith and Grabosky, above n 448, 4–5.

⁶⁰⁴ Vaclav Matyas et al, 'Authorizing Card Payments with PINs' (2008) 41(2) *Computer* 64, 65.

but simultaneously captures the consumer's PIN.⁶⁰⁵ The consumers' keystrokes 'are logged before being passed onto the actual keypad'.⁶⁰⁶

The fake overlay has memory to store any PIN data that has been captured. The fake overlay is then removed and the captured PIN data is downloaded.⁶⁰⁷ Diaz contends that unless an expert, the ordinary bank consumer will never notice this fraud method; it is a situation that persists in Indonesia among uninformed consumers who are largely unaware of the existence of this method in the country (such presence being attested to by some interviewees).⁶⁰⁸ However, from the author's observations of banking security practice and consumer education materials, this method has never revealed to bank consumers and so it difficult for consumers to know to increase their vigilance in this regard at ATMs.

Diebold, in its white paper further described the use of a thin fake PIN pad overlay that was even more difficult to detect.⁶⁰⁹

Figure 17: PIN-Pad Overlay



Source: Brian Krebs⁶¹⁰

⁶⁰⁵ Jesus Diaz, *This ATM Keyboard Will Steal Your Card PIN and You Will Never Notice It* (5 January 2011) Gizmodo <<http://gizmodo.com/5725859/this-is-how-cyber+criminals-steal-your-money>>. See also Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7. See also Mohamad, above n 302, 10.

⁶⁰⁶ Barwise and Bachfeld, above n 377.

⁶⁰⁷ Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7.

⁶⁰⁸ Diaz, above n 605. See also Interviews with consumers:C-1–C-30).

⁶⁰⁹ Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7.

An additional type of overlay that is more difficult to detect is a "thin" overlay that is transparent to the consumer. With this tool, not only is the PIN intercepted, it also allows the transaction to proceed in a normal way. This method used in conjunction with card data theft provides the criminal with the information needed to access an unsuspecting consumer's account.

A criminal may also attach a portable monitor and card reader on top of the actual ATMs monitor and card reader to obtain the card and PIN information. The false monitor and card reader record the account information and present a message to the customer that the transaction cannot be completed; after the customer leaves the criminal will return and remove the portable device: at 3.

⁶¹⁰ Krebs, 'ATM Skimmers, Part II', above n 480.

4.2.2.4. Pinhole Camera

The fraudster typically places a covert video camera (also called a pinhole camera) in ‘hard to detect locations’ in order to capture cardholder PIN numbers.⁶¹¹ To get a clear view of the keypad and record all of the ATM PIN entry, a camera is secretly positioned near the ATM.⁶¹² The camera can be positioned directly above the keypad, but sometimes also to the side — such as on the wall inside a pamphlet box. There is also a case in Indonesia where an ATM maintenance officer interviewee reported having detected a pinhole camera positioned underneath the PIN pad cover case in an ATM booth and pointed directly at the PIN pad area.⁶¹³ The date entry video of consumer PINs is then stored.⁶¹⁴ Apparently, this is the most popular method for fraudsters to steal consumers PIN and used in conjunction with magnetic stripe skimming.

Figure 18: Hidden Camera in False Panel above PIN Pad



Source: Krebs⁶¹⁵

Figure 19: Pinhole Camera in Brochure Holder



Source: Mike Barwise and Daniel Bachfeld⁶¹⁶

⁶¹¹ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 102–4.

⁶¹² Mohamad, above n 302, 10.

⁶¹³ BMO-5. Interview conducted at Bank Indonesia’s lobby area (Jakarta, 5 April 2013).

⁶¹⁴ Barwise and Bachfeld, above n 377.

⁶¹⁵ Krebs, ‘ATM Skimmers, Part II’, above n 480. See also Barwise and Bachfeld, above n 377.

⁶¹⁶ Barwise and Bachfeld, above n 377.

Most customers usually do not cover the PIN pad sufficiently to completely obscure it from a camera.⁶¹⁷ Hence, banks often encourage consumers to cover the keypad with their hand when performing a PIN entry. However, even though consumers probably sufficiently cover the PIN pad to avoid monitoring from a pinhole camera (if one is in place), this effort will be meaningless if the fraudsters actually use a fake PIN pad overlay or have installed malware, or are tapping the communication line to obtain consumer PINs.

4.2.2.5. PIN Interception/‘Cracking’

In ATM/debit card transactions, a PIN is the only consumer authentication method. PIN acquisition by fraudsters is probably the most important and difficult process in the identity theft, even when compared to acquisition of consumer magnetic stripe data.⁶¹⁸

Banking and security researchers have noticed for years that fraudsters are successfully attacking financial PIN processing application program interfaces (APIs) to obtain consumer PINs.⁶¹⁹ Banks generally secure consumer PINs by utilising a tamper resistant ‘Hardware Security Module’ (HSM). When consumers enter a PIN at consumer activated terminals, the PIN along with magnetic stripe data are sent to the verification facility (the issuing bank or other authorised entities) for verification.⁶²⁰

Hence, the PIN can be captured either inside the consumer activated terminals, or when the PIN is transmitted to the bank’s host computer for PIN authentication. In the research undertaken by Berkman and Ostrovsky, they argue that both a fraudster bank insider or insider of a third party switching provider could use the HSM to reveal the encrypted PIN codes and exploit them to make fraudulent transactions.⁶²¹

To give more understanding about ‘PIN cracking’, Manan and Oorschot describe the point where flaws are often found in widely deployed security APIs in ATMs:

PIN transfers in banking networks rely on symmetric key cryptography where the third-party controlled intermediate switches also possess shared keys to decrypt encrypted PINs (but have no access to issuer/verification keys). Although decrypted PINs (and the decryption key itself) are not (ideally) accessible from outside of an HSM, API flaws

⁶¹⁷ Walsh, above n 323, 10.

⁶¹⁸ Bond and Zielinski, above n 328.

⁶¹⁹ Ibid 1.

⁶²⁰ Berkman and Odelia, above n 239, 224.

⁶²¹ ‘Scientists Find Insider PIN Cracks’ (2006) 3(12) *Computer Fraud and Security* 3.

allow attackers to realistically extract enough information from the HSM (through legitimate API calls) to enable PIN cracking attacks.⁶²²

Fraudsters have employed many cracking techniques to reveal consumer PINs. For instance, Bond and Zielinski have claimed that by using adaptive decimalisation tables and guesses, a 30-minute attack on an HSM can discover approximately 7000 PINs (rather than 24 with the 'brute force' method).⁶²³ In another instance, Berkman and Ostrovsky have noted that an attack on the financial PIN processing API can reveal up to 18 million PINs in an hour. They even believed that the attack they described probably is the cause of many phantom withdrawals in payment card fraud.⁶²⁴

The flawlessness of PIN entry devices in the EFTPOS terminals is also highlighted by Drimer, Murdoch and Anderson, researchers from the University of Cambridge. According to them, merchants and corrupt employees, or even consumers that have access to EFTPOS terminals, can tamper with them, even if the EFTPOS terminals are tamper resistant ones (that is, they have anti-tampering mechanisms).⁶²⁵ Further they assert that in order to get consumer data from anti-tampering chip ready EFTPOS terminals, the fraudster taps the data line of the pin entry device (PED), the smart card interface that is not encrypted.⁶²⁶

4.2.3. Identity Fraud: Counterfeit Card Fraud

Most instances of ATM/debit skimming or other types of data theft (such as using malware, cracking, eavesdropping method and so on) will conclude with the production of counterfeit ATM/debit cards to perform unauthorised ATM/debit card transactions, through either ATM withdrawals or ATM funds transfers, or a combination of both.

Nowadays, it is relatively cheap to produce a payment card with a magnetic stripe.⁶²⁷ Criminals that have successfully skimmed ATM/debit card information can then

⁶²² Mannan and Oorshchot, above n 588, 2.

⁶²³ Bond and Zielinski, above n 328.

⁶²⁴ Berkman and Odelia, above n 239, 236.

⁶²⁵ Saar Drimer, Steven J Murdoch and Ross Anderson, 'Failures of Tamper-Proofing in PIN Entry Devices' (2009) 7 *IEEE Security & Privacy Magazine* 39, 40.

⁶²⁶ Ibid. The PIN entry devices (PED) used in the research is the Ingenico 1330, the most widely deployed PED in the UK. To tap the consumer's data from a PED, researchers just utilise simple tools such as a bent paperclip, a needle, a short length of wire, and some creative thinking. A small field programmable gate array (FPGA) or microcontroller board with some non volatile memory can easily fit inside the Ingenico PED's compartment and record thousands of transaction details without the cardholder's knowledge.

⁶²⁷ Diebold Incorporated, *White Paper: Battling Card Fraud through Chip and PIN Technology*, above n 209, 2.

perfectly write this information or download it onto a counterfeit or cloned card.⁶²⁸ In essence, counterfeit card fraud occurs when ‘a fake card is created by fraudsters using compromised details from the magnetic stripe of a genuine card’ and is presented to obtain funds or purchase goods or services.⁶²⁹ Consumer counterfeit cards, along with the consumer PIN, can be used at any ATM/EFTPOS as if it is genuine card (as it is an exact copy of the original).⁶³⁰

This counterfeit card can be any form of media that has a magnetic stripe on it, either new (such as a blank white plastic card)⁶³¹ or used (such as an ATM/debit/credit card or re-encoded expired cards),⁶³² a store loyalty card, hotel access door card, library card, a security card, a parking ticket and the like.⁶³³

If the skimmed data is written into the magnetic stripe on a used card using card writer, it will overwrite the old information in the magnetic stripe. Unless a bank’s system adds a dynamic element to the transaction record so that every transaction is unique,⁶³⁴ a

⁶²⁸ S J Murdoch, ‘Reliability of Chip & PIN Evidence in Banking Disputes’ (2009) 6(12) *Digital Evidence and Electronic Signature Law Review* 1, 2. See also APCA, ‘Payment Fraud Statistics Methodology Paper’ cited in Mohamad, above n 302, 6–7. See also: Smart Card Alliance, ‘Fraud in the US Payments Industry’, above n 297, 14; Richard Tyson, ‘Counterfeit Card Fraud Soars in the UK’ (2001) 13(4) *Card Technology Today* 2, 2; Devos and Pipan, above n 297, 6–7; Oracle Corporation, above n 398, 3–5. According to the APCA, counterfeit card fraud is:

the use of altered or illegally reproduced cards including the replication/alteration of the magnetic stripe and changes to the details on the face of the card with intent to defraud. Most of this fraud involves a technique called skimming. Skimming is a form of magnetic stripe counterfeiting in which criminals are able to copy magnetic stripe track information (including Card Verification Value – CVV) from a valid card. Information may then be encoded on a counterfeit or stolen card and used fraudulently.

⁶²⁹ Financial Fraud Action UK, above n 346, 15.

⁶³⁰ Model Criminal Code Officers’ Committee of the Standing Committee of Attorneys-General, above n 466, 4.

⁶³¹ A blank white card with a magnetic stripe can be freely purchased from card manufacturers and dealers. See Hendry, above n 203, 37. Blank white cards with magnetic cards can also easily be obtained from online sellers, such as through ebay (eBay is a company operating on the Internet that allows for vendors of any kind to auction or sell merchandise of a variety of types).

⁶³² Meyer and Matyas, above n 72, 445–6.

⁶³³ See Model Criminal Code Officers’ Committee of the Standing Committee of Attorneys-General, above n 466, 4; Krebs, ‘Beware a Card - and Cash Trapping at the ATM’, above n 428.

⁶³⁴ See Smart Card Alliance, ‘Fraud in the US Payments Industry’, above n 297, 11. See also European Central Bank, above n 344, 10. In the European Central Bank report, to detect counterfeit fraud, some card payment schemes generate a random number by the central server and store it on the *magstripe* of the card. Thus, numbers stored on the server and the card are compared at the beginning of each transaction. At the exact moment a card is cloned, the information on the two cards and the server is identical. Subsequently, new random numbers generated by the server will be stored on only one of the two cards and transactions can be blocked as soon as the second card is used. This mechanism can prevent fraud losses in the first place if the original card is used before the cloned card is used for the first time.

bank's system can not distinguish whether the transactions are coming from the cloned card or the genuine one (as the cloned card is an exact replica of the original).⁶³⁵

However, if the skimmed data is written onto a counterfeit card in a form other than bank's card, it is unlikely to be able to be used to purchase goods 'over the counter'.⁶³⁶ Nonetheless, this counterfeit card can be used safely to perform unauthorised ATM transactions, such as cash withdrawals or funds transfers, since the fraudster will be alone inside the ATM booth and most of the ATM cameras are not actively monitored (or may not even have been activated). In the interviews with officers of various banks, it was revealed that CCTV was not installed in every ATM for the sake of 'efficiency' as there is no regulation obligating banks to install CCTV at or in ATMs.⁶³⁷ It is also possible to use the skimmed information (especially from a debit card) to procure goods over the phone or on the Internet without the need for a counterfeit card or for creating 'any physical record of the skimmed data'.⁶³⁸ However, the latter fraud will not be discussed since it is beyond the scope of this thesis.

Counterfeit ATM/debit cards are one of the most prominent card-based frauds worldwide. It is generally achieved through a technical process called 'skimming'.⁶³⁹ A skimming attack is the fraudster's favourite violation in ATM transactions.⁶⁴⁰

Meyer and Matyas have argued that counterfeit cards are one of the fraudulent activities that should be given special attention because of their broad presence of cards across the country (providing the opportunity for mass fraud). Further, they assert that if the national EFT system were to be flooded with thousands of counterfeit cards, it would not only cause monetary loss for thousands of unsuspecting bank consumers,⁶⁴¹ but also

⁶³⁵ See Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 2.

⁶³⁶ Ibid 4.

⁶³⁷ Interviews with BO-1; BO-2; BO-4; BO-5; BO-6.

⁶³⁸ Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, above n 466, 4.

⁶³⁹ Kondabagil, above n 194, 93. Sometimes the skimming method is also called 'cloning'. See Tyson, above n 628, 2.

⁶⁴⁰ Mohammed, above n 195, 216–17.

⁶⁴¹ The use of a counterfeit version of a legitimate card would not be detected until the legitimate cardholder examined his next statement or received notification that his account was overdrawn. See Meyer and Matyas, above n 72, 445–6. See also Smart Card Alliance, 'Fraud in the US Payments Industry', above n 297, 14.

have the potential to trigger outright fraudulent claims of fraud,⁶⁴² first party fraud, and the most serious risk, namely ‘the loss of customer good will, and customer confidence in the EFT system’.⁶⁴³

Counterfeit card fraud attracts many perpetrators, even though it requires more resources than CNP fraud. One of the reasons is because such cards can be used for transactions such as cash withdrawals at ATMs or purchasing goods at all locations globally that accept the relevant payment card.⁶⁴⁴ Other than that, as many ATMs and/or EFTPOS terminals are unattended and located outside of the bank’s perimeter, the opportunities for and incentives to perpetrate card fraud are also high, with little risk of being caught by law enforcement entities.

The latest ATM scam related to counterfeit ATM/debit card that leaves consumers vulnerable is what has been termed a ‘flash attack’. Using this method, fraudsters withdraw money using hundreds of cloned cards at ATMs across a wide region within a very short period of time. The amounts withdrawn are usually within a range that would not immediately ‘raise a red flag’. This type of fraud deliberately targets ATM/debit cards, which have less sophisticated fraud detection systems in place than credit cards.⁶⁴⁵

4.3. Identity Theft and Fraud Figures, Challenges, and the Dearth of Fraud Reports in ATM/Debit Card Transactions in Indonesia

4.3.1. ATM/Debit Card Fraud Figures (Unpublished)

In Indonesia, the advances and exponential growth in information, communication and technological infrastructure have enabled the banking industry to provide modern payment systems to its consumers, including payment card system services. However, similar to what is happening in other jurisdictions, the greater financial system dependence on information technology, such as through the pervasive use of ATM/debit card in e-commerce and banking transactions, has been shown to increase the risks associated with payment card transactions.

⁶⁴² Card holders who claim fraud because of transactions they have honestly forgotten. See Meyer and Matyas, above n 72, 445–6.

⁶⁴³ Ibid.

⁶⁴⁴ Oracle Corporation, above n 398, 3–5. See also Hendry, above n 203, 37–9.

⁶⁴⁵ Jeremy Kirk, *Fraudsters Find Holes in Debit Card Fraud Detection* (2010) Computerworld <http://www.computerworld.com/s/article/9193378/Fraudsters_find_holes_in_debit_card_fraud_detection?taxonomyId=17&pageNumber=1>. See also Siciliano, above n 455.

Concerns about e-banking or e-commerce transaction trustworthiness indeed exist in Indonesia. In their assessment of Information and Communication Technologies in Indonesia, Owen et al concluded that there is a widespread lack of trust and confidence in the security, integrity, reliability, and enforceability of electronic transactions.⁶⁴⁶ The biggest concern for bank depositors is whether their funds will be lost through unauthorised transactions, which utilise electronic banking system weaknesses.

Banks are most vulnerable to and apparent targets of several methods of fraud. Despite each individual transaction being of relatively small value, the total number (and thus value) of unauthorised transactions that steal consumers funds from banks are believed to be very high. This can be seen from Bank Indonesia's consumer complaint records concerning ATM/debit card fraud, which has increased quite significantly. In 2012, consumer complaints regarding ATM/debit card transactions numbered 24,400 complaints, an increase 28.42% compared to the previous year's complaint volume.⁶⁴⁷

Apart from this report, the number of consumer complaints about unauthorised ATM/debit transactions appearing in various mass media (both paper-based or on-line) are relatively high and sufficient to draw attention to the problem. Consumer complaints were not only about pervasive fraud in ATM/debit operations, but also highlighted the failure of bank–consumer dispute resolution processes within the banking industry. Most of the complaints were about the occurrence of payment card fraud and the objections of the banks to redressing consumer losses.⁶⁴⁸

In Indonesia, all payment card institutions have an obligation to report fraud in their payment card system to Bank Indonesia on monthly basis. The importance of accurate statistical data is recognising by Bank Indonesia.⁶⁴⁹ Bank Indonesia's policy on how

⁶⁴⁶ Owen et al, above n 64, 10.

⁶⁴⁷ Karnoto Muhamad, 'Adu Pelayanan di Tengah Ancaman [Service Competition in the Middle of Threat]', *Infobank* May 2013, 22–3.

⁶⁴⁸ Unfortunately, there is no comprehensive data about the number of consumer complaints appearing in the mass media.

⁶⁴⁹ Ida Nuryanti and Susiati Dewi, 'Chapter 3: the Development of E-Payment and Challeges in Indonesia' in Vincent Lim Choon Seng (ed), *The Development of E-Payments and Challenges for Central Banks in the SEACEN Countries* (South East Asian Central Banks (SEACEN) Research and Training Centre, 2008) 96. According to them, providing accurate statistical data of e-payment industry and ensuring that operators comply with Bank Indonesia regulation, including the customer protection principle, is 'of great importance': at 96. Accurate statistical data will help the regulator in making the right policies in developing a healthy e-payment industry. Operators' compliance with regulation, especially to consumer protection principles, is of a great importance since public trust is one of the main factors to develop the industry': id.

banks should treat payment card reports is very clear. Bank Indonesia has urged that every report, all information and/or data submitted by the principal, issuer, acquirer, and other institutions to Bank Indonesia, must be submitted in full, and be correct and accurate.⁶⁵⁰ Nevertheless, comprehensive, easy to access, correct and accurate fraud data on e-banking transaction in Indonesia is still not available to the public.

Data obtained from an unpublished report from the Electronic Data Warehouse in Bank Indonesia reveal that there is an increasing volume and value of an ATM/debit card fraud in Indonesia, as is shown below:

Table 1: Type of ATM/Debit Card Fraud and Data

Type of Fraud	Bank's ATM/Debit Card Fraud Data			
	2011		2012	
	Volume	Value*	Volume	Value*
Counterfeit Card	96	945.15	101	1,139.92
Lost/Stolen Card	10,059	225.14	10,498	234.17
Damage Card	377	42.97	381	42.45
Card Not Received	2	0	2	1.98
Application Fraud	0	0	0	0
Card Not Present Transaction	0	0	0	0
Miscellaneous	951	0.60	443	0.20
Total:	11,485	1,213.86	11,425	1,418.72

*Value in million Indonesian Rupiah.

Sources: Bank Fraud Monthly Report – Electronic Data Warehouse (unpublished)

The increasing incidence of fraud has also been identified by the central bank. The magnitude of the problem can be gauged from the number of incidents of fraud that have come to light in the recent past. The escalating number and volume of transactions has been matched by a significant rise in card-based payment instrument crimes.⁶⁵¹ The fact that such incidents are not only increasing in number but also are more varied in terms of fraud methods has forced Bank Indonesia (as the central bank of the Republic of Indonesia) to enact more detailed Bank Indonesia regulations concerning the security aspect and reliability of the system.⁶⁵²

⁶⁵⁰ *BIR-CBPI* art 34.

⁶⁵¹ See 'General Review' in the elucidation of Peraturan Bank Indonesia Nomor 6/30/PBI/2004 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan kartu [Bank Indonesia Regulation Number 6/30/2004 Concerning Operation of Card-Based Payment Instrument Activities].

⁶⁵² See the consideration section of Bank Indonesia Regulation Number 14/2/PBI/2012 Concerning Amendment of Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Operation of Card-Based Payment Instrument Activities] (*'BIR-CBPI'*).

4.3.2. ATM/Debit Card Identity Theft/Fraud Methods in Indonesia

Apart from those fraud reports, the sporadic incidents of fraud in the ATM/debit card industry in Indonesia has long been acknowledged and reported to the central bank on a case-by-case basis.⁶⁵³ These incidents mostly were never revealed to the public. Hence the public and payment system authority always have difficulty in gauging the real level of payment system risk exposure, either on a national basis or for a specific bank.

The rash of ATM/debit card skimming that occurred across several cities at the end of 2010 in Indonesia (and widely covered by national mass media) was a revelation as to the pervasiveness and serious impact of identity theft that had facilitated fraud to be perpetrated across the payment system industry in Indonesia. To overcome the problem, Bank Indonesia as payment system authority in Indonesia, has a clear policy that urges banks to tighten their ATM security. Bank Indonesia has enacted several regulations to improve bank security systems. It has instructed banks to take several actions to reduce ATM and debit card fraud. These include forming a task force to exchange information about fraud and find the way to circumvent it. Bank Indonesia also encourages banks to increase surveillance in public access terminal more frequently, install anti-skimmer devices, add ATM pin-pad shield and continue to roll out consumer education programme about the importance of keeping ATM/debit card PINs secret.⁶⁵⁴

⁶⁵³ Indonesia, ATM skimmer fraud has long been acknowledged. In 2003, John Petrus, an Indonesian citizen, and Eng Kim Hook, a Malaysian citizen, both ATM fraudsters, were convicted of a criminal offence by Jakarta District Court and sentenced to imprisonment of six and three years respectively (verdict No. 532/PID.B/2003/PH.JKT.PST dated 4 June 2003 and No. 427/PID.B/2003/PN.JKT.PST dated 12 June 2003). Both fraudsters were prosecuted according to articles 263(2) (forgery in writings), 65(1) (conjunction) or 362 (theft) and 65(1) of Indonesia's Penal Code (KUHP).

⁶⁵⁴ Financial System Stability Bureau Directorate of Banking Research and Regulation, 'Financial Stability Review No. 14, March 2010' (Bank Indonesia, 2010) <<http://www.bi.go.id/NR/rdonlyres/9379845A-3B22-488D-A5BA-6D08321BAD03/20251/FSR14March2010.pdf>>, 57. In this report, Bank Indonesia's policy to reduce fraud in ATM/debit card transactions can be seen from Box 3.2: ATM and Debit Card Fraud, as follows:

Realizing the importance of security in the card based payment industry, Bank Indonesia has introduced a number of acquirer and principal requirements in order to improve security technology, manage operational risk and regulate reporting. These aspects are legislated by Bank Indonesia Regulation No. 11/ 11/PBI/2009 and Bank Indonesia Circular No.11/10/ DASP dated 13 April 2009 regarding Card Based Payment Instruments.

At the outset of 2010 Bank Indonesia implemented a number of measures to help prevent the spread of fraudulent ATM and ATM/Debit card activity including, among others, forming a task force made up of banks that had been affected by skimming cases as well as switching companies. The task force is mandated with facilitating the banking industry in terms of simplifying the identification and introduction of preventative measures against fraudulent activities. In addition, a technical forum will be established involving the Police Department, Bank Indonesia and other related parties. The technical forum will facilitate an exchange of information pertaining to

While the 2010 ATM skimming cited above employed a ‘conventional identity theft/fraud method, in contrast,’ the Body Shop fraud of 2013 (also widely covered by the media) employed one of the most sophisticated and advanced identity theft methods, that is, malicious software (malware). Before the Body Shop fraud, none of the bank management staff in Indonesia who became the author’s respondents had been aware of the possibility of malware attack either in ATMs or EFTPOS machines. Many of the bank officers did not even know that their payment card system could actually be compromised by malware.⁶⁵⁵ Hence, it is not surprising that banks’ payment card systems were vulnerable to malware attack, since none of them had installed anti-malware programs in their payment card system, including on ATMs and EFTPOS terminals. Therefore, similar to the 2010 skimming deluge fraud in Indonesia, the Body Shop fraud could also be considered ‘a key opener’ for (an indicator of) the fact that ‘high technology’ fraud was already in existence in Indonesia. The Body Shop fraud in the payment card industry in Indonesia that employed malware as its mode of operation has opened the possibility that many unrevealed ‘phantom withdrawals’ in the ATM/debit card transactions may actually have been caused by malware that had been implanted by fraudsters in the ATM/debit card or EFTPOS systems.

Whilst lacking reliable fraud data, it appears that the most prominent ATM/debit card fraud methods based on its frequency of occurrence in the mass media and occasional fraud incident reported to Bank Indonesia are ATM/debit card skimming in ATMs/EFTPOS machines and card trapping in ATMs.

criminal activity, counterfeiting and non-cash payment system related crime, to expedite the treatment and prosecution of criminal activity.

Bank Indonesia has appealed to banks to continually improve their physical surveillance of ATM machines, in particular those that are located outside branch offices, to ensure that no suspicious equipment is installed as well as monitor unusual transactions. Furthermore, Bank Indonesia has also reminded banks to apply risk mitigation measures against fraudulent activity including formulating an adequate Standard Operating Procedure (SOP), settling transactions according to the SOP, as well as monitoring and applying prudential principles when evaluating and accepting new merchants. Meanwhile, preventive, anti-fraud measures that can be introduced by banks include installing anti-skimmers, CCTV cameras and PIN covers, as well as monitoring the security and cleanliness of their ATM machines.

Of equal importance is for banks to continue rolling out customer education programs regarding the importance of PIN security, regularly changing PIN numbers, and keeping PIN numbers private. Bank customers are also encouraged to pay attention to the physical condition of ATM and EDC machines and report anything suspicious immediately to their nearest branch or authorized personnel.

⁶⁵⁵ See, eg, interview with an ATM Operation Division’s team in one of the major state banks (Jakarta, 17 August 2012) (BO-2). It is difficult to believe that employees of one of most prominent banks in Indonesia who are in charge in the ATM operations were unaware of the risk of malware in ATMs/EFTPOS machines. See also BO-1; BO-3; and BO-5.

Nevertheless, many of the ‘phantom withdrawals’ from consumer bank accounts were not revealed until now. In the absence of incentives for banks to equip themselves with various sophisticated devices for crime/fraud prevention, monitoring and detection, revealing a fraud incident is sometimes not easy for banks. Without ATM CCTV records or CCTV records with a good quality picture, neural network, the state-of-the-art anti malware programs, experienced fraud auditor staff, and good will from banks to exhaustively investigate the possibility of the occurrence of fraud, it is very difficult for banks to detect and reveal a typology of any particular ATM/debit card fraud incident.

From interviews with various banks’ officers in Jakarta in 2012, it is known that banks are reluctant to expand the fraud investigation to the ‘next’ level, such as involving the Indonesian Police Department, and/or tracing the transactions trails to reveal and catch the genuine perpetrators. The most popular reasons given not for not expanding the investigation were to limit the cost of investigation (involving the police means banks have to provide police with ‘operational costs’ for the investigation) and to avoid reputation risk and ‘hassle’ regarding court litigation. Nonetheless, with the change of shareholders in one of the biggest retail banks, the new management urged the fraud department to exhaustively investigate all occurrences of fraud and bring the perpetrators to justice. Even though the goal was to give the message to all the ATM/Debit card fraudsters ‘don’t mess with us’, the effect for consumers was also good. Besides some successfully apprehensions of some ATM/debit card fraudsters that it was claimed had reduced fraud incidents, some previously unrevealed phantom withdrawal cases could also finally be solved. Previous to that investigation, a bank officer admitted that the phantom withdrawal claimed by a consumer was rejected on the basis that consumer must be negligent in some way and this enabled the fraud to occur. The investigation then revealed that the fraudster, using skimming and pin-hole camera device implanted in the bank’s ATM, was the real cause of the consumer’s loss. As result, an arrangement was made with the affected consumer.⁶⁵⁶

⁶⁵⁶ For reasons for bank reluctance to not expand investigations, see eg, BO-2; BO-3; BO-4 and BO-5. In terms of the good will of bank management being very important in contributing to their willingness to reveal fraud incidents, see also interview with Wani Sabu, Division Head Halo BCA, PT Bank Central Asia, Tbk (Jakarta, 14 August 2012).

4.3.3. ATM/Debit Card Identity Theft/Fraud Challenges

With the greater implementation of anti-skimming devices at bank ATMs, it appears that skimming fraud has decreased, while card-trapping fraud is seemingly on the rise in Indonesia, as ATM maintenance officers frequently attest.⁶⁵⁷ The evidence of the latter fraud is easy to detect, since the fraudsters generally will have left the ‘tools’ used in the fraud (such as toothpick, ribbon, or matchstick) inside the ATM slot. On some occasions (depending on the ATMs level of sophistication and specific programming menu), the ATM will switch to malfunction mode and notify bank management as soon as someone puts a foreign device in the ATM slot.

In regard to a skimming attack allegation, a bank can start its investigations by sorting all unauthorised ATM/debit card reports from victimised consumers. Commonly, the bank then can identify ‘the common purchase/transaction point’ either in the ATM or EFTPOS machine as the point of compromise. If the fraudulent activities occurred at ATMs/EFTPOS machines, the bank can confirm this by, for example, conducting direct or on the spot investigation to collect evidence. If the devices have already been removed, the CCTV recording (if any) generally will help.

However, malware fraud generally is more difficult to detect and investigate compared to the other fraud method. Malware is normally programmed so as not to jeopardise ATM/EFTPOS operation and insidiously hidden in the computer root directory. As result, infected ATM/EFTPOS machines will still operate very normally, just as uninfected machines do.

⁶⁵⁷ See Muhamad, ‘Adu Pelayanan di Tengah Ancaman,’ above n 647, 24. In the author’s office, there are more than ten ATMs. ATM maintenance officers admit that almost every day they receive calls to fix jammed ATMs in many ATM locations in Jakarta caused by card-trapping fraud: see, eg, BMO-1; and BMO-2. See also news about card-trapping fraudsters who were more recently apprehended by the Indonesian Police Department: Andri Haryanto, *Wartawan 'KPK' Terlibat Pembobolan ATM Diringkus Polisi* [‘KPK’ Journalist Involved in ATM Theft, Apprehended by Police] (24 April 2013) Detik.com. In other news, seven card-trapping fraudsters had been detained by police when police found at least 42 ‘consumers cards on them, that had been trapped in several ATMs in the cities of Jakarta and Bogor, and Lampung province. The total amount lost was around IDR376.3 million (AUD37.000 approximately). See also Indra Subagja, *Tersangka Pembobol ATM itu Dibekuk Saat Bercinta di Hotel di Alam Sutera* [ATM Theft Suspect was Apprehended While Making Love in Alam Sutera Hotel] (25 June 2013) Detik.com. In the last account, at least four suspects were apprehended after four months conducting card-trapping fraud in several cities (such as Jakarta, Tangerang, Sukabumi, Cirebon and Bogor). One of the card-trapping victims lost about IDR240 million (approximately AUD24,000) in this fraud. See also PIN, ‘Empat Pembobol ATM ditangkap: Polisi, Jangan Panik Jika Kartu ATM Tertelan [Four ATM Thieves Busted: Police, Do Not Panic When ATM Card Get Swallowed],’ *Kompas* 27 September 2013, 27. In the latest card-trapping incident as reported in *Kompas*, four ATM card trappers have been apprehended by the Jakarta Soekarno-Hatta Airport’ police. When interviewed, the thieves admitted that they had frequently conducted the illicit activities, at least six times before being caught.

Attempts to detect malware on ATM/EFTPOS machines, of course, are the first step for banks to take. Banks should have an appropriate program to detect malware. If a bank does not have this, it is impossible to confirm the nature of the fraud, even if the malware is still inside the computer. Even if the bank has installed such a program, it is not easy to detect malware, because it can be located in each ATM or EFTPOS terminal, or in the bank's and/or bank counterpart's database server, such as in a merchant's or switching company's computer. This difficulty is twofold or even greater, if the bank does not have access to investigate its counterparts, such as merchants or switching companies.

Without thorough, open and honest cooperation from banks, it is difficult for the payment system authority and the public to gauge how large is the risk of exposure to each ATM/debit card fraud method. However, without proper investigation using the correct tools, skill and techniques by banks as the party that issued, acquired and/or outsourced its payment card operations, it is also difficult to identify the fraud's point of compromise and by whom and how the fraud was perpetrated.

This complex situation could be exacerbated, if the legal and regulatory framework that regulate fraud (such as in relation to fraud mitigation and fraud liability) is unclear and/or uncertain. Unfair treatment of unauthorised ATM/debit card transactions could lead banks to face legal risk and/or reputation risk. For the innocent victimised consumer, unauthorised ATM/debit card transactions and unfair fraud liability treatment could ruin their life. However, the factor that poses the greatest potential damage to the banking and payment system industry as a whole is probably the significant decrease of consumer trust in banks — that could, in turn, hinder or even halt e-banking development in Indonesia.

4.3.4. The Dearth and Unreliability of ATM/Debit Card Fraud Reports

According to the CPSS, fraud incidents in banks are also of concern to the banking supervisor for three reasons:

On a large scale, it may threaten the solvency of banks and the integrity and soundness of the financial system. Second, it may be indicative of weak internal controls that will require supervisory attention. Thirdly, there are potential reputational and confidence implications, which may also spread from a particular institution to the system.⁶⁵⁸

In accordance with these concerns, the CPSS urged banks to take greater action. In addition to enhancing their internal fraud mitigation, banks were urged to report suspicious activities and significant incidents of fraud to the banking supervisor. Consequently, the banking supervisor (in Indonesia, Bank Indonesia) does need to ensure that appropriate authorities and stakeholders have been alerted to raise awareness so that the spread to other banks or repetition of new and various types of fraud activity elsewhere can be prevented.⁶⁵⁹

Anderson et al in their work have concluded that there are at least five economic barriers to network and information security, one of which barriers is information asymmetries. They note that asymmetric information ‘where one party to a transaction has better information than other ... can be a strong impediment to effective security’. In general, the public has very little information about the effectiveness of many security products and services employed by institutions.⁶⁶⁰

Included in the instances of information asymmetries that are often found in the information security market is a dearth of data sharing concerning vulnerabilities and attacks. Anderson et al believe that publishing quantitative metrics of fraudulent activities to the public or wider community is crucial for reducing information asymmetries. Further, they contend that the main justification for government agencies to collect and publish statistical data regarding companies’ security breaches ‘is the mitigation of information asymmetries by generating useful signals for economic decision making, whether by policymakers, firms, or individuals’.⁶⁶¹ Sullivan (in his

⁶⁵⁸ Committee on Payment and Settlement Systems (CPSS), Bank for International Settlements, 'Core Principles for Effective Banking Supervision (Basel Core Principles)' (Bank for International Settlements, 1997) 31.

⁶⁵⁹ Ibid.

⁶⁶⁰ Anderson et al, above n 338, 18–24.

⁶⁶¹ Ibid 18, 27–8. Individuals and organisations benefit from data on security properties when making consumption and investment decisions. Security professionals in organisations need statistical data to plan

work on payment fraud statistics for the United States) argues that a lack of fraud statistics undermines any ‘war against fraud’ because of the difficulties that authorities endure trying to gauge the dimension of the fraud problem. A lack of accuracy could lead them to target unimportant causes, lead to misdirected efforts, prevent effective coordination among stakeholders, and result in a failure to notice liability shift.⁶⁶²

However, companies tend to be reluctant to expose the incidence and nature of attack events (which would reveal their vulnerabilities) and instead hide such events, even though the attacks can be mitigated more rapidly and effectively if information is shared in a coordinated manner with the wider community.⁶⁶³ Several companies provided reasons for their reluctance to share security breach data, namely: ‘loss of reputation and trust; risk of liability and indemnification claims; negative effects on financial markets; signal of weakness to adversaries; job security and individual career goals.’⁶⁶⁴

Until now, there has been no comprehensive ATM/Debit Card Fraud Report or Payment Card Fraud Report publicly available in Indonesia to raise public awareness about fraudulent activities in e-banking, and smaller rather than larger banks were far more likely to report.⁶⁶⁵ Bank Indonesia, as the banking industry supervisor, has indeed collected fraud reports from banks, but seems reluctant to publish comprehensive data.

and implement appropriate protection and to react to current levels of threat. Accurate statistics can support policy evolution to fight frauds. While consistent, comparable metrics enable greater transparency, better data will bring further rewards in the form of deeper understanding that will in turn lead to better policies in the long term.

⁶⁶² Richard J Sullivan, *The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States* (Federal Reserve Bank of Kansas City, 2009) 1.

⁶⁶³ Anderson et al, above n 338, 18–24. In the USA, fraud information sharing has been tackled by information-sharing associations, security-breach disclosure laws and vulnerability markets. An instance of security-breach disclosure laws to be enacted in the United States was California’s A.B.700 in September 2002, which came into force as Cal Civil Code § 1798.29 in July 2003. It applies to public and private entities that conduct business in California, and requires them to notify affected individuals if personal data under their control is believed to have been acquired by an unauthorised person. A specific instance of the application of this law is where an ATM is fitted by criminals with a skimmer that then steals card details. The bank would be required to notify every customer who had used that machine during the period in which the skimmer could possibly have been in use, regardless of whether they were one of that bank’s customers or not.

⁶⁶⁴ Anderson et al, above n 338, 40–1.

⁶⁶⁵ Payment card fraud figures were never revealed on the Bank Indonesia—Payment System Department website <<http://www.bi.go.id/web/en/Sistem+Pembayaran/>> nor in any Bank Indonesia printed materials, such reports like the Bank Indonesia Annual Report or Bank Indonesia Payment System Report. In contrast, BI has published data related to counterfeiting and fraud in cheque account withdrawals. This can be found in many Bank Indonesia publications. The most disturbing aspect of the fraud reports that has been published is material concerning the presence of unreliable fraud data. An investigation of the raw data that has been sourced has revealed that for years such data had only been submitted by less than one fifth of reporting banks. Most of the banks that reported were small banks; whereas most of big ten banks — that contributed more than 75% of the volume of payment card transactions in Indonesia and

Unlike many other countries such as Australia⁶⁶⁶ and United States,⁶⁶⁷ Bank Indonesia does not publish a fraud report as one aspect within its official report in various Bank Indonesia publications concerning facts related to the country's payment system. The only Bank Indonesia publications in regard to figures for payment card fraud — and such figures are general (that is, without detailed descriptions of the taxonomy of fraud) — are found in Bank Indonesia Payment System Reports or in statements issued by high ranking officers of the Payment System Department in payment system press releases or in statements made at various relevant public occasions, such as seminars on the payment system or for payment system institutional stakeholders such as issuing banks and so on. For instance, the 2011 Bank Indonesia Payment System Report supplied the total number of occurrences of payment card related fraud (for October 2011), which was 1,954 cases of fraud with a total loss of IDR3.08 billion (the report for 2012 revealed 11,468 cases with the value of total losses reaching IDR1.4 billion); but although the reports segregated the data on the basis of various popular fraud *modus operandi* (methods), this tended to confuse the stakeholders since it did not properly follow accepted or common definitions and/or a commonly recognised fraud taxonomy.⁶⁶⁸

commonly also are prominent targets of fraudulent activities — never sent fraud reports to Bank Indonesia for years. Hence the total figure for fraud that is released by Bank Indonesia (as the sole authority in payment system in Indonesia) definitely does not reflect the real level of fraud occurring in payment card operations in Indonesia. This unreliable figure is also exacerbated by the 'dark figure' phenomenon and different interpretations of fraud typology between banks and the central bank. Hence, the available incomplete fraud data are definitely insufficient, fragmented, incomparable and lacking a good metric standard that make it difficult to use as a basis for specific fraud mitigation activities.

⁶⁶⁶ For payment system fraud figures in Australia (most recent and historical data), see Australian Payments Clearing Association (APCA), *Fraud Statistics* <<http://www.apca.com.au/payment-statistics/fraud-statistics>>. The APCA is the self-regulatory body for Australia's payment industry. It has 90 members, including Australia's leading financial institutions, major retailers and other principal payments service providers. In regard to fraud statistics, APCA has been publishing cheque and card fraud statistics since November 2006 as part of the payment industry's commitment to improve disclosure. APCA believes that the fraud figures help consumers and business in Australia understand how fraud occurs so that they can take steps to minimise the risks when using cheques and cards, and allows the industry to monitor fraud trends and develop targeted mitigating strategies.

⁶⁶⁷ See Anderson et al, above n 338, 18, 26. In the US, lack of data sharing about vulnerabilities and fraud attacks has been tackled by information-sharing associations, security-breach disclosure laws and vulnerability markets. Further Anderson et al argue that the point of security breach notification is to provide encouragement or supply incentives for firms to improve the protection of personal data. Competent firms have nothing to fear from breach notification, and should welcome a situation where incompetent firms who 'cut corners' to save money will be exposed (naming and shaming), incur costs, and lose customers. This levels the playing field and prevents the competent being penalised for taking protection seriously.

⁶⁶⁸ For instance, see Herdaru Purnomo, *Duh! Pembobolan Transaksi Kartu Hampir Capai 16.000 Kasus* [Ouch! Payment Card Fraud Almost Reaches 16.000 Cases] (2 January 2012) detik.com <<http://finance.detik.com/read/2012/01/02/144723/1804731/5/duh-pembobolan-transaksi-kartu-hampir>

One way to reduce fraud is by limiting the opportunity for fraudsters to commit fraud. Toughening security has become one of the most popular anti fraud methods to restrain or reduce fraud. However, Bank Indonesia fraud reports do not exhaustively enumerate the types of fraud. Hence, it is impossible to know what sorts of identity theft fraud methods are being employed by fraudsters in Indonesia, resulting in the use of that information to later create a counterfeit card for unauthorised ATM/debit card transactions. Thus the specific types of payment card system frauds that are supposed to be tackled with an appropriate anti fraud tools are hard to identify in the first place. It is difficult to ‘fight a war’ on fraud if the location, actions and nature of the enemy are unknown.

As a consequence, the poor and unpublicised fraud data in Indonesia not only fails to give accurate (and therefore valuable) input for payment system stakeholders to act promptly and accurately to restrain fraud, but could also misdirect fraud policy adopted by the payment system authority. This is because the fraud figures compared to payment card transactions become very sparse and insignificant in terms of special risk mitigation action. From a consumer viewpoint, lack of fraud data — especially for individual bank fraud figures — might create more difficulties for victims of fraud who hope to obtain redress in the court or other alternative dispute settlement body. As Bolton and Hand assert, failure to provide fraud data with reliable figures always makes them difficult to evaluate.⁶⁶⁹ The lack of data sharing concerning vulnerabilities and attacks also creates information asymmetry in terms of the information security industry.⁶⁷⁰ This can lead to create a market failure in the payment system industries. Such information asymmetry can also affect not only the information security industry associated with the banking industry, but also government policy makers, and the public.

A market failure can occur when market participants such as banks do not have incentives to provide a good and timely e-security that prevents or detects breaches and

capai-16000-kasus?f9911023>. In this article, popular fraud methods enumerated are: fraudulent applications, account takeovers, unauthorised use of account numbers, counterfeit cards and skimming, ATM scams, not received items, and identity theft. Payment card fraud figures are derived from the Indonesia Payment System yearly reports for 2011 and 2012.

⁶⁶⁹ Bolton and Hand, above n 257, 236. See also Anderson et al, above n 338, 27. According to Anderson et al, ‘the primary value of statistical data, and the main justification for its collection by government agencies, is to mitigate information asymmetries by generating useful signals for economic decision making, whether by policymakers, firms or individuals’.

⁶⁷⁰ Anderson et al, above n 338, 18.

issues fraud reports. Reasons given for failing to disclose this kind of information is to avoid damage to their reputation and public confidence. Hence, it is obvious that regulators of the payment system can correct this market failure by requiring timely and accurate reporting of e-security breaches/fraud to the authority, and process them meticulously in order to provide valuable information to the payment system industry. This will also help determine appropriate fraud risk mitigation in the country. As Anderson et al have observed, ‘a coordinated view of attacks could prompt faster mitigation to everyone’s benefit’.⁶⁷¹

4.4. Conclusion

A payment card system that uses magnetic stripe cards as a means of data storage combined with a PIN as an authentication tool remains as one of the most widely used payment card technologies today. Nonetheless, it is also notoriously vulnerable to identity theft and fraud. Criminals know that if they are able to obtain consumer data from the magnetic stripe card and its associated PIN (identity theft), they can easily create fake or counterfeit cards that can be used to make unauthorised ATM/debit card withdrawals.

So, as in other jurisdictions, the proliferation of payment card transactions in Indonesia has been followed by a rise in unauthorised ATM/debit card transactions. ATMs and EFTPOS machines along with their networks and data storage systems have become the most frequently used avenues for fraudsters to compromise consumers’ card and PIN data. Inherent vulnerabilities in the ATM/debit card payment system are also exaggerated by the dearth of accurate data and unreliability of the data that is available in ATM/debit card fraud reports.

Identity theft in payment card transactions can be conducted passively or actively — by insider or outsider perpetrator/s. Nevertheless, to identify the fraudsters involved, the fraud methods used and the party or parties that are responsible for fraud prevention/liability for damages, it is necessary to know about the point of compromise for the identity theft. From the type of attack (those perpetrated on ATM/debit card transactions), the point of compromise for identity theft can be divided into three

⁶⁷¹ Ibid.

‘locations’: cardholders themselves; bank ATM/debit card activated terminals and cardholder; and the bank and/or its agent’s network or system.

In situations where the cardholder alone is the point of compromise, fraudsters have attacked and stolen or swapped a consumer’s genuine ATM/debit card and used it to make unauthorised purchases or withdrawals of funds from the consumer’s account (active attack). Fraudsters can determine the consumer’s PIN associated with the stolen ATM/debit card by guessing, ‘cracking’, or extracting it from the consumer identity (such as date of birth), or by social engineering. In addition to situations involving outsider fraudsters, dishonest cardholders themselves can also defraud banks by making fraudulent claims or transaction reversals. This type of identity theft and fraud, however, is not significant in terms of number.

Meanwhile, in situations where the bank consumer activated terminals and cardholders are the point of compromise, the use of skimming devices and the card-trapping fraud method is prominent. Identity theft using skimming devices at ATMs is probably the most popular method employed by fraudsters in Indonesia. Its effectiveness in harvesting hundreds or even thousands of numbers of ATM/debit consumer cards in Indonesia was demonstrated by various identity theft incidents (such as in the late 2010 ATM fraud in Bali, or the Bank BCA and Mandiri skimming fraud of late 2013 / early 2014). All these huge cases of identity theft and fraud in Indonesia, apparently involved international syndicates. Most of the unauthorised withdrawals occurred in outside of Indonesia, in countries such as Canada, Australia, Bulgaria, Malaysia and so on.

Where consumer activated terminals/systems and/or communication networks are the point of compromise, it should be noted that the proliferation of ATMs/EFTPOS machines open a wide doorway for fraudulent activities (as well as benefits for consumers). Relatively unguarded consumer activated terminals and their communication networks make these more vulnerable to fraud attacks. Card skimming, eavesdropping, EFTPOS tampering and malware (to name a few) are some commonly adopted fraud methods at this point (passive attack). Meanwhile, consumer PINs remain able to be easily stolen by the use of installed a pinhole camera, pin-pad overlay, or shoulder surfing method.

In dealing with fraud, enhancement of prevention measures to prevent the occurrence of fraudulent activities — such as by the implementation of cardholder identification and authentication using more advanced technology (such as: ICC/chip card, better encryption tools, stronger PIN and so on) — is very important. However, almost all the (often physical) anti-fraud tools which are ultimately computer-based programs can be circumvented by fraudsters (who use anti jitter, fraudulent anti-skimmer devices, malware, card trapping, and so on). There needs to be implemented additional fraud mitigation methods to avoid more damage to banks and/or consumers, such as neural networks, ‘out of band’ alert, and so on.

Overall, in order to succeed in reducing or neutralising fraud, every fraud prevention, detection and mitigating effort in payment cards (their creation, transaction processing, data storage and so on) should always involve a synergy between banks and their third party affiliates, and consumers. As a payment system owner and/or developer, banks should always improve and update their security features, deliver high quality education material to their consumers concerning payment system risks and fraud methods, and implement good quality neural networks and issue timely consumer transaction reports.

CHAPTER 5 – REGULATION OF ATM/DEBIT CARD TRANSACTIONS, CONSUMER PROTECTION, AND LIABILITY RULES ON UNAUTHORISED ATM/DEBIT CARD TRANSACTIONS IN INDONESIA — WITH A BRIEF COMPARISON TO LOSS ALLOCATION RULES IN THE UNITED STATES AND AUSTRALIA

5.1. Introduction

A well-founded legal basis for the payment system is indisputably very important. Its usefulness is not only to provide a framework and legal certainty for participants and operators who are involved in the payment system, but also to provide a clear and concise statement of the rights and obligations of the payment system participants/operators. Hence, laws and regulations for the payment system that are good, detailed and fair can protect consumers' rights and increase their confidence in banking products and services. In a dispute between consumers and banks over unauthorised ATM/debit card transactions, the party that failed to comply with one or more legal obligation could be deemed negligent or at fault, and thus liable for losses.

This chapter describes the most relevant legislation and regulations for bank ATM/debit card operations in Indonesia. Legal and regulatory framework aspects of ATM/debit card transactions, consumer protection, and liability law in Indonesia are also enumerated in detail. Various BI regulations in regard to its function as the payment system regulator in ensuring the implementation of a robust, efficient, and secure payment card system and consumer protection in payment system services are also described quite exhaustively. It is expected that — in the event of a dispute — these enumerations of the legal and regulatory frameworks for ATM/debit card transactions, will be able to be used as a standard to gauge the extent to which the rights and obligations of banks and consumers have been fulfilled in regard to ATM/debit card transactions/operations.

Consumer protection principles that align with international best practice have become a required standard in banking operations in Indonesia, as can be seen from the Indonesian Banking Architecture Framework enacted by Bank Indonesia. Therefore — even though not exhaustively — the legal frameworks of the United States and

Australia relating to fraud liability provisions for unauthorised ATM/debit card transactions are also presented. In most developed countries, in order to render more equal the position of the consumer's and the business actor, consumer protection regulations tend to produce a more balanced or a pro-consumer risk allocation. The comparison with other countries' regulation this area is deemed important to benchmark whether or not Indonesia's legal and regulatory provision relating to the ATM/debit card fraud liabilities and consumer protection issues are on a similar level and/or comply with international best practice.

5.2. Legal and Regulatory Framework for ATM/Debit Card Transactions in Indonesia

In the operation of the market economy, the payment system is intertwined with and cannot be separated from the monetary and banking system. The payment system itself consists of 'the set of legal frameworks, rules, institutions,⁶⁷² and technical mechanisms for the transfer of money'.⁶⁷³

Bank and payment systems are integral parts of critical economic infrastructure in every country. According to the Gup and Kolari, 'banks are the core of the payments system'.⁶⁷⁴ The role of banks in the payments system takes on an important social dimension because an efficient payments system is vital to economic stability and growth.⁶⁷⁵ Fraud that happens in the payment system, such as illegal access and hacking, can have complex ramifications for a country's entire economy.⁶⁷⁶

Cesare Calari, Vice President of the Financial Sector of the World Bank, in his foreword to the World Bank Working Paper on Electronic Safety and Soundness, contends that it is essential for business to be responsible in securing their electronic business. Besides using technology, 'sound business principles such as responsibility, accountability and trust are also essential to building infrastructure and framework that can support e-business'. He further argues that market participants need the right

⁶⁷² Nowadays, most market economies' structure comprises of two-tiered banking where payment services are provided. Authorized Depository Institutions (such as banks, savings institution, credit union, etc) as the first tier - generally supply payment service and product to its consumers; while the central bank and other payment intermediaries (such as payment network institutions) provide clearing and settlement services to banks.

⁶⁷³ Hancock and Humprey, above n 199, 1575.

⁶⁷⁴ Benton E Gup and James W Kolari, *Commercial Banking: The Management of Risk* (John Wiley & Sons, Inc, 3rd ed, 2005) 9.

⁶⁷⁵ Ibid.

⁶⁷⁶ Glaessner, Kellermann and McNevin, above n 51, 18.

incentives to ensure their best involvement in the system. Hence, an effective legal, regulatory, and enforcement environment is the essential driving factor in creating these incentives.⁶⁷⁷

The proliferation of payment system transactions and the increasing use of technology in the delivery of financial services have attracted public interest in this area. As result, ‘legal and regulatory practice is especially important to define’.⁶⁷⁸

Sullivan argues that ‘confidence in the safety of payments is particularly important’.⁶⁷⁹ Beside technological security features, legal assurance in payment system practice is one of the most important preconditions for banking consumer confidence. The Committee on Payment and Settlement System – Bank for International Settlement has highlighted the importance of a legal framework for payment systems:

It is well established that the legal basis for a payment system is critical to its overall soundness. The legal basis typically consists of framework legislation as well as specific laws, regulations, and agreements governing both payments and the operation of the system. A sound legal basis for a payment system defines, or provides the framework for relevant parties to define, the rights and obligations of operators, participants and regulators. Most risk management mechanisms are based on assumptions about the rights and obligations of parties to payment transactions. Therefore, if risk management is to be sound and efficient, the rights and obligations relating to payment system operations and to risk management itself need to be established with a high degree of certainty.⁶⁸⁰

Nakajima also highlights that the existence of well-founded legal basis is very important, particularly to provide a frameworks and legal certainty for participants and operators involved in the payment system. In contrast, even if a legal framework is available, but fails to provide clear and concise rights and obligations of the payment system participants/operators, it most likely will cause legal disputes in the future.⁶⁸¹ Aligned with Nakajima’s view, the author also concur with Idroes and Sugiarto view which suggest that regulation of banking related to its products and services must be

⁶⁷⁷ Ibid v.

⁶⁷⁸ Ibid 24–5.

⁶⁷⁹ Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 101.

⁶⁸⁰ CPSS, ‘Core Principles for Effective Banking Supervision’, above n 658, 16.

⁶⁸¹ Masashi Nakajima, *Payment System Technologies and Functions: Innovations and Developments* (Business Science Reference, 2011) 91.

addressed in order to protect consumers' rights and increase their confidence in those products and services.⁶⁸²

These scholars' views are deemed very important and it is considered important that they be comprehensively put into practice in Indonesia not only to introduce or restore confidence among banking customers, considering that electronic banking is being implemented on a massive scale in Indonesia, but also for several other reasons as follows: First, these provide the legal basis and the validity of the electronic form of ATM/debit card transactions. Secondly, they are guidelines for banks and consumers in the provision and performance of such transactions, so that ATM/debit card operations can be done effectively and safely. Third, the regulations essentially provide the rights and obligations of the bank and the customer in the transactions. Thus, in the event of an unauthorised ATM/debit card transaction, the parties that were negligent in their compliance with one or more of these regulations could be held accountable for any damages incurred (statutory/regulatory duty).

5.2.1. Legal Framework for ATM/Debit Card Transactions

In Indonesia, there is no statute that specifically governs ATM/debit card transactions. Instead, the legal framework for ATM/debit card transactions is fragmented in various laws that cover the relevant area of ATM/debit card transactions, such as the institution responsible for payment card regulation, recognition of ATM/debit card transactions as an electronic transaction and/or electronic contract, PIN as functional equivalent of electronic signature, the rights and obligations in funds transfer, and so on, as outlined below.

5.2.1.1. Law No 7 of 1992 on Banking as Amended by Law No 10 of 1998 (LB)

In banking operation and practice, *LB* states that 'Banks in Indonesia shall conduct their business according to the principle of economic democracy applying the prudential principle'.⁶⁸³ The prudential principle can be observed in several provisions in *LB*, such

⁶⁸² Ferry N Idroes and Sugiarto, *Manajemen Risiko Perbankan: Dalam Konteks Kesepakatan Basel dan Peraturan Bank Indonesia* [Risk Management in Banking: Within Basel and Bank Indonesia Regulatory Context] (Graha Ilmu, 2006) 16.

⁶⁸³ *LB* art 2. See Yusuf Shofie, *Kapita Selektta Hukum Perlindungan Konsumen di Indonesia* [Consumer Protection Law in Indonesia] (PT Citra Aditya Bakti, 2008) 15; Hermansyah, *Hukum Perbankan Nasional Indonesia* [Indonesia National Banking Law] (Kencana, 2005) 146–7; Neni Sri Imaniyati,

as articles 29(2) and 29(4).⁶⁸⁴ This emphasises the importance of the prudential principle as it is to be applied in every banking business. Therefore, in conducting their business, banks should always abide by the regulations — so that all their business is legitimate.⁶⁸⁵ Fuady argues that banks as a trusted business entity should always comply with all banking regulation as part of their ethical requirements.⁶⁸⁶

Besides observing the prudential principle, banks should also implement other inherent principles in the banking business, which are the fiduciary relation principle⁶⁸⁷ and the ‘know your customer’ principle (‘KYC’).⁶⁸⁸ In order to be able to implement KYC effectively and efficiently, banks ‘shall establish adequate management information systems, which can identify, analyse, monitor and report effectively the characteristics of bank customers’ transactions’,⁶⁸⁹ including any suspicious transaction.⁶⁹⁰

In relation to ATM/debit card transactions, and based on interviews conducted with several banks officers in Indonesia (such as PT Bank Central Asia, PT Bank Mandiri Tbk, PT Bank BNI Tbk, PT Bank Danamon, PT Bank Rakyat Indonesia and so on),⁶⁹¹ typically banks in practice offer consumers an ATM/debit card as an obligatory part of opening a savings account.⁶⁹² However, *LB* does not regulate payment card operations

Pengantar Hukum Perbankan Indonesia [Introduction to Indonesia Banking Law] (Refika Aditama, 2010) 16–17; Djumhana, above n 68, 177.

⁶⁸⁴ *LB* art 29(2): ‘A Bank shall maintain its soundness in accordance with the provisions concerning the adequacy of capital, quality assets, quality of management, liquidity, profitability, solvency, and other aspects related to the operations of a bank, and shall be required to conduct operations in accordance with the prudential principle.’ *LB* art 29(4): ‘In the interest of its Customer, a Bank shall provide information concerning the risk of possible losses relating to Customer transaction[s] conducted through a Bank.’

⁶⁸⁵ Hermansyah, above n 683, 147.

⁶⁸⁶ Djumhana, above n 68, 197.

⁶⁸⁷ See *LB* art 29(4). See also Djumhana, above n 68, 337; Imaniyati, above n 683, 17–18. The fiduciary principle is a principle of trust which underlies the relationship between banks and bank customers. Banks seek funds from the public to deposit in trust, so that each bank needs to keep its bank healthy while maintaining public confidence.

⁶⁸⁸ Peraturan Bank Indonesia Nomor: 3/10/PBI/2001 Tentang Penerapan Prinsip Mengenal Nasabah [Bank Indonesia Regulation Number: 3/10/PBI/2001 Concerning Implementation of Know Your Customer Principles]. Know your customer principle (KYC) is the principle applied by banks to recognize and know the identity of customers, monitor customer transactions, including reporting any suspicious transactions related to customer accounts.

⁶⁸⁹ *Ibid* art 9.

⁶⁹⁰ *Ibid* art 12. The meaning of ‘suspicious transaction’ is a transaction that is not consistent with a customer’s profile and characteristics.

⁶⁹¹ Interviews with BO-1; Bo-2; BO-3; Bo-4 and BO-5. Officers of these banks were interviewed during field research in Jakarta, Yogyakarta and Denpasar (Indonesia, July to August 2012).

⁶⁹² See Peraturan Bank Indonesia Nomor: 3/10/PBI/2001 Tentang Penerapan Prinsip Mengenal Nasabah [Bank Indonesia Regulation Number: 3/10/PBI/2001 Concerning Implementation of Know Your Customer Principles] art 1(9): ‘Savings [are] a deposit which can only be withdrawn according to certain agreed conditions, but which shall not be withdrawn by means of a cheque, “bilyet giro”, and/or other equivalent instruments.’ Bilyet Giro is a payment system instrument that functions almost like a cheque,

in particular, apart from a provision that bank operations may encompass various activities, including those related to transferring money, either on its own behalf or at the request of the customer, and conducting credit card business.⁶⁹³

Unfortunately, there is no direct provision in this law that governs legal protection for consumers' funds (which they have deposited in the bank) in the event of fraud. Protection only applies when the bank is closed by the authority or goes into bankruptcy.⁶⁹⁴

5.2.1.2. Law Number 23 of 1999 on Bank Indonesia as Most Recently Amended by Law Number 6 of 2009 on the Stipulation of Government Regulation in Lieu of Law Number 2 of 2008 on the Second Amendment to the Law Number 23 of 1999 on Bank Indonesia (*LCB*)

Historically, the role of Bank Indonesia in the payment system especially in regard to cash and non-cash payments (giro payments) circulation was first recognised under article 7(2) of Law No 11 of 1953 on Establishment of the Basic Law of Bank Indonesia.⁶⁹⁵ Bank Indonesia's role in the payment system was further developed by the enactment of Law No 13 of 1968 on Central Bank (*LCB*). According to article 30(a) of the *LCB*, Bank Indonesia as a central bank is mandated to support the Indonesian government, among other things, by expanding, smoothing and regulating giro payment mechanism and providing inter-bank clearing.⁶⁹⁶

Arising from the need for better objectives and focus for the independent central bank in Indonesia, the Government enacted Law No 23 of 1999 on Bank Indonesia to replace *LCB 1968*. Law Number 23 of 1999 was later amended by Law No 6 of 2009 on Stipulation of Government Regulation in Lieu of Law No 2 of 2008 on the Second

but cannot be cashed; instead, the monetary value that is contained in the instrument can only be stored in the beneficiary's bank account. It has also a maturity date. This means that the value on the bilyet giro only can be claimed from the maturity date onward.

⁶⁹³ Ibid art 6.el.

⁶⁹⁴ Sentosa Sembiring, *Hukum Perbankan: Edisi Revisi* [Banking Law: Revision Edition] (Mandar Maju, 2012) 181.

⁶⁹⁵ *Undang-Undang Nomor 11 Tahun 1953 Tentang Undang-Undang Pokok Bank Indonesia* [Law Number 11 of 1953 on Bank Indonesia Core Act] (Indonesia). Article 7(2) of this act gives Bank Indonesia authority to circulate money in Indonesia, including expanding a giro payment. See also Tim Buku Media Indonesia, Tim Penulis Universitas Islam Indonesia and Tim Buku Bank Indonesia, *Era Baru Transformasi Bank Sentral [New Era of Central Bank Transformation]* (Media Indonesia Publishing, 2010) 28. This act has been repealed.

⁶⁹⁶ *Undang-Undang Nomor 13 Tahun 1968 Tentang Bank Sentral* [Law No 13 of 1968 on Bank Sentral] (Indonesia). This act has been repealed.

Amendment Law No 23 of 1999 on Bank Indonesia Becomes Law (*LBI*).⁶⁹⁷ *LBI* not only guaranteed the independence of Bank Indonesia, but also highlighted its extensive payment system role to regulate and safeguard the smoothness of the payment system in Indonesia. Pertaining to this task, Bank Indonesia has various powers in the payment system, including power to license payment system services, oversight, power to determine the use of payment instruments, regulate and operate the interbank clearing system and the final settlement of interbank payment transactions, and to issue and circulate Indonesia's currency.⁶⁹⁸

In implementing the task of regulating banks, Bank Indonesia is authorised to prescribe banking regulations that contain the prudential principles. Typically, such banking regulation will be prescribed in the form of a Bank Indonesia Regulation. It is also very common for the Bank Indonesia Regulation to prescribe further details in a Bank Indonesia Circular Letter⁶⁹⁹ as can be seen in section 5.2.2 below.

5.2.1.3. Law Number 11 of 2008 on Information and Electronic Transactions (*LIET*)

LIET is Indonesia's first comprehensive cyber-law and cyber-crime law that adopts the major provisions of the Model Law on E-commerce and the Model Law on Electronic Signatures issued by the United Nations Commission on International Trade Law,⁷⁰⁰ and the Council of Europe *Convention on Cybercrime* 2001.⁷⁰¹

⁶⁹⁷ *Undang-Undang Republik Indonesia Nomor 23 Tahun 1999 Tentang Bank Indonesia Sebagaimana Telah Diubah Terakhir Dengan Undang-Undang Republik Indonesia Nomor 6 Tahun 2009 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2008 Tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 1999 Tentang Bank Indonesia Menjadi Undang-Undang* [Law No. 23 of 2009 on Bank Indonesia as latest amended by Law No. 6 of 2009 on Stipulation of Government Regulation in Lieu of Law No. 2 of 2008 on Second Amendment to the Law No. 23 of 1999 on Bank Indonesia Into Act] (Indonesia) (*'LBI'*) arts 7, 8(b). This payment system role (along with other monetary and banking roles) became the third pillar of Bank Indonesia's task in achieving its objective: 'to establish and maintain rupiah stability'. Bank Indonesia's mandate to regulate and supervise banks has been moved to another independent body, namely the Otoritas Jasa Keuangan/Financial Service Authority. See *Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan* [Law No 21 of 2011 on Financial Service Authority] (Indonesia).

⁶⁹⁸ *LBI* arts 15–23. See also *LBI* 1999 art 32 pertaining to Bank Indonesia's role to regulate and develop an interbank information system.

⁶⁹⁹ *LBI* art 1(8). Bank Indonesia Regulations are the legal provisions which are prescribed by Bank Indonesia and bind every individual or entity. They are published in the State Gazette of the Republic of Indonesia. For instance of *LBI* mandate to prescribe *LBI* 1999 regulation as a Bank Indonesia Regulation, see *LBI* arts 10(3), 14(5), 15(2).

⁷⁰⁰ UNCITRAL, 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment' (United Nations, 1996), above n 235. See also Mark Flaming, Klaus Prochaska and Stefan Staschen, 'Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia' (CGAP, 2009)

One of the considerations of the Government in issuing this law was to support the fast development of information technology via law and regulatory infrastructure, so that the use of the information technology could be protected from any misuse with regard to Indonesian religious, social and cultural values.⁷⁰²

The *LIET* is a very important piece of legislation for the development of e-banking, in particular the payment card system in Indonesia. Even though the Act does not directly regulate e-banking transactions, it is concerned with the validity or acceptability of, among other things, electronic information,⁷⁰³ electronic documents,⁷⁰⁴ electronic transactions,⁷⁰⁵ electronic systems,⁷⁰⁶ electronic signatures,⁷⁰⁷ and electronic contracts,⁷⁰⁸ for the purposes of EFTs provided that they are generated by an electronic system in compliance with the requirements set out in the *LIET*.⁷⁰⁹

<<http://www.cgap.org/gm/document-1.9.34817/Branchless%20Banking%20Diagnostic%20in%20Indonesia.pdf>>, 7.

⁷⁰¹ The convention document can be retrieved from the Council of Europe website: <<http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>>. See also Ahmad M Ramli, Pager Gunung and Indra Apriadi, Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik [Toward Legal Certainty in Information and Electronic Transaction] (*Departemen Komunikasi dan Informatika Republik Indonesia* 2006) 69–81.

⁷⁰² See consideration section in *LIET*.

⁷⁰³ See *LIET* art 1(1): ‘Electronic Information is one or a set of electronic data, including but not limited to writing, voice, drawing, map, design, photo, electronic data interchange (EDI), electronic mail, cable wire, telex, telecopy, or similar kind, character, sign, numeral, access code, symbol or perforation which after being processed have meaning or can be understood by anyone capable to understand it.’

⁷⁰⁴ Ibid art 1(4): ‘Electronic Document is any electronic information made, forwarded, sent, received, or stored in analogue, digital, electromagnetic, optical form or similar kind, which can be seen, presented, and/or heard through computer or electronic system, including but not limited to writing, voice, drawing, map, design, photo or similar kind, character, sign, numeral, access code, symbol or perforation which have meaning or can be understood by anyone capable to understand it.’

⁷⁰⁵ Ibid art 1(2): ‘Electronic Transaction is a legal action performed by using computer, computer network, and/or other electronic media.’

⁷⁰⁶ Ibid art 1(5): ‘Electronic System is a set of tools and electronic procedures with the function to prepare, collect, process, analyse, save, present, publish, send, and/or to disseminate electronic information.’

⁷⁰⁷ Ibid art 1(12): ‘Electronic Signature is a signature consists of electronic information attached to, associated with or related to the other electronic information as an instrument of verification and authentication.’

⁷⁰⁸ Ibid art 1(17): ‘Electronic Contract is an agreement between the parties made through electronic system.’

⁷⁰⁹ See *ibid* art 11. For instance, the requirements for the electronic signature to be valid and legally binding are: a) The data about the making of electronic signature relates only to the signatory; b) The data about the making of electronic signature at the time of electronic signing process is only in the authority of the signatory; c) Any and all changes to the electronic signature that occur after the time of signing must be acknowledged; d) Any and all changes to the electronic information related to the electronic signature after the time of signing must be acknowledged; e) There is a certain method used to identify the signatory; f) There is a certain method to indicate that the signatory has given approval to the related electronic information.

In relation to ATM/debit card transactions, besides giving legal assurance to the operation of payment card system electronically, *LIET* is the first law in Indonesia that clearly recognises the legal status of consumer activated terminals such as ATM/EFTPOS machines, known as an electronic agent, and the PIN as the substitute for a handwritten signature.⁷¹⁰ The law also provides flexibility for the parties conducting electronic transactions to undertake such transactions directly between themselves, through their proxies, or through an electronic agent.⁷¹¹

In the case of disputes between parties involved in an electronic transaction, the law provides the possibility for any person to file a lawsuit against the provider of the electronic system which has caused any loss to society.⁷¹² A civil claim can be filed with the court or other alternative dispute resolution institution pursuant to the laws and regulations.⁷¹³ As a proof, electronic information and/or electronic document and/or its printout can be used as an extension of legitimate electronic evidence in the existing procedural law.⁷¹⁴

5.2.1.4. Government Regulation Number 82 of 2012 on The Operation of Electronic System and Transaction (*GR-OEST*)

GR-OEST is a Republic of Indonesia Government Regulation that was put in place to stipulate *LIET* in greater detail.⁷¹⁵ Therefore, it is expected that it could be use as a guideline for the use of information technology in Indonesia, especially for electronic system operators in interpreting and implementing *LIET* in practice.

On the other hand, *GR-OEST* also provides many obligations for electronic system providers to comply with in their operations. Hence, in practice the *GR-OEST* can also be used along with other relevant regulations,⁷¹⁶ as a ‘benchmark’ in assessing the

⁷¹⁰ Ibid art 1(8): ‘Electronic Agent is a part of an electronic system made to perform an action automatically toward certain electronic information, performed by [the] Person (person here refers to natural person or legal institution/company).’

⁷¹¹ Ibid art 21(1).

⁷¹² Ibid art 38(1).

⁷¹³ Ibid art 39(1), (2).

⁷¹⁴ Ibid art 5(2).

⁷¹⁵ *Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik* [Government Regulation of the Republic of Indonesia Number 82 of 2012 on The Operation of Electronic System and Transaction] (Indonesia) (*‘GR-OEST’*).

⁷¹⁶ Such as the Bank Indonesia Regulation on risk management, security improvement obligation, and consumer protection.

adequacy of the electronic system provider's compliance with the associated information technology regulation in Indonesia.

In general, the *GR-OEST* regulates various aspects related to electronic system operations, electronic agents, electronic transaction operations, electronic signatures, electronic certificate operations, the Trustmark certification agency and domain name management,⁷¹⁷ as follows below.

5.2.1.4.1. Electronic Systems

GR-OEST regulates the operators of electronic systems (such as bank with its e-banking product) so that they are obliged to ensure (among other things) that:

- electronic system operators for public services shall guarantee the software that they use so that such a system is secure and reliable. For instance, they are to ensure that software is free from hidden malicious codes such as ‘Trojan viruses’, ‘worms’ and from the possibility of ‘backdoor’ access.⁷¹⁸
- service level agreements, information security agreements, and information security and internal communication facilities are available. The operator also is obliged to guarantee that each component and the integration of the entire electronic system could be able to be operated as it should.⁷¹⁹
- a risk management policy is applied to each damage or loss that may occur. ‘Apply risk management’ here means that the operator should do a risk analysis and formulate mitigation and handling measures to cope with threats, disturbances, and obstacles to the electronic system being operated.⁷²⁰
- the operator possesses a good governance policy, standard operational procedures and accountable audit mechanisms;⁷²¹ the operator should also provide an audit trail for all electronic system operational activities. The audit trail record is used for oversight, law enforcement, dispute resolution, verification, testing and other kinds of examinations. The operator shall notify consumers every time their transactions have been successfully conducted, and assure that the audit trail function can also detect intrusion efforts and/or intrusion trail for review and evaluation purposes.⁷²²

⁷¹⁷ *GR-OEST* art 2.

⁷¹⁸ Ibid art 7.

⁷¹⁹ Ibid arts 12, 23.

⁷²⁰ Ibid art 13.

⁷²¹ Ibid arts 14, 16, 17.A

⁷²² Ibid art 18.

- the operator safeguards the confidentiality, integrity, availability, authenticity, accessibility, traceability of personal data/electronic information or document that they have managed. In cases where the confidentiality of data is being compromised, the operator is obliged to give a written notice to the personal data owner.⁷²³
- the operator owns and applies security procedures (both for fraud prevention and mitigation, such as by applying antiviral software, firewalls, intrusion detection systems, and so on) and facilities to secure the electronic system to avoid disturbances, failures and damage;⁷²⁴
- the operator is obliged to protect users and the public from loss caused by the operation of its electronic system. Anyone working in the electronic system is obliged to secure and protect the electronic system’s infrastructure and facilities or any information transferred through the electronic system. The operator is also obliged to provide, educate and train personnel in charge of and responsible for securing and protecting infrastructures and facilities of the electronic system.⁷²⁵

5.2.1.4.2. Electronic Agents

GR-OEST regulates in such a way that the operator of the electronic system can function on its own or through an electronic agent. The electronic agent shall operate in accordance with the rules including that:

- the electronic agent used can be in the form of visual, audio, electronic data, and other forms;⁷²⁶
- the electronic agents are obliged to contain or to convey information pertaining to consumer protection, which at least includes information pertaining to the identity of the electronic operator, transacted object, worthiness of security feature of the electronic agent, method to use the tools, and call centre number for a consumer’s complaint;⁷²⁷

⁷²³ Ibid arts 15, 22.

⁷²⁴ Ibid arts 19, 20. ‘ “Disturbances” are any action which is destructive in nature or causes serious impacts to the electronic system such as making it fail to function properly; “failures” are a part or full cessation of all electronic system functions which are essential in nature, causing the electronic system to fail to function properly; “damages” are the impacts of the failure or the damages of electronic system that caused a legal impact to users, operator, and other third party either materially or immaterially.

⁷²⁵ Ibid arts 27, 28.

⁷²⁶ Ibid art 34.

⁷²⁷ Ibid art 35.

- in the operation of electronic agents, the operator is obliged to consider the principles of: prudence, security and integration of the information technology system, security control over electronic transaction activities, cost effectiveness and efficiency, and consumer protection in accordance with laws and regulations. The operator is also obliged to have and run standard operating procedures that fulfil the user data security control principle in regard to electronic transactions, which includes confidentiality, integrity, availability, authenticity, authorisation and non-repudiation.⁷²⁸
- the operator must conduct an authentication of identity and authorisation test for each user that accesses system, database and is involved in the application of electronic transactions. The operator is also required to have and implement policies and procedures to take action if there is an indication of data theft.⁷²⁹
- the operator shall prepare and implement methods and procedures to protect the data, notation, and information related to electronic transactions. The operator also is required to have procedures for handling unexpected events quickly and appropriately to mitigate the impact of an incident, fraud, and the failure of the electronic system.⁷³⁰
- the operator is obliged to prepare and stipulate a procedure to ensure electronic transaction that cannot be denied by the consumers (non repudiation).⁷³¹

5.2.1.4.3. Electronic Transaction Operation

GR-OEST states that the operator of electronic transactions is obliged to ensure amongst other things:

- Electronic transaction operators in the Indonesia jurisdiction must pay attention to security, reliability, and efficiency aspects as regulated by laws and regulations enacted by the associated oversight and regulatory authority. In regard to the payment system conducted by the banking industry, the sole authority with the responsibility for such oversight and the regulatory role is Bank Indonesia, the Central Bank of the Republic of Indonesia.⁷³²

⁷²⁸ Ibid art 38.

⁷²⁹ Ibid art 39(a)–(d).

⁷³⁰ Ibid art 39(e), (g).

⁷³¹ Ibid art 39(2).

⁷³² Ibid arts 43(1), 43(3), 45(2).

- Electronic transaction operations performed by parties must consider good faith, the prudential principle, transparency, accountability, and reasonability. ‘Reasonability’ refers to adhering to prevailing propriety consistent with business recent habits and practices.⁷³³

5.2.1.5. Law No 3 of 2011 on Fund Transfer (*LFT*)

At the moment, Indonesia still does not have a specific Payment System Act in place. Instead, Bank Indonesia and the Indonesian government have initiated promulgation of the Law on Fund Transfer (*LFT*). One of the ultimate goals of the *LFT* was to provide legal certainty and protection for all the parties that are involved in fund transfer system operations. Having a comprehensive legal basis for fund transfer operations either domestically or internationally (cross-border fund transfer), it can be expected that the ultimate objective of payment system, which is to safeguard the safety and smooth operation of the payment system, could always be achieved.⁷³⁴

Pertaining to ATM/debit card operation, the *LFT* in essence gives legal recognition for fund transfer activities using ATM/debit cards in Indonesia. In particular, the *LFT* has legally acknowledged various fund transfer activities both domestically and cross-border, to be initiated or processed in the electronic form, among other things in relation to fund transfer instruction,⁷³⁵ electronic signature,⁷³⁶ and the authentication and acceptance process.⁷³⁷ Similarly to the *LIET*,⁷³⁸ the *LFT* also extends the existing procedural law,⁷³⁹ by accepting electronic information, electronic documents and/or their print-outs as valid legal evidence.⁷⁴⁰

However, apart from delay and error liabilities as regulated in articles 54 and 55 of *LFT*, the Act does not regulate unauthorised funds transfer transactions nor provide fraud

⁷³³ Ibid art 46.

⁷³⁴ Elucidation of *LFT*.

⁷³⁵ Ibid art 7(1): A fund Transfer Order may be transmitted in a written or electronic form.

⁷³⁶ Ibid art 77.

⁷³⁷ Ibid arts 1(14), 1(15): “‘Authentication’ is the procedure performed by a receiving provider to ensure that a funds transfer order, or amendment or cancellation thereof, is indeed issued by the party named in the funds transfer order as the rightful sender; ‘Acceptance’ is an action by a receiving provider indicating approval to execute or fulfil the contents of a received funds transfer order.’

⁷³⁸ See Chapter Five / section 5.2.1.3.

⁷³⁹ *LFT* art 76(2): ‘Electronic information, electronic documents and/or printouts thereof as referred to in paragraph (1) constitute an extension of valid legal evidence in accordance with the applicable code of legal procedure.’

⁷⁴⁰ Ibid art 76(1): ‘In funds transfer activities, electronic information, electronic documents and/or printouts thereof constitute valid legal evidence’.

liability rules for the parties involved in the fund transfer system. Hence, this Act itself fails to give a clear guidance to overcome prolonged disputes between consumers and banks in regard to unauthorised ATM/debit card transactions in Indonesia.

5.2.2. Regulatory Framework for ATM/Debit Card Transactions: Bank Indonesia Regulations Concerning the Prudential Principle, Risk Management, and Security Improvement

In e-banking practices in Indonesia, e-banking is regulated by Bank Indonesia, the Central Bank of Republic Indonesia as provided by its mandate given by *LB*.⁷⁴¹ The *LB* provides the foundation for Bank Indonesia to regulate and safeguard the smooth operation of the payment system in order to achieve an efficient, expeditious, safe and reliable payment system.⁷⁴² A payment system in this Act is defined as ‘a system which includes regulations, institutions, and mechanisms, used in conducting a transfer of funds in order to fulfil an obligation arising out of an economic activity’.⁷⁴³

Bank Indonesia’s core task in payment system has been enumerated in articles 15 to 23 of the *LB*. In these articles, authority is given to Bank Indonesia to act and issue licences to any institutions that provide payment system services; payment systems institutions are obliged to report their activities; and payment system instruments are designated.⁷⁴⁴ The licensing role aims to ensure that all payment system providers fulfil minimum requirements in security and efficiency; the reporting obligation is introduced so that Bank Indonesia may oversee payment system data and practices; the payment system instruments are designated to ensure that all instruments used by the community meet the security requirements in accordance with the prudential principle and in compliance with international standards and best practice.⁷⁴⁵

The increasing development of non-payment instruments, especially payment cards and electronic based payment in Indonesia,⁷⁴⁶ has pushed Bank Indonesia (as the provider

⁷⁴¹ Bank Indonesia is the sole government authority body that under *LB* 1999 that is authorised to provide and regulate the payment system. In accordance with this mandate, Bank Indonesia articulates its task to regulate payment system by enacting Bank Indonesia Regulations and/or Bank Indonesia decrees.

⁷⁴² See *LB*, art 8.

⁷⁴³ *Ibid* art 1(6).

⁷⁴⁴ *Ibid* art 15(1).

⁷⁴⁵ *Ibid* arts 15–23. See also Bank Indonesia, *Ikhtisar Undang-Undang No. 23 Tahun 1999 Tentang Bank Indonesia* [Excerpt of Law of 1999 on Bank Indonesia] (*Indonesia*) (2008) Bank Indonesia <<http://www.bi.go.id/NR/rdonlyres/C7402D01-A030-454A-BC75-9858774DF852/13303/ikhtisar.pdf>> 4.

⁷⁴⁶ See full details of the development of payment card industry (figures, infrastructures, institutions, and so on) in Appendix 1.

and regulator of the national payment system in Indonesia) to undertake various anticipated actions, including the first payment card regulation in 2005.⁷⁴⁷ The enactment of payment card regulation was expected to encourage the creation of a less-cash society through the use of non-cash transactions that are more secure, prudent, and consumer protection oriented, which then (it was hoped) would be able to create greater security and increased comfort in the community in regard to payment card transactions. This was expected to ultimately improve the efficiency of the national economy and contribute to greater economic well-being.⁷⁴⁸

As the regulator of the card payment industry, Bank Indonesia has issued various regulations for the implementation of payment system policy in the form of Bank Indonesia Regulations and Bank Indonesia Decrees.⁷⁴⁹ Not only has it issued new regulations, Bank Indonesia has also from time to time revised the out-of-date payment card regulation in an effort to improve prudential and consumer protection aspects in payment card operations.⁷⁵⁰ Bank Indonesia Regulations not only cover bank but also non-bank institutions;⁷⁵¹ however, given that ATM/debit cards can only be issued by the bank as an institution that can collect and store consumers' funds, this thesis only addresses regulation on banks as issuers of ATM/debit cards and their counterparts in payment card operations.⁷⁵²

Basically, Bank Indonesia regulations and decrees consist of at least three different aspects, namely prudential regulation, risk mitigation and consumer protection aspects.⁷⁵³ However, instead of being under one comprehensive regulation, these three

⁷⁴⁷ Karnoto Mohamad et al, *Mendorong Langkah Maju Menuju Less Cash Society [Encouraging Step Forward toward Less Cash Society]* (Infobank, 2008) 125. The first payment card regulation enacted by Bank Indonesia was Bank Indonesia Regulation Number 6/30/PBI/2004 on 28 December 2004 Concerning Operation of Card-Based Payment Instrument Activities. This regulation was repealed in 2005. The latest Bank Indonesia Regulation concerning Payment Card is Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Card Based Payment Instrument Activity as amended by Bank Indonesia Regulation Number 14/2/PBI/2012] (*'BIR-CBPI'*)

⁷⁴⁸ Mohamad et al, above n 747, 60.

⁷⁴⁹ *LBI* art 15(2).

⁷⁵⁰ Bank Indonesia, '2011 Economic Report on Indonesia: Indonesia's Economic Resilience: Amid Global Uncertainty' (Bank Indonesia, 2011) 157.

⁷⁵¹ See *BIR-CBPI* arts 1(2), 2(1), 5(1), 7(1).

⁷⁵² All the disputes concerning unauthorised transactions were between ATM/debit card issuer bank and its consumer. Therefore, this thesis tries to distil Bank Indonesia Regulations and decrees pertaining to each role of the payment system actors in the ATM/debit card transactions, in particular to the issuer bank.

⁷⁵³ Another aspect (among others) is Bank Indonesia Payment System Oversight and its administrative aspects. However, these aspects will not be discussed in this thesis. See also Nuryanti and Dewi, above n 649, 96–8. According to Nuryanti and Dewi, Bank Indonesia's policy on e-payment principally

aspects are scattered among various Bank Indonesia regulations and decrees. Regulations concerning payment cards are generally enacted by the Bank Indonesia Payment System Department. While some other regulations pertaining to risk management (including information security provisions), prudential regulation and consumer protection for e-banking activities were enacted by the Payment System Department, some were also enacted by the Bank Indonesia Banking Department.⁷⁵⁴

5.2.2.1. Prudential Provisions for Payment Cards

As a financial institution that manages huge amounts of consumers' funds, a bank should always apply the prudential principle in all their activities to guarantee the safety of consumer funds and to create a sound, robust and secure banking industry in the Indonesia. Every bank in Indonesia is obliged to apply the prudential principle in their activities.⁷⁵⁵ Consequently, Bank Indonesia as the bank regulator and supervisor, has issued various provisions related to prudential principles. The prudential provisions were developed by referring to best practice and international standards.⁷⁵⁶

In regard to the prudential principles aspect of ATM/debit card operation,⁷⁵⁷ various provisions make them manifest in the Bank Indonesia regulations and decrees. Among other things, regulation requires that a bank which intends to act as a Principal,⁷⁵⁸ Issuer,⁷⁵⁹ and/or Acquirer⁷⁶⁰ obtain approval from Bank Indonesia.⁷⁶¹ Some of the

emphasises on three regulating aspects. First, the payment system aspect, which consists of, among other things, regulations to ensure that e-payment instruments can be used safely, efficiently, promptly and reliably; second, the prudential regulation aspect, consisting of regulation to ensure the quality and integrity of e-payment activity and to enhance security and minimise fraud on e-payment activity; and third, the cardholder protection aspect, consisting of regulations to encourage issuers to implement consumer protection aspects and to educate cardholders in using their cards.

⁷⁵⁴ See *Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan* [Law No 21 of 2011 on Financial Service Authority] (Indonesia). According to this law (effective 31 December 2013), the regulatory and supervisory functions, duties, and powers of financial services activities in the sectors of Capital Markets, Insurance, Pension Funds, Finance Institutions, and other financial services institution such as banking, shall pass *from* the Minister of Finance and the Capital Market and Financial Institution Supervisory Agency, and Bank Indonesia, *to* the Financial Service Authority. However, the remaining central bank functions such as payment system and monetary policy, will still reside with Bank Indonesia, as the Republic of Indonesia's central bank. Hence, this thesis focuses only on Bank Indonesia's payment system regulations and other Bank Indonesia's relevant regulations.

⁷⁵⁵ *LB* art 2.

⁷⁵⁶ Bank Indonesia Regulation Number: 9/4/PBI/2007 Concerning Revocation of Some Decrees of the Board of Managing Director of Bank Indonesia and Bank Indonesia Circular Letters Related to Banking Prudential Principles.

⁷⁵⁷ Shofie, '*Kapita Selekta Hukum Perlindungan Konsumen di Indonesia*', above n 683, 15.

⁷⁵⁸ *BIR-CBPI* art 1(8): 'Principal is Bank or Non-Bank Institution responsible for managing the system and/or network among its members, regardless [whether] act[ing] as an issuer and/or acquirer, in payment card transaction in which collaboration to its member was based on a written agreement.'

⁷⁵⁹ *Ibid* art 1(9): 'Issuer is Bank or Non-Bank Institution who issued payment card.'

minimum requirements that must be met by the bank in order to obtain approval as payment card issuer include a number of documents that provide information regarding:

- risk management readiness (which includes internal regulation concerning the active supervisory role of commissioners and directors, in particular in regard to management of payment card risks and the security policy for issuing payment card instruments);
- security control procedures, such as PIN management and card delivery, segregation of duties in the payment card process, authentication process, audit trail of cardholder activities, data integrity assurance, and confidentiality of cardholder identity;
- reputation risk and operational risk management, which should at least include: information regarding benefit and risk of having payment card instruments, disaster recovery plan, and business continuity plan. Specific to operational risk management, the issuer of payment cards has an obligation to manage operational risk, by (among other things) using proven technology which includes the presence of various aspects of an information technology security system, such as two factor authentication, confidentiality, data integrity, authentication system and data, non-repudiation, and availability.⁷⁶²
- audit trail system and procedures;
- good results from an information technology audit that show the employment of proven technology in payment card operations and fulfilment of requirements for security on system and network;⁷⁶³
- the bank as an acquirer has an obligation to educate and nurture its merchants, and stop cooperation with merchants if they perform actions that could harm others, such as collusion with fraudsters to steal consumers' card data, perform cash withdrawal transactions, and so on.⁷⁶⁴
- cooperation of the bank with other parties (such as a switching company, card manufacturer, and so on) to provide support for payment card operations. The banks are obligated to fulfil all Bank Indonesia's prudential provisions concerning

⁷⁶⁰ Ibid art 1(10): 'Acquirer is Bank or Non-Bank Institution that [has] cooperation with merchant, which [is] able to process payment card data issued by other parties.'

⁷⁶¹ Ibid arts 2(2), 5(2), 7(2).

⁷⁶² See Surat Edaran Bank Indonesia No. 15/23/DASP Perihal Penyelenggaraan Transfer Dana [Bank Indonesia Circular Letter No. 15/23/DASP Concerning Fund Transfer Operation] art II.A.1.a.

⁷⁶³ *BIR-CBPI* arts II, VII.F.

⁷⁶⁴ Ibid art 8(1)–(2).

their relations with other parties, and abide by the Bank Indonesia Regulation concerning Implementation of Information Technology Risk Management for Banks. Such banks also have to have evidence regarding their counterparts' system reliability, security and confidentiality (should be proven by an audit of information technology by an independent IT auditor).⁷⁶⁵

5.2.2.2. Risk Management for Payment Cards

Bank Indonesia has set forth some risk management provisions in various Bank Indonesia regulations, to ensure that bank payment card operations are in conformity with Bank Indonesia's minimum risk management standard.⁷⁶⁶ According to Bank Indonesia, risk management is a series of procedures and methodology employed to identify, measure, monitor, and control risks arising from the business operations of a bank.⁷⁶⁷ Risks that have to be managed encompass various risks such as credit risk, market risk, liquidity risk, operational risk, legal risk, strategic risk and compliance risk.⁷⁶⁸

In general, banks are obliged to apply effective risk management principles in their operations, which should be commensurate with the goal, business policy, size and complexity of its business, and the capacity of the bank. Application of a bank's risk

⁷⁶⁵ Ibid arts 13, 21. The provision of article 21 of *BIR-CBPI* before it was amended has a 'liability rule' regarding cooperation with other parties. It was a rule that the Issuer of the payment card should be responsible for the cooperation scheme. However, this rule was eliminated when *BIR-CBPI* was amended. See also *BIR-CBPI* art VII.D. See also *Peraturan Bank Indonesia Nomor 13/25/PBI/2011 Tentang Prinsip Kehati-hatian Bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain* [Bank Indonesia Regulation Number 13/25/PBI/2011 Concerning Prudential Principle for Commercial Bank which Outsource Some Parts of Its Works to Other Party] ('*BIR-Outsource to Other Party*'); *Surat Edaran Bank Indonesia No. 14/20/DNPN Perihal Prinsip Kehati-hatian bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain* [Bank Indonesia Circular Letter No. 14/20/DPNP Concerning Prudential Principle for Commercial bank which Outsource Some Parts of Its Works to Other Party].

⁷⁶⁶ For instances, see *Peraturan Bank Indonesia Nomor 8/4/PBI/2006 Tentang Pelaksanaan Good Corporate Governance Bagi Bank Umum sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor 8/14/PBI/2006* [Bank Indonesia Regulation Number 8/4/PBI/2006 Concerning Implementation of Good Corporate Governance for Commercial Bank as amended by Bank Indonesia Regulation Number 8/14/PBI/2006] ('*BIR-GCG*'); *Peraturan Bank Indonesia Nomor: 5/8/PBI/2004 Tentang Penerapan Manajemen Risiko Bagi Bank Umum sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor: 11/25/PBI/2009* [Bank Indonesia Regulation Number 5/8/PBI/2004 Concerning Risk Management Implementation for Commercial Bank as amended with Bank Indonesia Regulation Number: 11/25/2009] ('*BIR-Risk Management*'); *Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 Tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah* [Bank Indonesia Regulation Number: 7/6/PBI/2005 Concerning Transparency of Banking Product Information and the Use of Bank Customers' Personal Data] ('*BIR-TBPI&UBCPD*').

⁷⁶⁷ *BIR-Risk Management* art 1(3).

⁷⁶⁸ Ibid art 4. However, risks discussed in this thesis only include legal risk (including compliance risk), operational risk that caused by fraud (fraud risk) and reputational risk.

management should encompass at least the following aspects: a) active supervision by the Board of Commissioners and Board of Directors; b) adequacy of policy, procedure, and establishment of limits; c) adequacy of processes of identification, measurement, monitoring, and control of risks and the risk management information system; and d) comprehensive internal control system.⁷⁶⁹

Understanding that the use of information technology in the bank's e-banking operations could also increase bank risk, Bank Indonesia has enacted special regulations in the information technology area concerning 'Implementation of Risk Management in the Use of Information Technology by Commercial Banks' ('IT Risk Management').⁷⁷⁰ In providing e-banking services, banks should consider the prudential principles for banking, the security and integrity of their IT systems, cost effectiveness, and implementation of adequate consumer protection as well as measures in line with the bank's business strategy.⁷⁷¹

Based on this IT Risk Management regulation, Bank Indonesia has obliged banks to implement effective risk management in the use of information technology, which should at least include active supervision by the Board of Commissioners and Directors, sufficient policies and procedures for information technology use; adequate processes for identification, measurement, monitoring and risk control in the use of information technology; and internal control systems for the use of information technology.⁷⁷² This provision is an obligation of banks regardless of whether the implementation and operation of information technology is done by the bank itself or by a third party service provider.⁷⁷³ Further, this regulation also obliged banks to identify risks that may arise from e-banking activities, whether resulting from the product itself or from the use of information technology as consequence of using electronic delivery channel. Hence in order to able to calculate and forecast the occurrence or probability of risk posed by an

⁷⁶⁹ Ibid arts 2–3. See also *BIR-GCG* art 53.

⁷⁷⁰ *Peraturan Bank Indonesia Nomor: 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum* [Bank Indonesia Regulation Number: 9/15/PBI/2007 Concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks] ('*BIR-RMUITCBs*')

⁷⁷¹ See Chapter VIII art 8.1 of Guidelines for the Implementation of Risk Management in the Use of Information Technology by Commercial Banks in the appendix 1 of *Surat Edaran Bank Indonesia Nomor 9/30/DPNP Perihal Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum* [Bank Indonesia Decree Number 9/30/DPNP Concerning Risk Management in the Use of Information Technology by Commercial Banks] ('*BID-RMUITCB*').

⁷⁷² Ibid art 2. See also related provisions pertaining to art 2 in Chapter III of the regulation.

⁷⁷³ *BID-RMUITCB* art II.1.

e-banking product, banks must develop a loss event database (historical database),⁷⁷⁴ and perform risk mitigation on general risk and specific risk that may arise in e-banking service provision.⁷⁷⁵

From the technological and security regulation perspective, many Bank Indonesia regulations in the payment card area are intended to prevent and reduce crime and simultaneously enhance public confidence in the payment card in Indonesia.⁷⁷⁶ Payment card issuers are required to enhance the security of the technology used in their payment card system.⁷⁷⁷ As result, Bank Indonesia has enacted some special provisions concerning risk management in payment card operations. These provisions include:

- Banks who issue ATM/debit cards are obliged to implement the risk management principle in their payment card system in accordance with Bank Indonesia's risk management provisions.⁷⁷⁸ For instance, pertaining to new electronic banking products, banks should prove their readiness to implement risk management, especially in security control to ensure the fulfilment of the principles of confidentiality, integrity, authentication, non-repudiation and availability.⁷⁷⁹
- To reduce exacerbated losses in the occurrence of fraud and to assist issuers in managing their liquidity, issuer banks are obliged to observe security and proper controls in the issuance of ATM cards. This includes the following measures:
 - The maximum nominal limit of transferable funds between accounts of different banks through ATMs shall be set at IDR25 million per account in one day. This provision does not apply if the transfer is made to an account at the same bank.
 - The maximum cash withdrawal limit using ATM cards and credit cards on ATMs shall be IDR10 million per account in one day.⁷⁸⁰

⁷⁷⁴ Ibid appendix 1, art 8.4.1.

⁷⁷⁵ Ibid appendix 1, art 8.4.2.

⁷⁷⁶ *Surat Edaran Bank Indonesia Nomor 11/10/DASP Perihal Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu sebagaimana telah diubah dengan Surat Edaran Bank Indonesia Nomor 14/17/DASP* [Bank Indonesia Decree Number 11/10/DASP Concerning The Operation of Card-Based Payment Instrument Activities as Amended with Bank Indonesia Decree Number 14/17/DASP] (*BID-CP & Security*) Clause VII.C.1.

⁷⁷⁷ Nuryanti and Dewi, above n 649, 88–91.

⁷⁷⁸ *BIR-CBPI* art 22(1).

⁷⁷⁹ *BIR-RMUITCB* art 23(4).a.5).

⁷⁸⁰ *BID-CP & Security* clause VII.B.8. See also appendix 1 of *BID-RMUITCB* art 8.4.2.2.b.

5.2.2.3. Security Improvement for Payment Cards

The improvement of payment card security is aimed to minimise crime/fraud, and also to improve public confidence pertaining to payment card usage. Some provisions in Bank Indonesia Regulations have enumerated quite detailed material regarding principle or ‘security standards’ that should be employed by banks in their e-banking operations. The following are among these set standards.

- In the authentication method employed, banks should implement at least two factor authentication, that is ‘what you know’ (PIN, password), ‘what you have’ (magnetic cards with chips, token, digital signature), “something you are” or “biometric” (retinal image, fingerprint);
- maximum limit for incorrect PIN attempt inputs and its logged list should be set, in order to avoid unauthorised access and collect possible evidence of fraud;
- non-repudiation aspect, so all transactions are credible;
- segregation of duties in the e-banking operation;
- installation of antivirus software to minimise external threats such as viruses and malicious transactions at all entry points and each computer system and software to detect intrusion (intrusion detection system);
- conduct of periodic penetration testing on internal and external networks;
- testing of the integrity of e-banking transactions data;
- availability of a clear audit trail mechanism for all e-banking transactions;
- performance of detection and monitoring of unauthorised transactions, that is, using IDS and/or fraud detection system (neural network);
- protection of the confidentiality of e-banking information, and so on.⁷⁸¹

Pertaining to improving the security technology employed in the ATM/debit card system, issuer banks are obligated to use reliable and secure systems, maintain and improve payment card security technology, have written policy and standard operating procedure for payment card activities management, and safeguard the security and confidentiality of payment card data.⁷⁸² Improvements should be made to the security of

⁷⁸¹ *BID-RMUITCB* appendix 1, art 8.4.2.1.

⁷⁸² *BIR-CBPI* art 29(1) and its explanatory section. ‘Security’ in this Article includes the security in the card issuing process, data management, physical card security, and security of the whole entire system used in payment card processing. It means that the electronic system used in the payment card should be physically and logically protected.

the cards themselves and that of the entire payment card system processing or technological infrastructure, as follows:

- by implementing chip technology and a six digit PIN,⁷⁸³ the use of which would also function as a replacement of the cardholder's handwritten signature.⁷⁸⁴ All banks will be obliged to use and process on-line ATM/debit card transactions with chip technology and six digits PIN as a sole authentication method at the end year 2020,⁷⁸⁵ without a fallback option of magnetic stripe technology if a chip card for some reasons could not be processed.⁷⁸⁶
- by implementing physical security control on equipment and rooms to protect consumers and their transactions from the danger of theft, sabotage and other criminal action so as to improve consumer comfort and security in ATM and EFT-POS transactions that involve the use of physical equipment like ATMs; and by performing routine monitoring to ensure the security and comfort of consumers using e-banking services.⁷⁸⁷
- by ensuring the availability of security measures on data transmission between Electronic Funds Transfer (EFT) terminals and the host computer to protect against risks of transmission error, network disturbance, unauthorised access, and so on. Security measures shall comprise equipment control, monitoring of quality and accuracy of network equipment performance and transmission lines, as well as monitoring access to controller software ('Host-Front End').⁷⁸⁸
- by ensuring that the party providing Point of Sale (POS) terminals always increases physical security in the vicinity of POS terminals and of the POS terminals themselves by (amongst other measures) using POS terminals that minimise the possibility of interception on such POS terminals or in the party's communication network. (Point of Sales (POS)/Electronic Data Capture (EDC) enables electronic funds transfer from a customer's account to an acquirer or merchant's account for payment of a transaction.) It should be noted that while transactions undertaken via POS terminals located in shopping centres or supermarkets generally involve a

⁷⁸³ *BID-CP & Security* arts VII.C.1, 2, 3.c, 4.b, 5.b.

⁷⁸⁴ *BID-Chip & PIN* art I.B.2.

⁷⁸⁵ *Ibid* art V.B.1. See also art V.C.

⁷⁸⁶ *Ibid* art V.B — last paragraph.

⁷⁸⁷ *BID-RMUITCB* appendix 1, art 8.4.2.2.c.

⁷⁸⁸ *Ibid* appendix 1, art 8.4.2.2.d.

card-based payment instrument supplied by an issuer bank, POS may be provided by the bank itself, or financial acquirer, technical acquirer or switching company.⁷⁸⁹

5.3. Legal and Regulatory Framework for Consumer Protection in ATM/Debit Card Transactions in Indonesia

5.3.1. Legal Framework for Consumer Protection

5.3.1.1. Constitution of the Republic of Indonesia 1945

Indonesia is a unitary state governed by the rule of law. As a rule of law country, the protection of the human rights of all citizens within the country is necessary and has become a basic characteristic of Indonesia as rule of law country (*rechtsstaat*).⁷⁹⁰ Indonesia has also embraced democratic principles in the economic sector. Hence, democracy in its economic aspects requires that each citizen is equally able to be involved in actively participating in economic activities, such as in the trade and production of goods and services.

In Indonesia, the Constitution of the Republic of Indonesia has become the highest manifestation of the rule of law.⁷⁹¹ Since human rights are accepted as a factor in Indonesia as a state law country, consumer protection has automatically become an integral part of the human rights principles embraced by the country.⁷⁹²

Consumer protection as part of a citizen's basic rights in Indonesia can be found in the paragraph 4 of the Preamble to the Constitution of Indonesia 1945, which highlights the country's promises to protect the people, improve people's general welfare and intellectual life based on principles of 'freedom, abiding peace and social justice'. Further, the legal protection concerning basic rights and obligations of Indonesia consumers is enumerated more clearly in several provisions of the Constitution, as follows:

⁷⁸⁹ Ibid appendix 1, art 8.4.2.2.e.

⁷⁹⁰ See Consideration Section of *Undang-Undang Republik Indonesia Nomor 12 Tahun 2011 Tentang Pembentukan Peraturan Perundang-Undangan* [Law of Republic of Indonesia Number 12 of 2011 on Making Regulations] (*LMR*). See also Sjahputra, above n 15, 30–1.

⁷⁹¹ See *LMR* arts 3, 7(1).

⁷⁹² Janus Sidabalok, *Hukum Perlindungan Konsumen di Indonesia* [Consumer Protection Law in Indonesia] (PT Citra Aditya Bakti, 2010) 6.

- every person is entitled to (legal) recognition, security, protection, legal certainty, and equal treatment before the law;⁷⁹³ and
- every person is entitled to the protection of her/himself, family, honour, dignity and property under their authority, and is entitled to the sense of security and protection from the threat of fear to do or not do something that is a fundamental right.⁷⁹⁴

As a consequence, based on provision in Article 28D of the Constitution, legislators have created in various Acts and regulations governing the rights and obligations of consumer, with the aim to protect every citizen's right in the country.⁷⁹⁵ Meanwhile, it is deemed appropriate that Article 28G(1) of the Constitution (the second dot point above and especially the second part) applies when an ATM/debit card consumer conducts an ATM/debit card transaction at consumer activated terminals.

5.3.1.2. Law No 8 of 1999 on Customer Protection (LCP)⁷⁹⁶

In line with the increasing awareness of the law to protect the consumer in more complex economic transactions, the Indonesian government and the legislature has issued the *LCP*, which became effective on 20 April 2000. Acknowledgment of this complex economic market has led to law reform in regard to the relationship between producer and consumer. The law reform itself marked a paradigm shift in the relationship between the producer and the consumer, where the relationship that was previously based on the doctrine of *caveat emptor*⁷⁹⁷ ('let the buyer beware') has changed into a doctrine of *caveat venditor*⁷⁹⁸ ('let the seller beware').⁷⁹⁹

⁷⁹³ *Undang-Undang Dasar Republik Indonesia 1945* [Constitution of the Republic of Indonesia 1945] arts 28D(1), 28H.

⁷⁹⁴ *Ibid* art 28G(1).

⁷⁹⁵ Sjahputra, above n 15, 30–1. See also Inosentius Samsul, *Perlindungan Konsumen: Kemungkinan Penerapan Tanggung Jawab Mutlak* [Consumer Protection: the Possibility to Apply Absolute Liability] (Universitas Indonesia, 2004) 7–8.

⁷⁹⁶ Referring to *LCP* arts 1(1), 1(2): 'consumer protection' is every effort made to guarantee legal certainty aimed at providing protection to the consumers. Meanwhile, what is meant by 'consumer' is anybody using goods and/or services which are available in the community, for his own purpose, for the purpose of his family and other people, as well as for other living creatures and which are not to be further traded.

⁷⁹⁷ Bryan A Garner (ed), *Black's Law Dictionary* (West Group, 9th ed, 2009) 152. *Caveat emptor* is the principle that a person who buys something is responsible for finding any faults in what they buy prior to purchase or bear the consequences (that is, purchasers buy at their own risk). Modern statutes and cases have greatly limited the importance of this doctrine.

⁷⁹⁸ *Ibid*.

⁷⁹⁹ Samsul, 'Perlindungan Konsumen', above n 795, 4–5. See also Sjahputra, above n 15, 47–55.

This development of consumer protection in the *LCP* is also in line with the development of consumer protection in many developed countries' regulations and/or international guidelines and standards (such as the United Nations (UN) Guidelines for Consumer Protection) where legal reforms have been made relating to product liability.⁸⁰⁰ One of the main reasons for reforms in the consumer protection law is to facilitate and simplify the provision of compensation for consumers who suffer losses due to using business actors' products and/or services in the community.⁸⁰¹

As a result, the provisions and scope of *LCP* are quite similar to the UN Guidelines for Consumer Protection.⁸⁰² According to Sidabalok, a prominent consumer protection expert in Indonesia, this similarity is evidence that consumer protection is a universal issue that has been formulated by many international organisations and shaped the guidelines for many countries' consumer protection enactments, including those of Indonesia.⁸⁰³

LCP was enacted to serve as a strong legal foundation to empower consumers by means of improving their dignity, awareness, knowledge, concern, ability and independence so as to enable them to protect themselves, and to create and develop responsible behaviour on the part of business actor.⁸⁰⁴ The establishment of *LCP* also aimed to protect consumer interests in an integrated and comprehensive manner, which can be effectively enforced in the community. It was not designed to put business actors out of

⁸⁰⁰ See as an example of international guideline standard the UN-Guidelines for Consumer Protection: Department of Economic and Social Affairs, 'United Nations Guidelines for Consumer Protection (as expanded in 1999)' (United Nations, 2003). In these guidelines, governments are asked to 'develop or maintain a strong consumer protection policy that should be taking [its] guidelines ... and relevant international conventions ...[setting out their] priorities in accordance with [their] economic, social and environmental circumstances ... and the needs of the population, bearing in mind the costs and benefits of the proposed measures': at 2.. The guidelines should meet the following goals (at 2–3):

- (a) The protection of consumers from hazards to their health and safety;
- (b) The promotion and protection of the economic interests of consumers;
- (c) Access of consumers to adequate information to enable them to make informed choices according to individual wishes and needs;
- (d) Consumer education, including education on the environmental, social and economic impacts of consumer choice;
- (e) Availability of effective consumer redress;
- (f) Freedom to form consumer and other relevant groups or organizations and the opportunity of such organizations to present their views in decision-making processes affecting them;
- (g) The promotion of sustainable consumption patterns.

⁸⁰¹ Sjahputra, above n 15, 52–3.

⁸⁰² See CUTS International, *Consumer Rights and Its Expansion: Rights and Responsibilities* (1999) CUTS Centre for Consumer Action Research and Training (CART) <<http://www.cuts-international.org/consumer-rights.htm>>.

⁸⁰³ Sidabalok, above n 792, 37–43.

⁸⁰⁴ See *LCP* Consideration (d).

business.⁸⁰⁵ It was written in the spirit of creating a balance of protection between the consumer and business actor's interests in order to create a healthy and just economy.⁸⁰⁶

Consumer protection in Indonesia has a broad scope, that is, it covers protection of consumer goods and services,⁸⁰⁷ including various aspects related to the consequences arising from the use of goods and services. One of the main aspects of consumer protection in Indonesia is the question of the responsibility of the business actor for damages arising from the use of their goods and/or services.⁸⁰⁸

Some provisions in the LCP that are vital in ATM/debit card transactions to empower consumer protection in Indonesia.⁸⁰⁹ These include that:

- Consumer protection is based on the principles of consumer benefit, justice, balance, security and safety, and legal certainty;⁸¹⁰
- Consumer protection goals include (among others) to improve the quality of the goods and/or services which will guarantee that businesses will continue producing goods and/or services, conforming with the health, comfort, security and safety requirements of consumers;⁸¹¹
- The rights and obligations of the consumers and business actors are enumerated quite exhaustively. What become rights for consumers on one hand will become

⁸⁰⁵ See *LCP* Elucidation.

⁸⁰⁶ *Ibid.*

⁸⁰⁷ Goods shall be anything which is either tangible or otherwise, which is either movable or otherwise or which can be used up or otherwise and which can be traded, put on, used or utilised by consumers; A service shall be any service in the form of a job or an achievement which is made available to the community in order to be utilised by consumers. See *LCP* arts 1(4), 1(5).

⁸⁰⁸ Sidabalok, above n 792, 10–11.

⁸⁰⁹ *LCP* arts 1, 2. Consumer protection is 'all means which can guarantee the legal certainty to protect consumers' interests.' Meanwhile, a 'consumer' is 'each user of goods and/or services that available in society, for the benefit of themselves, family members, other people, and other living creatures and which are not for trading.' Consumers in this law refer to 'end consumers' which are end users of a product.

⁸¹⁰ *Ibid* elucidation of art 2:

"The principle of benefit" aims to ensure that every effort in providing consumer' protection must give the maximum benefit to the interest of consumers and business actors as a whole; "The principle of justice" aims to ensure that the participation of the entire people can be realized to the maximum and give an opportunity to consumers and business actors to have their rights and perform their obligations actively; "The principle of balance" aims to provide balance between the interests of consumers, business actors, and the government in the material or spiritual sense; "The principle of security and safety" of consumers aims to provide a guarantee of security and safety to consumers in using and utilisation of goods and/or services consumed or used; "The principle of legal certainty" aims to ensure that both business actors and consumers shall comply with the law and obtain justice in the provision of consumers' protection, while the state shall guarantee the legal certainty.

⁸¹¹ *Ibid* art 3.

obligations for business actors on the other hand — and vice versa. Some rights and obligations that relevant to the thesis are set out in the Table 2 below:⁸¹²

Table 2: Consumer Rights v Business actor Obligations

Consumer Rights	Business actor Obligations
To obtain comfort, security and safety in using or consuming the goods and/or services.	To act in good faith in conducting the business.
To obtain correct, clear and honest information on the condition and warranty of the goods and/or services; To obtain consumer training and education.	To provide correct, clear and honest information with regard to goods and/or services.
To be heard when expressing opinions on and complaints about the goods and/or services the used or consumed.	To treat and serve the consumers properly and honestly and in a non-discriminatory manner.
To obtain proper advocacy, protection and settlement in consumer protection disputes.	
To obtain compensation, redress, and/or substitution, if the goods and/or services received are not in accord with the agreement or not received as requested.	To provide compensation, redress and/or substitution for the damages caused by the use, consumption and application of the goods and/or services; or if the goods and/or service received or used do not accord with the agreement.
To obtain rights as regulated in the other provisions of the law.	
Business actor Rights	Consumer Obligations
To receive payment in accordance with the sales agreement on the conditions and conversion value of the goods and/or services.	To pay the price in accordance with the agreed conversing on value.
To obtain legal protection from consumers who act in bad faith.	To act in good faith in performing the transaction of purchasing the goods and/or services.
To undertake proper self-defence in the legal settlement of a consumer's dispute.	To follow the proper legal settlement in a consumer protection dispute.
To rehabilitate its good reputation if it is legally proven that the consumer's damage is not caused by the goods and/or service purchased.	To read or follow the information instructions and application or usage procedures of the goods and/or services for security and safety.
To obtain rights as regulated in the other provisions of the law.	

⁸¹² Ibid arts 4–7.

- In offering the goods and/or services for trading, the business actors are prohibited from making or including a standard clause in each document and/or agreement, among others if it states the transfer of the business actor's responsibility, and/or if it regulates matters related to proving the loss of use of the goods or utilisation of the services purchased by consumers. These provisions are intended to ensure that consumers should have an equal position to the business actor on the basis of the principle of the freedom to make a contract. Violation by an business actor of the standard clause provisions in this law can cause the agreement to be deemed invalid (null and void).⁸¹³

5.3.2. Regulatory Framework for Consumer Protection

In order to maintain public confidence in payment card activities, Bank Indonesia continuously strives to ensure that the e-payment industry in Indonesia operates in a nurturing and efficient environment. One important aspect that will always be a goal for Bank Indonesia is to achieve sound payment system operations in Indonesia where there is an effective and efficient implementation of customer protection principles in payment card operations.⁸¹⁴

Consumer protection as an issue in the Indonesian banking industry has become more prevalent with the implementation of Indonesian Banking Architecture (*Arsitektur Perbankan Indonesia* (API)),⁸¹⁵ where one of the six API pillars is 'realizing the empowerment and the protection of consumer of banking services.'⁸¹⁶ It demonstrates the commitment of Bank Indonesia as a regulator and supervisor of the banking industry to balance the consumer's position with that of banks. To achieve this goal, society, the banking industry and Bank Indonesia together create a mechanism for consumer complaints, establish a banking mediation body, increase transparency of information products, and educate consumers concerning bank products and services, including their

⁸¹³ Ibid art 18.

⁸¹⁴ Nuryanti and Dewi, above n 649, 96–8.

⁸¹⁵ See Hermansyah, above n 683, 189–92. API is the architecture that contains policy direction in the form of the banking development program to achieve the healthy, robust, and efficient national banking industry to create financial system stability in order to improve national growth.

⁸¹⁶ Bank Indonesia, *Enam Pilar API* [API's Six Pillars] (2010). Bank Indonesia, *API's Six Pillars (Enam Pilar API)* (2010) <http://www.bi.go.id/NR/rdonlyres/2502404A-6622-46A4-9030-00CF3FC86A7A/1378/enam_pilar.pdf>; Hermansyah, above n 683, 195.

inherent risks.⁸¹⁷ As a result, customer protection provisions exist in almost all Bank Indonesia regulations and decrees.

In payment card regulation, all institutions involved in the payment card operations are urged to pay attention to consumer interest and safety. In addition to this, consumer education is an important aspect that is supposed to be highlighted by banks in their information technology operations.⁸¹⁸ Understanding the significant element of consumer protection in banking operations (especially in the payment card system), Bank Indonesia has enacted some regulations with many provisions concerning the consumer protection issue in the payment card activities. A number of these are outlined below.

5.3.2.1. Consumer Education

Generally, consumer choices of bank products are often based more on benefits or advantages to be derived from such products as explained by the banks. Typically, banks prefer to explain only the benefits of a product as opposed to the costs or inherent risks associated with it. Banks do this to win consumers' hearts for the sake of bank revenue, reputation and consumer confidence. Hence, the rights of consumers to obtain a complete, accurate, current, and complete information regarding bank products (including their inherent risks) from banks, as banks are obliged to provide under the consumer protection laws, are often not fulfilled. Consequently, a dispute often then arises between the bank and its customers in practice. Such disputes can arise due to gaps in information about the characteristics of the products offered by banks to customers.

Therefore, transparency of information about all aspects of bank products becomes a necessity that cannot be avoided if banking institutions are to maintain their credibility and consumer rights be protected (as mandated by *LCP*).⁸¹⁹ To overcome these problems, Bank Indonesia has enacted Bank Indonesia Regulation Number 7/6/PBI/2005 Concerning Banking Product Information Transparency and Personal Consumer Data.

⁸¹⁷ Hermansyah, above n 683, 202–3; Djumhana, above n 68, 338.

⁸¹⁸ *BIR-RMUITCB* art 23(4)a.8.

⁸¹⁹ General explanation of *BIR-TBPI&UBCPD*.

In this regulation, Bank Indonesia has asserted that in order to improve consumer protection, transparency in bank product information is very important to banking customers so that they can really understand clearly about the benefits and pertinent risks associated with the products.⁸²⁰ Consequently, banks are obliged to create a written policy and procedure in implementing transparency of information regarding bank products. This includes: (1) banks being obliged to provide complete and clear written information in Bahasa Indonesia regarding the characteristics of each bank product;⁸²¹ (2) such information to contain as a minimum the name, type, benefit and risk associated with the products, their requirements and how to use the product, and cost of product (in terms of risk, there should be a balance between potential benefit versus risk that may arise to the consumers).⁸²²

In regard to consumer education, banks must educate e-banking customers in an attempt to make consumers understand the risks involved in e-banking. Customer education is to comprise the rights, obligations and responsibilities of all related parties. Education must at least be given when customers apply for e-banking service. Items about which consumers need to be educated are (amongst others) in regard to the importance of keeping PIN/password secure, for example, by:

- keeping PIN/password confidential and not disclosed to anyone including bank employees;
- periodically changing PIN/password;
- using PIN/password that is not easy to predict (not using personal information such as date of birth);
- not writing down the PIN/password;
- ensuring that the PIN for one product is different from the PIN for another;⁸²³
- implementing prudential principles when using ATMs, which include: a) examining the security of the environment around the ATM before deciding to

⁸²⁰ See Consideration Section in *BIR-TBPI&UBCPD*. ‘Customer’ in this regulation is the person or institution which uses bank’s services, and includes a person or institution who does not have an account but use bank services for their financial transaction (walk-in customers).

⁸²¹ *BIR-TBPI&UBCPD* art 4.

⁸²² *Ibid* art 5.

⁸²³ *Surat Edaran Bank Indonesia Nomor 9/30/DPNP Perihal Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum* [Bank Indonesia Decree Number 9/30/DPNP Concerning Risk Management in the Use of Information Technology by Commercial Banks] (*BID-RMUITCB*) appendix 1 art 8.4.2.3.e.

draw money; and b) ensuring that the money and the card are already retrieved before leaving the ATM location.⁸²⁴

In educating their customers, ATM/debit card issuers are obliged to provide written information to cardholders using simple Bahasa Indonesia language, readable font, and delivered to consumer in the appropriate manner and in a timely fashion. Issuers of ATM/debit cards should submit the written information mentioned above directly to their potential customer or to the cardholder/consumer's address using media such as a consumer request form, welcome pack, pamphlet, and/or notice/information letter. In the event that there have been changes to the substance of the information, the issuer of the payment card must re-submit the amended written information to the consumers using similar procedures.⁸²⁵ Issuers are also obliged to provide 'hotline' telephone access for consumers, to ensure that consumers have an easy access to verify bank facilities and/or information.⁸²⁶ This written information should at least include:

- procedure and user guidelines regarding the use of ATM/debit cards, facility attached to an ATM/debit card, and risks that might arise from the use of ATM/debit card;
- rights and obligations of ATM/debit card cardholders, which at least includes:
 - important aspects that should be scrutinised by cardholders, including all risks that might arise from the use of ATM/debit card, such as a warning not to share PIN with others and precautions to be used when consumers conduct transactions in ATMs;
 - rights and obligations of cardholders and/or issuers of ATM/debit cards in case 'something bad' happens that could cause a loss to the consumer or issuer bank, such as when unauthorised payment card transactions occur, bank systems malfunction, and so on.⁸²⁷
 - procedures for filing complaints related to problems with the use of ATM/debit cards and duration of the complaint handling.⁸²⁸

⁸²⁴ Ibid appendix 1 art 8.4.2.3.e.1–2)(a)–(b).

⁸²⁵ *BID-CP & Security* art VII.A.4.a–b.

⁸²⁶ *BIR-CBPI* art 23. See also *BID-CP & Security* art VII.A.1.a, b. See also *BIR-TBPI&UBCPD* arts 4–8; *Surat Edaran Bank Indonesia Nomor 7/25/DPNP Perihal Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah* [Bank Indonesia Decree Number 7/25/DPNP Concerning Transparency of Bank Product Information and the Use of Bank Customers' Personal Data] art II.

⁸²⁷ *BID-CP & Security* art VII.A.2.

⁸²⁸ Ibid.

5.3.2.2. Resolution of Consumer Complaints

In banking practice that involves customer activities, very frequently the rights of customers are not routinely nor duly upheld by banks, leading to disputes between them, as indicated by the increasing customer complaint incidents related in the mass media or in online forums. Such situations, if not resolved quickly and in an appropriate way, can potentially develop into prolonged disputes that will cause greater loss to both parties.⁸²⁹ The increasing number of complaints that are reported in the media⁸³⁰ may create reputational risk for banks and have a corrosive effect on public confidence in banking products and services. Therefore, to mitigate these problems, Bank Indonesia has enacted Bank Indonesia Regulation Number 7/7/PBI/2005 Concerning Resolution of Customer Complaints as amended by Bank Indonesia Regulation Number 10/10/PBI/2008 to minimise reputation risk, which urges banks to establish an effective mechanism for resolution of customer complaints within an adequate timeframe. This regulation also aims to empower customers in their dealings with the banks in regard to their problems.⁸³¹

Some of the important provisions for customer interest in this regulation are that:

- Banks are required to resolve each complaint lodged by a customer and/or their representatives related to their financial transaction using comprehensive procedures covering activities to receive complaints, to handle and resolve complaints, and to monitor complaint handling and resolution;⁸³²
- It is among the responsibilities of a bank's board of directors that they must ensure that their bank meets the requirement to have a unit and/or function established specifically to handle and resolve customer complaints and publish them to the public;⁸³³

⁸²⁹ Elucidation of *Peraturan Bank Indonesia Nomor: 7/7/PBI/2005 Tentang Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor: 10/10/PBI/2008* [Bank Indonesia Regulation Nomor: 7/7/PBI/2005 Concerning Resolution of Customer Complaints as amended by Bank Indonesia Regulation Number 10/10/PBI/2008] (*BIR RCC*). See also *Surat Edaran Bank Indonesia Nomor 7/24/DPNP Perihal Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Surat Edaran Bank Indonesia Nomor 10/13/DPNP* [Bank Indonesia Letter Number 7/24/DPNP Concerning Resolution of Customer Complaints as amended by Bank Indonesia Letter Number 10/13/DPNP].

⁸³⁰ See *BIR-RCC* art 1(4) where it is stated that 'complaint' in this regulation means 'the expression of customer dissatisfaction arising from potential financial loss to the customer thought to be caused by error or negligence on the part of the bank.'

⁸³¹ *BIR-RCC*.

⁸³² *Ibid* art 2.

⁸³³ *Ibid* arts 3–5.

- Banks, at any time, may be required to explain and provide information about the complaint when the customer requests an explanation about the status of the lodged complaint. For complaints in writing, banks should convey the result also in writing.⁸³⁴

5.3.2.3. Consumer Protection in Payment System Services

Bank Indonesia recognises that in the relationship between banks and consumers, consumers are often in a weak position. The weakness is caused by an imbalance in the relationship between banks and consumers, which is partly due to asymmetric information distribution, power imbalances, poor quality of service to consumers, misuse of consumer personal data, and lack of effective mechanisms for resolving disputes between banks and consumers.⁸³⁵

In this regard, Bank Indonesia felt the need to establish a culture of consumer protection based on international standards for the payment systems services industry in Indonesia. The international standards and best practice are also used by Bank Indonesia in order to improve legislation as well as security and efficiency in the country's payment system.⁸³⁶ To achieve these goals, Bank Indonesia has issued Bank Indonesia Regulation Number 16/1/PBI/2014 Concerning Consumer Protection on Payment System Services on 16 January 2014. The regulation includes several important principles. Among them are the principles of fairness and reliability, transparency, protection of personal data, as well as the effective handling and resolution of customer complaints.⁸³⁷

Apart from those important principles, this regulation also includes some other important provisions, among them:

- a prohibition of any 'hard to read' standard clause in the agreement between the bank and the consumer which by its location or shape is hardly visible or cannot be

⁸³⁴ Ibid arts 12, 13.

⁸³⁵ Elucidation of *Peraturan Bank Indonesia Nomor 16/1/PBI/2014 Tentang Perlindungan Konsumen Jasa Sistem Pembayaran* [Bank Indonesia Regulation Number 16/1/PBI/2014 Concerning Consumer Protection on Payment System Services] 1.

⁸³⁶ Financial System Stability Bureau Directorate of Banking Research and Regulation, 'Financial Stability Review I - 2006' (Bank Indonesia, 2006) 60–2.

⁸³⁷ See *BIR CPPSS* art 3 and its elucidation. The principle of fairness and reliability of the system aims to ensure payment system providers treat consumers in a fair and non-discriminatory manner and ensure the providers provide accurate and secure payments.

read clearly or is difficult for consumers to understand, and any such clause that has the effect of shifting liability from the bank to the consumer;⁸³⁸

- an obligation on the banks to:
 - provide a reliable system and maintain the confidentiality of data and consumer information in the operation of their payment system services;⁸³⁹
 - be liable for consumer losses incurred due to the fault of a provider's management and/or staff;⁸⁴⁰ However, again, there is no provision in this regulation concerning fraud liability for payment card transactions.
 - provide information about the benefits, risks, and consequences for consumers in the use of the bank's payment system services;⁸⁴¹ and
 - have a consumer complaints handling mechanism and implement it. This includes activities such as receipt of consumer complaints, the handling and resolution of such complaints, and monitoring the handling and resolution.⁸⁴²

5.4. Legal and Regulatory Framework of Liability Rules on Unauthorised ATM/Debit Card Transactions in Indonesia

5.4.1. Legal Framework of Liability Rules

5.4.1.1. The Indonesian Civil Code: Tortious Liability

Liability is one of the most significant terms in the field of law, especially in the civil law area. In general, liability provision based on fault or negligence, also known as liability based on tort law (in Indonesia, known as *tanggung gugat*),⁸⁴³ can be found in articles 1365 to 1369 of Indonesia's Civil Code of 1848. Pertaining to liability issues that occur in the event of unauthorised ATM/debit card transactions, the relevant provisions that fit the situation are Articles 1365, 1366, and 1367 of Indonesia's Civil Code.

⁸³⁸ See *Peraturan Bank Indonesia Nomor 16/1/PBI/2014 Tentang Perlindungan Konsumen Jasa Sistem Pembayaran* [Bank Indonesia Regulation Number 16/1/PBI/2014 Concerning Consumer Protection on Payment System Services] art 8. This regulation has in principle adopted similar provisions regarding standard clause to those in *LCP 1999* art 18.

⁸³⁹ *Ibid* arts 9, 14.

⁸⁴⁰ *Ibid* art 10.

⁸⁴¹ *Ibid* art 11.

⁸⁴² *Ibid* art 16.

⁸⁴³ See Marzuki, '*Pengantar Ilmu Hukum*', above n 155, 88. See also Erman Rajagukguk, *Perbuatan Melawan Hukum* [Unlawful Act/ATort] (2009) <<http://webcache.googleusercontent.com/search?q=cache:meNPWduRDH8J:www.ermanhukum.com/Makalah%2520ER%2520pdf/PERBUATAN%2520MELAWAN%2520HUKUM.pdf+&cd=1&hl=en&ct=clnk&gl=id&client=firefox-a>> 1.

According to Article 1365 of Indonesia's Civil Code, a party who commits an [at] fault or negligent act which causes damage to another party shall be obliged to compensate the damage. Meanwhile Article 1366 of Indonesia's Civil Code further explains that the liability for an act as mentioned in Article 1365 exists not only in relation to an intentional act by the party responsible for the damage, but also includes any damages that were incurred due to the party's negligence or recklessness (incautious conduct). These provisions are probably some of the most popular provisions used in the civil lawsuit practices in Indonesia. Typically, in every tort case in the Indonesian courts where compensation is sought for damages that have occurred as a consequence of one party's action, this provision is the basis for the suit.

An action undertaken by one party will be considered as a tort if the act was contrary to the law in general. 'The law' here not only refers to formal regulations but also includes unwritten law such as customs, prudential behaviour, and/or other matters that normally the community should abide by. The damages that result from the tort can only be claimed when (a) there is a correlation between the act and the loss; and (b) loss arising is due to the fault of the offender, whether arising by intention or due to negligence. Tort or unlawful act is not only by commission of an act (doing something) but also an 'act' of omission (failure to do something).⁸⁴⁴

Indonesia's Civil Code also states that each person/institution is not only liable for damage caused by their own actions, but also for damage caused by acts of their dependants (vicarious liability), or caused by items or infrastructure under their control (occupiers' liability).⁸⁴⁵

Further, Hassanah⁸⁴⁶ and Ratnawati⁸⁴⁷ argue that tort doctrine as contained in Articles 1365 to 1369 of the Indonesian Civil Code can be used within or outside of court (arbitrage, mediation, and so on) to claim restitution from banks or other financial

⁸⁴⁴ R Soeroso, *Pengantar Ilmu Hukum* [Introduction to Law] (Sinar Grafika, 2004) 294.

⁸⁴⁵ *Kitab Undang-Undang Hukum Perdata* [Civil Code] (Indonesia) art 1367.

⁸⁴⁶ Hetty Hassanah, *Tinjauan Hukum Mengenai Perbuatan Melawan Hukum Dalam Transaksi Jual Beli Melalui Internet (E-Commerce) Dihubungkan Dengan Buku III KUH Perdata* [Tort Law Review on E-Commerce in Connection to Section III Indonesia Civil Code] (2006) 9 <http://www.google.com.au/search?sourceid=navclient&ie=UTF-8&rlz=1T4ADFA_enAU349AU349&q=Tinjauan+hukum+mengenai+perbuatan+melawan+hukum+dalam+transaksi+jual+beli+melalui+internet>.

⁸⁴⁷ Theresia Endang Ratnawati, *Pemberdayaan Hukum Untuk Mendukung Perkembangan Teknologi Dalam Transaksi Melalui Internet* [Law Empowerment for Technology Development Support in Internet Transaction] (Doctoral Degree Thesis, Diponegoro University, 2006) 78–80.

institutions. However, the party should prove that the loss of customer funds occurred owing to a bank's fault or negligence.⁸⁴⁸

5.4.1.2. Law on Information and Electronic Transactions (*LIET*)

LIET is a very important piece of legislation for the development of e-banking in Indonesia. Even though this Act does not directly regulate e-banking, it is concerned with the validity or acceptability of, among other things, electronic information/documents, electronic signatures and electronic contracts for the purposes of EFTs, provided that they are generated by an electronic system in compliance with the requirements set out in *LIET*.

In regard to liability,⁸⁴⁹ *LIET* governs civil and criminal liabilities arising from electronic transactions.⁸⁵⁰ *LIET* makes all electronic system providers, including financial institutions, principally responsible for the reliability and security of their electronic systems, including their electronic agents.⁸⁵¹

In regard to civil liability, Article 12 of the law prescribes that anyone who fails to act prudently to avoid unauthorised use of an electronic signature and secure the use of such signature in the electronic transaction should be liable for the damage that occurs.⁸⁵² Meanwhile, Article 15 of this law articulates the general principle that all electronic system providers should be responsible for the reliability and security of their electronic systems, including for the organisation of their electronic system.⁸⁵³ Further, Article 21 prescribes the liability rule in more detail and differentiates it on whether the transaction is done in person, by authority, or whether it is done through electronic agents in the following terms:

- all legal outcomes due to the execution of an electronic transaction shall become the responsibility of the parties doing the transaction if it is performed by himself/herself;

⁸⁴⁸ A more detailed explanation regarding liability based on tort (tortious liability) can be seen at Chapter 6.

⁸⁴⁹ Post and Telecommunication Directorate, Informatic and Communication Department - Republic of Indonesia, *Penggunaan UU ITE Dalam Penanggulangan Aksi Pembobolan ATM Bank [The Usage of IET Act to Overcome Banks' ATM Theft]* (2010) <http://www.postel.go.id/update/id/baca_info.asp?id_info=1416>.

⁸⁵⁰ See, *LIET* arts 27–37.

⁸⁵¹ *LIET* art 15.

⁸⁵² *Ibid* art 12.

⁸⁵³ *Ibid* art 15.

- all legal outcomes due to the engagement of an electronic transaction shall become the responsibility of the person who gives the authority if it is performed by means of authorisation; or
- all legal outcomes in the execution of an electronic transaction shall become the responsibility of the electronic agent organiser if it is performed through an electronic agent.⁸⁵⁴

Apart from the general liability principles regarding electronic signature and electronic transactions outlined above, *LIET* also stipulates specific provisions in regard of damages that occur pertaining to electronic agent operation. According to Article 21 of *LIET*, if the loss in an electronic transaction occurs due to the operation failure of the electronic agent caused by the third party's action directly on the electronic system, all legal outcomes shall become the responsibility of the electronic agent organiser.⁸⁵⁵ Conversely, if it can be proved that the failure of the operation of the electronic agent is caused by an act of God (*force majeure*) or the consumer's own fault or negligence, then all legal outcomes shall become the responsibility of said consumer.⁸⁵⁶

In regard to the implementation and provision of information technology to consumers, Makarim argues that besides fault/negligent liability or presumed liability that explicitly is contained in *LIET*, strict liability is nevertheless also adopted in the *LIET*. Therefore, he proposed that strict liability should also be applied in regards to the operation of information technology based on its nature and complexity, and the need to protect public interest and confidence in respect of information security.⁸⁵⁷

5.4.1.3. Law No 8 of 1999 on Customer Protection (*LCP*)

The bank's liability is set out in Article 19 to Article 28 in Chapter VI of the *LCP*.⁸⁵⁸ According to the *LCP*, in essence, a business agent shall be liable to provide compensation for damage, contamination, and/or losses sustained by consumers as a

⁸⁵⁴ Ibid art 21(2).

⁸⁵⁵ Ibid art 21(3).

⁸⁵⁶ Ibid art 21(4)–(5).

⁸⁵⁷ Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik* [Electronic Provider Liability] (RajaGrafindo Persada, 2010) 271–2.

⁸⁵⁸ In Indonesia, 'liability' or '*tanggung-gugat*' as a legal term — is often used interchangeably with 'responsibility' or '*tanggung-jawab*'. Even in the Big-Book of Indonesia Dictionary, '*tanggung-gugat*' as a phrase, is not recognised. However, in this thesis, if it is necessary, the phrase *tanggung-gugat* as a legal obligation to pay the damage will be used to distinguish it from *tanggung-jawab* as the term for an ordinary responsibility in the Indonesian language.

result of using goods and/or services produced or traded.⁸⁵⁹ The compensation itself can be in the form of cash or in another form which is of similar value (such as the goods, services, health maintenance, and so on),⁸⁶⁰ and should be payable within an interval of seven days from the date of the transaction.⁸⁶¹ However, business agent liability will be deemed void if the business agent can prove that the damage or loss is caused by the consumer's own fault.⁸⁶² However, the law did not elaborate on what is meant by the 'fault of the consumer'.

Samsul, a parliamentary expert staffer and prominent lecturer in consumer law, argues that to some extent, *LCP* contains good protection provisions for consumers. According to him, the *LCP* has adopted liability based on the fault/negligence principle:

- First, a business entity will always be deemed to be at fault or negligent (presumption of negligence); and
- Second, an business actor/business entity will be responsible for any damages incurred (presumption of liability principle).

Hence, the business actor entity will be always deemed responsible for any damage incurred by consumers (presumed liability), unless the business entity can prove that the consumer is the one who is at fault or has demonstrated negligence (contributory negligence doctrine).⁸⁶³ Thus the onus is on the business actor entity to prove the consumer is at fault or negligent in order to avoid liability; the onus is not on the consumer to prove the bank is negligent or at fault. Therefore, one can assume that in terms of liability for electronic transactions, the *LCP* adopts liability rules based on fault or negligence (fault/negligence liability). However, there is no further explanation in this legislation as to what constitutes 'fault' or 'negligence', especially in electronic funds transactions.

5.4.2. Regulatory Framework for Liability Rules

Liability regulation in the payment system is one aspect that probably is missing from many payments system regulations in Indonesia. In terms of fraud risk, most regulatory

⁸⁵⁹ *LCP* art 19(1).

⁸⁶⁰ *Ibid* art 19(2).

⁸⁶¹ *Ibid* art 19(3).

⁸⁶² *Ibid* arts 19(5), 23. According to the latter provision, the burden of proof for the aspect of consumer fault in a liability lawsuit is a business agent responsibility.

⁸⁶³ Samsul, 'Perlindungan Konsumen', above n 795, 145–6.

content only focuses on risk management and the improvement of security features that should be applied by banks. Provisions regarding the rights and obligations of banks and consumers in the event of fraud are relatively absent from those regulations. In contrast, such regulations have been embraced quite widely in other countries as part of the provisions for consumer protection.

5.4.2.1. Bank Indonesia Regulation Number 14/2/PBI/2012 (*BIR-CBPI*)

Nevertheless, Bank Indonesia Regulation Number 14/2/PBI/2012 Concerning Amendment of Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Operation of Card-Based Payment Instrument Activities (*BIR-CBPI*) can to some extent be utilised in determining parties' responsibilities and/or liabilities in regard to the occurrence of unauthorised ATM/debit card transactions.

In this regulation, the ATM/debit card issuer is obliged to implement risk management, which includes that concerning liquidity, operational matters, and information technology implementation. As part of risk management implementation, issuers of ATM/debit card 'shall be financially ready to meet their liability (payment obligation) that might arise in the event of ATM/Debit card fraud'.⁸⁶⁴

The last sentence above is the only provision on liability contained in the whole of Bank Indonesia regulation in the field of payment systems. Nevertheless, from the inclusion of the phrase 'that might arise' in the provision above, one can infer that there should be one or more conditions which should be met before the issuer is liable to pay for the damage. It is unfortunate that there is no further information or rules in the regulations concerning the sort of conditions that should be met before a bank is obliged to pay for the damage.

5.4.2.2. Bank Indonesia Regulation Number 13/25/PBI/2011

As more bank payment system instruments (such as the payment card system) increasingly rely on information and network technology, banks tend to outsource some of the technological aspects of their system to vendors, partners or other third parties for better solutions and service.⁸⁶⁵ It is very common now in payment card operations that

⁸⁶⁴ Bank Indonesia Regulation Number 14/2/PBI/2012 Concerning Amendment of Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Operation of Card-Based Payment Instrument Activities] (*BIR-CBPI*) art 22.

⁸⁶⁵ Kondabagil, above n 194, 7.

for the sake of efficiency and/or interoperability of ATM/debit card transactions, issuers and/or acquirers of ATM/debit cards might outsource some of their card operations to a third party.

In payment card operations, there are various points of compromise for identity theft that can be attacked. The location of points of compromise spread out from cardholder, through consumer activated terminal, line communications, and to the bank and/or third party's host computer. Thus, in practice, the institution that manages the payment card system at the point of compromise can be the issuer or acquirer, consumer, or another party to which operations are outsourced. Accordingly, there will be some complexity in determining which party should be legally responsible for the security of the compromised point in the payment card system: the consumer, the outsourced party or the issuer/acquirer bank.

To answer this question, Bank Indonesia has enacted Bank Indonesia Regulation Number 13/25/PBI/2011 concerning Prudential Principles for Commercial Banks which Outsource Some Parts of their Works to Another Party. This provision might be used as a guide for determining the party that should be responsible for identity theft/fraud that occurs in the party to which the bank has outsourced part of its operations. According to the regulation, the bank is the one which should be responsible for such occasions.⁸⁶⁶ Banks are also prohibited to outsource if this results in a shift of responsibility or risk to the associated outsourced party.⁸⁶⁷ This regulation aims to enforce prudential principles and risk management in banking operations in accordance with empowering consumer protection. The integrity of the banking system specifically and the financial system in general can be achieved.

⁸⁶⁶ *Peraturan Bank Indonesia Number 13/25/PBI/2011 Tentang Prinsip Kehati-hatian Bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain* [Bank Indonesia Regulation Number 13/25/PBI/2011 Concerning Prudential Principle for Commercial Bank which Outsource Some Parts of Its Works to Other Party] ('BIR-Outsource to Other Party') art 3(3).

⁸⁶⁷ Ibid.

5.5. Lessons to be Learned from Other Jurisdictions Pertaining to Fraud Liability Rules on Unauthorised ATM/Debit Card Transactions

5.5.1. United States: Electronic Fund Transfer Act 1978 and Regulation E

In the United States, the statutory and regulatory law that governs the relationship between the financial institution and the consumer whose deposit account is being debited or credited is the *Electronic Fund Transfer Act 1978 (EFTA)* (Codified at 15 USC §§ 1693–1693r) and its implementing regulation, *Regulation E* (12 CFR pt 205).⁸⁶⁸ Four common consumer electronic funds transfer services that are governed by *EFTA* are ATM transactions (such as cash withdrawals or deposits or transfers between accounts), pay-by-phone services (where consumers order their financial institution to make payments to another), EFT at point-of-sale system (EFTPOS) transactions (where funds are moved from a consumer's account in a bank to a merchant's account through use of a computer terminal at the merchant's place of business); and automated clearing house (ACH) transactions where a consumer's account is automatically debited for a recurring payment, or is regularly credited with wages, pension, and the like.⁸⁶⁹

EFTA was enacted by the Congress to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in the electronic funds transfer system (15 USC § 1693(b) (*EFTA* § 902(b))). It provides a basic framework of provisions to protect individual consumer's rights.⁸⁷⁰ Meanwhile, *Regulation E*, which was adopted by the Board of Governors of the US Federal Reserve Bank, is accompanied by an Official Staff Commentary, containing specific rules, examples, and guidance for financial institutions and practitioners on many specific issues of electronic funds transfers.⁸⁷¹ Basically, *EFTA* and *Regulation E* address two main areas in funds transfer operations, namely the adoption of a mandatory error-resolution process for

⁸⁶⁸ Linda J Rusch and Stephen L Sepinuck, *Payment Systems: Problems, Materials, and Cases* (West, 4th ed, 2011) 306–7. See also Carol Coye Benson and Scott Loftesness, *Payments Systems in the US* (Glenbrook Partners, 2010) 18–19; Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 241. *Regulation E* was issued and is implemented by the Board of Governors of the Federal Reserve System. According to *Regulation E* § 205.3(a), *Regulation E* applies to 'any electronic fund transfer that authorizes a financial institution to debit or credit a consumer's account.'

⁸⁶⁹ Dallas W Lee and Timothy R Zinnecker, *Payment Systems, Banking and Documentary Transactions: Problems, Cases and Comments* (Carolina Academic Press, 2003) 263. See also Wayne K Lewis and Steven H Resnicoff, *Negotiable Instruments and Other Payment Systems: Problems and Materials* (LexisNexis, 2004) 264.

⁸⁷⁰ Lewis and Resnicoff, above n 869, 249. See also Lary Lawrence, *An Introduction to Payment Systems* (Aspen Publishers, 1997) 471–2.

⁸⁷¹ Lawrence, above n 870, 472–3.

electronic funds transfers (*Regulation E*, 12 CFR § 205.11) and liability for unauthorised electronic funds transfers (*Regulation E*, 12 CFR § 205.6).⁸⁷²

Other than that primary concern, *EFTA* and *Regulation E* also oblige financial institutions to pay attention to many consumer protection aspects in fund transfer operations, such as the obligation to give initial disclosures before engaging in their fund transfer products or services (*Regulation E*, 12 CFR § 205.7), to give notice of changes in terms (*Regulation E*, 12 CFR § 205.8), to issue receipts for most transactions conducted at electronic terminals such as ATMs (*Regulation E*, 12 CFR §§ 205.9, 205.16), and to provide periodic statements of account activity (*Regulation E*, 12 CFR § 205.9).⁸⁷³ This last statement must contain various pieces of information. Among these are the amount, date, type, source, and payee of electronic funds transfers to and or from the account during the period covered by the statement, the customer's account number, any fees or charges imposed, the opening and closing account balances for the period, and the address and telephone number to use for error resolution (*Regulation E*, 12 CFR § 205.9(b)).⁸⁷⁴

5.5.1.1. Unauthorised and Authorised Fund Transfers

In the United States, an electronic funds transfer will be categorised as unauthorised if it satisfies two conditions. First, the electronic funds transfer is committed by a person without actual authority (expressly or impliedly) from the consumer (account holder) to initiate the transfer. Second, the consumer has not received a benefit from the transfer (15 USC § 1693i(11); 12 CFR § 205.2(m)).⁸⁷⁵ Therefore, according to Lewis and Resnicoff, an 'unauthorised electronic transfer' means 'a transfer from a consumer's account that is initiated by a person other than the consumer without actual authority, unless the transfer inures to the consumer's benefit.'⁸⁷⁶ Other than that, any electronic funds transfer if it is initiated with an access device that was obtained in an illegal manner, such as through robbery or fraudulent inducement, will also be deemed an unauthorised transaction (12 CFR § 205.2(m)(3), Official Staff Commentary).⁸⁷⁷ In

⁸⁷² Rusch and Sepinuck, above n 868, 314.

⁸⁷³ Ibid 313.

⁸⁷⁴ Fred H Miller and Alvin C Harrell, *The Law of Modern Payment Systems* (Thomson West, 2003) 517.

⁸⁷⁵ Lawrence, above n 870, 480–1.

⁸⁷⁶ Lewis and Resnicoff, above n 869, 256.

⁸⁷⁷ Lawrence, above n 870, 481. *Regulation E* Official Staff Commentary Q 2-27. However, if the consumer gives the access device to another person with actual limited authority which is exceeded, the consumer is liable for the transfers unless a notice revoking authority is given.

contrast, the exception applies so that the transfer is not ‘unauthorized’ where ‘a consumer furnishes an access device and grants authority to make transfer to a person (such as a family member or co-worker) who exceeds the authority given.

As Lewis and Resnicoff explain, according to 15 USC § 1693(11) (*EFTA* § 903(11)), an electronic funds transfer will be deemed ‘authorized’ if the person who accessed the consumer account has been furnished by the consumer with the consumer’s card, code, or other means of access, unless the consumer has notified the financial institution that said person is no longer authorised to access the account. The transfer will also be deemed authorised if the allegedly unauthorised transfer involved fraudulent intent on the part of either the consumer or anyone who acts in concert with the consumer (first party fraud).⁸⁷⁸

5.5.1.2. Consumer’s Liability for Unauthorised Funds Transfers

In general, consumers in the United States are not liable for unauthorised funds transfers. The consumer’s deposit bank is the one that should be held responsible for the unauthorised transfers. Therefore, the definition ‘unauthorised transfer’ is a very important factor in the allocation of fraud liability between consumers and payment system providers.

However, in specific circumstances, consumers could have limited liability for the unauthorised transfer, but only if these three conditions are met (15 USC § 1693g(a); 12 CFR § 205.6(a)): (1) an ‘access device’⁸⁷⁹ is used to initiate the unauthorised funds transfer; (2) the financial institution has provided the consumer with an access device such as PIN, signature, photograph, fingerprint, and so on to identify them when using the device (12 CFR *Regulation E*, § 205.6(a)); and (3) the financial institution has disclosed to the consumer in writing concerning its liability for unauthorised transfer — which includes (among other things) information in a summary of the consumer’s liability, the financial institution’s address and number which can be reached if it is

⁸⁷⁸ Lewis and Resnicoff, above n 869, 255–6. See also Lawrence, above n 870, 482–3.

⁸⁷⁹ See 12 CFR § 205.2(a)(1): An ‘Access Device’ is a ‘card, code or other means of access to a consumer’s account, or any combination thereof, that may be used by the consumer for the purpose of initiating electronic fund transfers.’ Also, an access device is ‘accepted’ when ‘the consumer requests and receives, or signs, or uses, or authorizes use of the device, or requests validation, of an unsolicited device, or receives a device in substitution or as renewal of an accepted device’: *Regulation E* § 205.2(a)(2). See also Lawrence, above n 870, 481. According to Lawrence, ‘a debit card, a PIN, and a code used to make telephonic fund transfers are also access device’.

believed that an unauthorised funds transfer has occurred, and the financial institution's business hours (12 CFR § 205.6(a)).⁸⁸⁰ This distribution of risk regulation gives the consumer's bank motivation to provide consumers with an access device, disclosure and other relevant information pertaining to the possibility of the occurrence of unauthorised funds transfers.⁸⁸¹

If the three conditions above are met, the consumer may incur liability for an unauthorised electronic funds transfer. However, the consumer's portion of liability will be very limited and depend on how rapidly the consumer reports the loss of their access device and promptly informs the financial institution of any unauthorised funds transfers. If this has occurred, then there will be three categories of consumer liability as follows:

- (1) consumer liability is limited to the amount of \$50 for unauthorised funds transfers if the consumer reports a lost or stolen ATM/debit card within two business days from the time s/he learns of it (*Regulation E* § 205.6(b)), whichever is the lesser. Consumers are not liable for any unauthorised funds transfer that occurs after notice has been given to the financial institution;⁸⁸²
- (2) consumer liability is limited to the lesser of whichever is the lesser \$500 or the sum of (1) the amount of unauthorised transfer that could have been prevented had notice been given within the required two business days, plus (2) the lesser of \$50 or the aggregate amount of unauthorised transfers that took place within those two business days, if the consumer reports a lost or stolen ATM/debit card more than two days from the time he learns of it (12 CFR *Regulation E* § 205.6);
- (3) consumer liability is unlimited or similar for all unauthorised funds transfers if a consumer fails to report any unauthorised funds transfer within 60 days of

⁸⁸⁰ Lawrence, above n 870, 483. See also Rusch, above n 106, 586.

⁸⁸¹ Rusch, above n 106, 586-7

⁸⁸² See Lawrence, above n 870, 483-4.

For example, you lost your ATM card on March 1st. Assume that you had reported the loss to your bank on March 2nd. Assume also that the finder makes an ATM withdrawal of \$20 on March 1st. He makes an additional ATM withdrawal of \$200 on March 3rd. Your liability in this example would be limited to \$20. Because the \$200 withdrawal was made *after* you gave notice to the bank of the loss of your access device, you are not liable for any part of that withdrawal. If, instead, the finder had made a \$200 withdrawal on March 1st, your liability would have been in the amount of \$50 because you are only liable for the lesser of the amount of the unauthorized electronic funds transfer of \$50.

receiving a financial institution's periodic statement showing the unauthorised transfer.⁸⁸³

In regard to the limited liability provisions above, consumer negligence that facilitates the occurrence of unauthorised funds transfer — for instance the consumer writing their PIN on the card so enabling the thief to access their account — is not relevant. The limitation on liability applies whether or not the consumer is negligent (12 CFR § 205.6(b)-2, Official Staff Commentary).⁸⁸⁴ Other than these rules that grants a financial institution's consumers in the United States very generous consumer protection, a few other miscellaneous rules provide even more solace to consumers, such as rules pertaining to notification and letter dispatch time, limit of liability, and extenuating circumstances for notification delay.⁸⁸⁵

5.5.2. Australia: ePayments Code

In Australia, regulation concerning unauthorised transfers derived from ATM/debit card transactions are governed by a voluntary codes, namely the ePayments Code (formerly the EFT Code of Conduct), which is administered by the Australian Securities and Investments Commission. The ePayments Code (the Code) sets out the obligations of businesses to consumers, consumer rights and responsibilities, and what to do in the event of a complaint or dispute (most commonly, unauthorised transactions).⁸⁸⁶ The

⁸⁸³ Lewis and Resnicoff, above n 869, 256. See also Miller and Harrell, above n 874, 522–3; Lawrence, above n 870, 483–4.

⁸⁸⁴ Lawrence, above n 870, 483–4.

⁸⁸⁵ Lewis and Resnicoff, above n 869, 256. Some examples of solace rules for ATM/debit card consumers in US are:

First, a cardholder is deemed to give notice as soon as he takes the reasonably necessary steps to provide the issuer with the necessary information. Thus, notice may be given in person, by telephone or in writing. If the cardholder mails the issuer a letter, notice is deemed to be given as soon as the letter is mailed. 12 C.F.R. §205.6(b)(5). Second, notice is deemed to be constructively given if the issuer becomes aware of circumstances that lead to the reasonable belief that an unauthorized transfer — to or from — the cardholder's account has been — or may be — made. Third, if state law or an agreement between the cardholder and the issuer provide a lower limit as to the cardholder's liability, then the cardholder's liability is limited to such lesser amount. Fourth and finally, if the cardholder's delay in notifying the issuer was due to extenuating circumstances, both the 2-day and 60-day time limits are extended to "a reasonable period." 12 CFR § 205.6(b)(4).

⁸⁸⁶ The Australian Securities and Investments Commission is responsible for the administration of the ePayments Code, including compliance monitoring and reviewing it regularly. This code was known formerly as the Electronic Funds Transfer Code of Conduct but renamed with the ePayments Code following a review completed in December 2010. The original code applied until 19 March 2013 when the ePayments Code commenced. There has been a regime for EFT transactions since 1986 when Federal and State Consumer Affairs Ministers endorsed a voluntary code known as the *Recommended Procedures to Govern the Relationship between the Users and Providers of EFT Systems*. For further history of EFT Code, see Alan L Tyree, *Banking Law in Australia* (LexisNexis Butterworths, 4th ed, 2002) 344.

Code is a voluntary code, but once adopted the Code is contractually binding on account institutions.⁸⁸⁷

The Code protects consumers⁸⁸⁸ when transferring fund electronically, including ATM and EFTPOS transactions, telephone and internet banking, debit card and credit card transactions, and some low value stored value products such as smart cards, pre-paid telephone cards and digital cash.⁸⁸⁹ The development of the Code was initially driven by community and government concern about the use of one-sided terms and conditions in allocating liability between the account holder and institution in the event of loss or theft of the account holder's transaction card or PIN.⁸⁹⁰ In preparing the draft of the Code, various overseas models of regulation (including self-regulation) of consumer electronic funds transfers,⁸⁹¹ and Cooter and Rubin's well-known economic theory on loss allocation for consumer payments,⁸⁹² were taken into consideration.

The Code applies only to funds transfers that utilise one or more components such as the use of a device (payment card),⁸⁹³ identifiers⁸⁹⁴ and pass codes⁸⁹⁵ or any

⁸⁸⁷ Virtually all banks, credit unions and building societies (along with a number of non-bank subscribers) currently subscribe to the EFT Code. Re-subscription by EFT Code subscribers to the ePayments Code commences from the Code's release date (20 September 2011). ASIC strongly encourages organisations that provide electronic payments who have not previously subscribed to the EFT Code to subscribe to the new Code. See also W S Weerasooria, *Banking Law and the Financial System in Australia* (Butterworths, 5th ed, 2000) 97.

⁸⁸⁸ See ePayments Code cl 2.6. 'Consumer means a holder in whose name a transaction is performed wholly or predominantly for personal, domestic or household purposes'. 'Holder means 'an individual in whose name a facility has been established, or to whom a facility has been issued'.

⁸⁸⁹ See *ibid* cl 2.5.

⁸⁹⁰ Australian Securities & Investments Commission (ASIC), 'Reviewing the EFT Code' (Consultation Paper 78, Australian Securities & Investments Commission, 2007) 11. See also Tyree, 'Banking Law in Australia', above n 886, 345–6; Australian Securities & Investments Commission, 'Discussion Paper on an Expanded EFT Code of Conduct' (Australian Securities & Investment Commission's, July 1999) ('Discussion Paper on an Expanded EFT') 26.

⁸⁹¹ See ASIC, 'Discussion Paper on an Expanded EFT', above n 890, 20. Some of this overseas regulation is: USA Federal Reserve Board *Regulation E* (Electronic Fund Transfers) (12 CFR Pt. 205); USA Federal Reserve Board Interim Rule Amending *Regulation E* to Permit Electronic Disclosures and Communications [Docket No.R-1002]; European Commission: (a) Communication: 'Boosting Customers' Confidence in Electronic Means of Payment in the Single Market' 9 July 1997 COM (97) 353; and (b) Recommendation Concerning Transactions by Electronic Payment Instruments, 30 July 1997 (OJ No L 208/52 ff); *Payment Cards Act 1984* (Denmark) Consolidated to September 1994; British Bankers' Association Banking Code; New Zealand Bankers' Association Code of Banking Practice (2nd ed. 1996).

⁸⁹² Cooter and Rubin, above n 105.

⁸⁹³ See 'defined terms' in ASIC, *ePayments Code*, cl 2.6. 'Device means a device given by a subscriber to a user that is used to perform a transaction. Examples include: ATM card, debit card or credit card, prepaid card (including gift card), electronic toll device, token issued by a subscriber that generates a pass code, and contactless device'.

⁸⁹⁴ *Ibid*. 'Identifier means information that a user: knows but is not required to keep secret; and must provide to perform a transaction. Examples include an account number or a serial number, or security number printed on a credit or debit card'.

combination of these. The Code was not intended to cover traditional transactions using a manual signature,⁸⁹⁶ because such disputes about the allocation of liabilities are adequately governed by Common Law rules. However, Common Law rules are not adequate to resolve disputes where an access method to conduct fund transfer uses an electronic signature such as PIN. Hence, a code that contains the rights and liabilities between parties involved in electronic funds transfer is a good solution when there is a dispute concerning liabilities.⁸⁹⁷

The Code requires subscribers to give consumers clear and unambiguous terms and conditions, and stipulates how changes in terms and conditions (such as fee increases) are to be notified or handled, and that receipts and statements need to be made or issued, and sets out the rules for determining who pays for unauthorised transactions.⁸⁹⁸ Together with revised legislation in many western countries (such as the US *Electronic Fund Transfer Act 1978*, *Danish Payment Card Act 1984* or less formal regulation such as EFT Code of Conduct in New Zealand), this regulation has produced a more balanced or a more pro-consumer risk allocation rules.⁸⁹⁹ However, Geva contends that, compared to regulation in other countries, the Australian EFT Code of Practice is one of the most comprehensive in both transaction coverage and treatment of issues of unauthorised electronic funds transfers.⁹⁰⁰

Grabosky, Smith and Dempsey have noted that the Code is an alternative to legislative regulatory controls in the banking industries to prevent fraud and to resolve disputes between institutions and customers. They state that codes offer two-fold benefits for the banking industry (including the banking consumers) as they: (1) act as a form of education and publicity for institutions and customers; and (2) provide a statement of recommended practice that can be relied upon to resolve individual disputes. The Code itself could be treated as a guideline to gauge whether or not the participants in the electronic funds transfer have breached civil legal obligations, such as duty of care,

⁸⁹⁵ Ibid. 'Pass code means a password or code that the user must keep secret, that may be required to authenticate a transaction or user. A pass code may consist of numbers, letters, a combination of both, or a phrase. Examples include: personal identification number (PIN), internet banking password, telephone banking password, and code generated by a security token'.

⁸⁹⁶ See ASIC, *ePayments Code*, cl 2.6. 'Manual signature means a handwritten signature, including a signature written on paper and or on an electronic tablet'.

⁸⁹⁷ See Tyree, 'Banking Law in Australia', above n 886, 345–6.

⁸⁹⁸ See ASIC, *ePayments Code*.

⁸⁹⁹ See ASIC, 'Discussion Paper on an Expanded EFT Code of Conduct', above n 890, 28.

⁹⁰⁰ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 257.

insurance, or contractual compliance. Entities that fail to abide by the provisions of the Code could have powerful economic and business sanctions applied as consequences for any breaches.⁹⁰¹

According to clause 2.6 of the ePayments Code, an ‘unauthorised transaction’ is defined as ‘a transaction that is not authorised by a user’. The same clause defines a user as ‘a holder⁹⁰² or an individual who is authorised by a subscriber⁹⁰³ and a holder to perform transactions using a facility held by the holder.’ Therefore, a transaction is authorised if it is performed by a user or by anyone who performs a transaction with the knowledge and consent of a user.⁹⁰⁴

An unauthorised transaction generally profits the fraudster and causes a loss (and a loss that in most incidents of such fraud cannot be recovered). Such losses are to be allocated between the account institution, the consumer, and probably other parties involved in the payment system or network. Prior to the enactment of the Code, financial institutions generally allocated the fraud liability to consumers (‘liability dumping’), at least of those losses that were incurred during the period before the consumers reported to the bank the loss of card and PIN or unauthorised incident.⁹⁰⁵

At its inception, the original EFT Code adopted a limited liability scheme in the event of a consumer not having been careless with the PIN. However, this scheme was only partly successful, because of the financial institutions’ attitudes which often assumed that the consumer must have been careless if any unauthorised transactions occurred. Another drawback of the original code was the absence of any provision in the Code that clearly identified the burden of proof.⁹⁰⁶

Under the ePayments Code, a limited or divided liability scheme is still adopted but in clearer and more detailed provisions. The unauthorised transaction losses are allocated to either the consumer (the account holder) or the account institution — depending on the circumstances of the case. From the consumer point of view, the liability rules adopted by the Code comprise fault-based liability. ‘Fault’ here means that the

⁹⁰¹ Grabosky, Smith and Dempsey, above n 266, 31–2.

⁹⁰² ePayments Code cl 2.6 [Defined Terms] ‘Holder means an individual in whose name a facility has been established, or to whom a facility has been issued’.

⁹⁰³ Ibid. ‘Subscriber’ means ‘an entity that has subscribed to this Code.’

⁹⁰⁴ Ibid cl 9.1.

⁹⁰⁵ Tyree, ‘Banking Law in Australia’, above n 886, 350.

⁹⁰⁶ Ibid.

consumer will be liable for the loss only if the consumer has contributed to the occurrence of the fraud, such as by perpetrating the fraud, leaving a card in an ATM, voluntarily disclosing one or more pass codes to anyone (including a family member or friend), and so on.⁹⁰⁷ Conversely, if a consumer has not contributed to the loss caused by an unauthorised transaction, the financial institution will be liable for the loss (presumed liability) — if such loss is caused by fraud or negligence of the financial institution's employee or agent, including its third party institution involved in system ('vicarious liability'), system malfunction, and/or third party fraudulent activities.⁹⁰⁸ In the ePayments Code, burden of proof is clearly set out and should be borne by the financial institution (subscriber).⁹⁰⁹ Proof of 'fault' by financial institutions must be 'on the balance of probabilities'.⁹¹⁰

5.6. Conclusion

The existence of a well-founded legal and regulatory basis of payment system in a country is an essential factor in creating incentives for all payment system participants to build sound business principles such as responsibility, accountability, trust and confidence. The proliferation of payment system transactions (especially the ATM/debit card transactions), the increasing use of technology in e-banking and more incentives for fraudsters to perpetrate identity theft and fraud in payment card operation have made the risk management mechanism for a robust and secure payment system more important.

In Indonesia, consumer protection has a very strong legal basis since it is governed not only by regulations but also by Indonesia's Constitution. In order to improve consumer protection, banks are obliged to: implement better corporate governance, provide comprehensive, fast and fair procedures to resolve consumer complaints, provide comprehensive and in writing consumer education, and ensure bank transparency, so as to help consumers understand about the benefits and pertinent risks involved in any given e-banking product. Banks also are prohibited from including 'liability dumping' in the standard clauses in their bank-consumer contract.

⁹⁰⁷ See ePayments Code cl 10 [Liability]. See also Tyree, 'Banking Law in Australia', above n 886, 351.

⁹⁰⁸ ePayments Code cl 10. It is clear that *novus actus interveniens* is not a defence in the ePayments Code for unauthorised transactions conducted by third party fraudsters.

⁹⁰⁹ Ibid cll 10.4, 11.2, 11.3.

⁹¹⁰ 'Balance of probabilities' refers to burden of proof in civil trials. It is also known as the 'preponderance of evidence'. In a civil trial, one party's case need only be more probable than the other.

In regard to fraud liability issues, unfortunately Indonesia still does not have specific regulation of loss allocation rules that could give incentives to the parties involved in ATM/debit card transactions to safeguard their transactions. Instead, Indonesia only has general fraud liability rules regulated by scattered regulation such as the *LCP*, *LIET*, and Indonesia's Civil Code (tort law). Even though all of this legislation revolves around bank or business actor liability for damages in relation to their products and services, typically liability will — in the end — be diverted to the consumer when it can be proved that the loss was incurred due to the fault or negligence of the consumer.

A subsequent difficulty, however, is to determine what constitutes negligence or fault in ATM/debit card transactions. In this regard, due to the existence of an asymmetry of information and the problem of lack of resources, consumers always experience difficulties in proving that they are actually innocent. The prolonged disputes themselves are not only detrimental to consumers, but also pose legal and/or reputational risk to the bank.

In contrast to the above problems, in United States (which has its *EFT Act 1978* and *Regulation E*), the bank is the party that should always be liable for unauthorised transactions, regardless of whether consumer negligence exists or not ('strict liability'). Consumers are only liable for the entire loss if it can be proved that they are involved in the unauthorised ATM/debit transaction, or fail to notify the bank within 60 days of the bank statement (listing the unauthorised transaction/s) having been mailed to the consumer.

Meanwhile, unlike the United States, Australia has an e-Payment Code which allocates presumed liability to the business actor and no fault liability for the consumer in the event of an unauthorised ATM/debit card transaction. A consumer might be liable for their loss only if the financial institution could prove on the balance of probability that the consumer was negligent or at fault so as to enable the unauthorised ATM/debit card transactions to happen (liability based on fault/negligence). The Code itself enumerated the nature of bank and consumer liability in ATM/debit card transactions in detail, and placed greater burdens on the banks as the owner of the system to prove consumer negligence. As result, prolonged disputes between bank and consumer about who should be liable for consumer losses caused by unauthorised ATM/debit card transactions in the United States and Australia generally can be avoided.

Therefore, specific and clear fraud liability regulation such as that in the US and/or in Australia that remains absent in Indonesia is strongly needed not only to improve consumer confidence, but also to provide legal certainty and incentives for consumer and banks to be more cautious in ATM/debit card transactions.

CHAPTER 6 THEORY AND PRACTICE OF LIABILITY AND CONSUMER PROTECTION LAW ON DISPUTE RESOLUTION BETWEEN CONSUMER AND BANK CONCERNING UNAUTHORISED ATM/DEBIT CARD TRANSACTIONS IN INDONESIA

6.1. Introduction

When the bank and/or the customer fails to prevent the occurrence of identity theft of the customer's ATM/debit card data that lead to identity fraud which eventually causes the loss of consumer funds, the big question that usually arises is who should bear the loss — whether the bank, the customer or other parties. In order to answer this question, in theory the disputant parties could rely on either the bank–consumer contract or country's loss allocation rules.

This chapter will elaborate on what sort of liability principle theories are relevant for use by the plaintiff in the allocation of losses in the event of an unauthorised ATM/debit card transaction; the remedies, the possibility of defence for the defendant; and the real condition of consumer protection law regarding an unauthorised ATM/debit card transaction. Several cases concerning unauthorised ATM/debit transactions in an alternative dispute resolution (ADR) institution or Indonesian courts also are discussed in order to understand whether there is gap between the liability theories and their implementation in consumer protection law in Indonesia.

There are various types of liabilities, such as vicarious liability, occupiers' liability and tortious liability. In this chapter, there is a detailed in depth discussion of tortious liability, more so than other types of liability. This is the most common type of liability and is often used by plaintiffs to claim redress from (defendant) banks in Indonesia. There is also a discussion of actions against negligence which involves fault elements.

6.2. Overview of Liability Law in Indonesia

Common law and civil law countries generally share common values in terms of liability law, not least in Indonesia, with relatively similar meaning. This is not surprising considering the likelihood of encounters between the common law systems and continental civil law derived systems. In the Netherlands (from whose civil law system many of Indonesia's laws were derived) and other civil law countries, the

judge's decisions (case law) is increasingly regarded as an important source of law,⁹¹¹ whereas in common law countries there is a tendency for statutes to increasingly encroach upon the common law.⁹¹² For instance, in the United States, Eskridge et al posit that '[s]tatutes in twenty-first century America are exuberantly bounteous'.⁹¹³

However, it has to be admitted that liability law in common law countries (such as the United States or Australia) is far more developed than that in Indonesia. One obvious background to this difference is that common law countries have the doctrine of precedent (whereby decisions of superior courts are binding on lower courts). This makes the development of the law very dynamic as it offers reliable guidance over time in various situations (by establishing like and dissimilar situations for the application of law) without the need for legislative change, which is generally a ponderous and most time-consuming undertaking. Meanwhile, in civil law countries (especially in Indonesia), the rule of law is mostly based on legislation rather than case law resulting in the development of liability rules being quite static.

As evidence of this, to date there has been no landmark decision in Indonesian courts over a tort liability case. The landmark decision pertaining to tort law that extended the scope of the tort-related article in the Indonesia Civil Code was the Dutch court's case of *Lindenbaum v Cohen* (1919). To this day, the Dutch case is referred to in every tort case in Indonesia.

The relative stagnation of liability law development in Indonesia can be seen from several pieces of evidence. First, it can be seen from the terminology of liability. The term of 'liability' is often translated as 'responsibility'. Hence, in many English translations of Indonesian law books, the use of the term 'responsibility' actually

⁹¹¹ Irianto, above n 160, 7.

⁹¹² *Penemuan Hukum* [Legal Discovery] (10 April 2010) <<http://wonkdermayu.wordpress.com/kuliah-hukum/penemuan-hukum-atau-rechtsvinding/>>. See also Pam Stewart and Anita Stuhmcke, *Australian Principles of Tort Law* (Federation Press, 2nd ed, 2009) 20. In Australia, the most recent and important example of the incursion of statute into the common law of torts is that of the legislation which has been introduced in every jurisdiction following the Ipp Report (tort law reform legislation), e.g., the *Civil Liability Act 2002* (NSW). The legislation aims to reform aspects of the common law tort of negligence.

⁹¹³ See Eskridge, Jr et al, 'Cases and Materials on Legislation: Statutes and the Creation of Public Policy'; and 'William D Popkin, 'Materials on Legislation: Political Language and the Political Process', cited in Robert F Blomquist, 'The Trouble with Negligence Per Se' (2009) 61(2) *South Carolina Law Review* 221, 222. According to Eskridge et al, 'more than 200,000 bills are introduced in the 50 state legislatures each biennium, and more than 10,000 in each Congress.' Meanwhile, Popkin asserts that 'Legislation is around us ... Statutes have infiltrated into traditional common law areas and created whole bodies of law to deal with the modern welfare state and to regulate activities of modern business.'

denotes two meanings but in practice the two Indonesian words are used interchangeably: namely, ‘responsibility’ (*tanggungjawab*) and ‘liability’ (*tanggung gugat*). Thus, the real meaning of ‘responsibility’ in many writings — that is, whether it connotes responsibility or liability — can only be inferred from the context of or circumstances around the related passages.

Second, many statutes, ordinances or administrative regulations prescribe no liability rules at all. That is, there is no provision that overtly governs compensation or redresses to the plaintiff for losses if the defendant breaches their duty of care and thereby enables fraudulent activities to occur (fraud liability). For example, *LFT* governs funds transfer operations very specifically and in detail. Unfortunately, the law only prescribes the ‘rules of the game’ if funds transfer is delayed or misplaced, but not when the consumer’s funds are missing due to fraud.

Nevertheless, in the *LCP*, *LIET* and Civil Code (tort), there are indeed provisions concerning the liability of the producer, provider, or tortfeasor that causes harm to the plaintiff. However, all the redress provisions in these laws, ultimately count on tortious fault/negligence-based liability. So the damages only can be awarded to the plaintiff if the defendant’s fault/negligence can be established, and the plaintiff is free from any fault (‘clean hands’ principle).⁹¹⁴ Even worse, in the tort law, the onus of proof lies with the plaintiff. Thus, the plaintiff has a burden to prove that a tort has been committed by the defendant. This is, in most cases, difficult or even impossible.

Since Indonesia’s law lacks regulatory provisions and good jurisprudence (case law) in the e-banking fraud liability area (such as in the unauthorised ATM/debit card transactions), the greatest legal value in assessing liability problems will be obtained not only from Indonesian law resources, but also from those of other jurisdictions that have similar problems and more pertinent and valuable jurisprudence.

Nevertheless, it should be borne in mind that some attributes of liability rules, such as the definition of contributory negligence as a means of defence in common law countries, now has a different meaning compared to that of Indonesia’s definition.⁹¹⁵ In

⁹¹⁴ Munir Fuady, *Perbuatan Melawan Hukum [Tort]* (PT Citra Aditya Bakti, 2010) 79–80.

⁹¹⁵ See contributory negligence and comparative negligence definitions in Garner, above n 797, 1134: ‘contributory negligence: A plaintiff’s own negligence that played a part in causing the plaintiff’s injury and that is significant enough (in a few jurisdiction) to bar the plaintiff from recovering damages. In most jurisdictions, this defence has been superseded by comparative negligence’; ‘comparative negligence: A

common law countries, the contributory negligence principle has transformed into a comparative negligence principle. In many western countries, the new definition of contributory negligence under current circumstances and legal policy is contained in a common law country's statute that is the result of that country's laws having been reformed.

Meanwhile, in Indonesia the contributory negligence principle retains the old and unchanged definition (known as 'pure contributory negligence' where the slightest fault on the part of the plaintiff renders any claim null and void), since the 'judge made law' function is almost never effectively utilised. In the absence of civil liability law reform, in practice, the liability law revolves on the old paradigm of tortious liability, with pure contributory negligence as a defence. As a result, this — coupled with the lack of current economic and technological knowledge among most law enforcers (including judges in the court) — makes a fair and just decision in a dispute between banks and their consumers over unauthorised ATM/debit card transactions often unreachable.

6.2.1. General Concept of Liability Rules and the Cause of Action

According to *Black's Law Dictionary*, liability is 'the quality or state of being legally obligated or accountable; legal responsibility to another or to society, enforceable by civil remedy or criminal punishment'.⁹¹⁶ Meanwhile, the law.com legal dictionary, defines liability as the 'legal responsibility for one's acts or omissions'. Gibson and Fraser contend that liability is actually:

the function of the law of tort to determine when the law will, and when it will not, provide a remedy for damages suffered to a plaintiff. Where a plaintiff has suffered damage in accordance with the rules of liability, providing that the rules are correctly stated, then they can be said to be the victim of a tort and entitled to seek a remedy for the infringement or breach of their interest. It is this pursuit of remedies by a plaintiff, which is the very essence of tort law.⁹¹⁷

Therefore, in essence, any person or institution who fails to fulfil their legal responsibility that is created either by regulation or contract, leaves themselves open to

plaintiff's own negligence that proportionally reduces the damage recoverable from a defendant'. See also 'contributory negligence' in Indonesia as defined by Fuady. According to Fuady, contributory negligence is a doctrine that completely bars a plaintiff's recovery if the damage suffered is partly the plaintiff's own fault (also known as 'pure contributory negligence' / 'clean hands' policy): Fuady, '*Perbuatan Melawan Hukum*', above n 914, 79–80.

⁹¹⁶ Garner, above n 797, 997.

⁹¹⁷ Andi Gibson and Douglas Fraser, *Business Law* (Pearson Prentice Hall, 2nd ed, 2006) 88.

a lawsuit for any consequential damages or court order award.’⁹¹⁸ Marzuki explains that liability (*aansprakelijkheid*) is a specific form of responsibility in the area of civil law.⁹¹⁹

When a consumer experiences harm while he or she is using a business product (goods or services), generally many countries in the world have established a consumer’s right to redress in their law on consumer protection.⁹²⁰ However, when business actors refuse to redeem a consumer’s loss, typically the consumer will struggle to attain redress through the liability law area. The terms for various liability rules that exist in the law regarding liability encompass many facets, including strict liability,⁹²¹ absolute liability,⁹²² civil liability,⁹²³ joint and several liability,⁹²⁴ vicarious liability,⁹²⁵ occupiers’ liability,⁹²⁶ contractual liability,⁹²⁷ presumed liability,⁹²⁸ and tortious liability.⁹²⁹

⁹¹⁸ Gerald Hill and Kathleen Hill, *Liability* (13 February 2013) Fine Communications <<http://dictionary.law.com/Default.aspx?selected=1151>>. See also Marzuki, *An Introduction to Indonesia Law*, above n 145, 258–9.

⁹¹⁹ Marzuki, ‘*An Introduction to Indonesian Law*’, above n 145, 258.

⁹²⁰ See Organisation for Economic Co-operation and Development (OECD), *G20 High-Level Principles on Financial Consumer Protection* (16 September 2012 2011) OECD <www.oecd.org/daf/fin/financial-markets/48892010.pdf> 7; OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (16 September 2000) OECD <<http://www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm>> 18; Organisation for Economic Co-operation and Development (OECD), *OECD Recommendation on Consumer Dispute Resolution and Redress* (12 July 2007) OECD <<http://www.oecd.org/sti/consumer/38960101.pdf>> 9; Organisation for Economic Co-operation and Development (OECD), ‘OECD Policy Guidance on Online Identity Theft’ (2008) 11; Department of Economic and Social Affairs, ‘United Nations Guidelines for Consumer Protection (as expanded in 1999)’ (United Nations, 2003) 6; Susan L Rutledge et al, ‘Good Practices for Consumer Protection and Financial Literacy in Europe and Central Asia: A Diagnostic Tool’ (The World Bank, 2010) 6; Consumer International, *In Search of Good Practices in Financial Consumer Protection* (12 July 2013) Consumer International, <<http://www.consumersinternational.org/news-and-media/resource-zone/in-search-of-good-practices-in-financial-consumer-protection/#.UkPxuT-tPSg>> 16.

⁹²¹ Garner, above n 797, 998. ‘Strict liability: liability that does not depend on actual negligence or intent to harm, but that is based on the breach of an absolute duty to make something safe.’

⁹²² Ibid. ‘Absolute liability’ equals ‘strict liability’. ‘Most [it] often applies either to ultra-hazardous activities or in products-liability cases ... also termed absolute liability; liability without fault.’

⁹²³ Ibid 997. ‘Civil liability: 1. liability imposed under the civil, as opposed to the criminal, law. 2. the state of being legally obligated for civil damages.’

⁹²⁴ Ibid. ‘Joint and several liability: liability that may be apportioned either among two or more parties or to only one or a few select members of the group, at the adversary’s discretion. Thus, each liable party is individually responsible for the entire obligation, but a paying party may have a right of contribution and indemnity from non-paying parties; Joint liability: liability shared by two or more parties.’

⁹²⁵ Ibid 998. ‘Vicarious liability: liability that a supervisory party (such as an employer) bears for the actionable conduct of a sub ordinate or associate (such as an employee) because of the relationship between the two parties.’

⁹²⁶ Gibson and Fraser, above n 917, 121, 123. Occupiers’ liability is a field of law of tort which is concerned with the responsibility of the occupiers who because of their control over the premises (through ownership or lease), then they have a duty of care to ensure that anyone (even a trespasser) who comes on to their premises is not exposed to any danger or risk of harm. According to Gibson and Fraser,

In Indonesia, contractual liability is never used by bank consumers to claim economic losses that occur due to unauthorised ATM/debit card transactions. In contrast, banks always use the bank–consumer agreement to reject consumer claims over unauthorised ATM/debit transactions. This fact is not surprising, since the bank–consumer contract is the bank’s standard contract. On the one hand, this contract has many provisions that limit bank liability; on the other hand, it attributes liability to the consumer and/or even shifts the bank’s liability to the consumer (liability dumping). Therefore, most of the damage claims by consumers concerning unauthorised ATM/debit card transactions in Indonesia are based on liability law under the Indonesia’s Civil Code or under *LCP* and not based on contract.

From court verdicts on unauthorised ATM/debit card transactions as can be seen in section 6.4.3.2.2 and 6.4.3.3 below — the tortious liability principle is widely used as a determining principle for allocation of loss in the Court of Justice or ADR institutions in Indonesia. Although tortious liability might be predominant in civil lawsuits in Indonesia, other types of liability law that are arguably inter-connected with tortious liability, such as occupiers’ liability and vicarious liability, will also be discussed.

Therefore, even though this thesis will focus quite exhaustively on tortious liability that arises from liability for breach of duty to take reasonable care that raises *prima facie* questions of negligence, nevertheless occupiers’ liability and vicarious liability also will be discussed whenever necessary.

premises in occupiers’ liability includes a wide range of fixed and movable structures, such as plant and machinery, as well as movables such as ships, railway carriages, and even ladders.

⁹²⁷ See definition of contractual liability at InvestorWords, *Contractual Liability* (2013) [www.investorwords.com <http://www.investorwords.com/19034/contractual_liability.html>](http://www.investorwords.com/19034/contractual_liability.html). Contractual liability is ‘the liability assumed when entering into a contract in which either party to the contract fails to perform in accordance with the terms, otherwise known as a breach of contract’. A promise to perform or deliver a service that may be enforced through adjudication.

⁹²⁸ See Celina Tri Siwi Kristiyanti, *Hukum Perlindungan Konsumen [Consumer Protection Law]* (Sinar Grafika, 2008) 94. In presumption of liability, the defendant is always considered responsible until he/she can prove that he/she is innocent. So, the burden of proof is on the defendant.

⁹²⁹ Garner, above n 797, 998. ‘Tortious liability: liability that arises from the reach of a duty that (1) is fixed primarily by the law, (2) is owed to persons generally, and (3) when breach, is redressable by an action for unliquidated damages. See also BusinessDictionary.com, *Tort Liability* (2013) [www.businessdictionary.com <http://www.businessdictionary.com/definition/tort-liability.html>](http://www.businessdictionary.com/definition/tort-liability.html). There tort liability is defined as:

legal obligation of one party to a victim as a results of a civil wrong or injury. This action requires some form of remedy from a court system. A tort liability arises because of a combination of directly violating a person’s right and the transgression of a public obligation causing damage or a private wrongdoing. Evidence must be evaluated in a court hearing to identify who the tortfeasor/liable party is in the case.

6.2.2. Tortious Liability

The law of tort is an area of law that generally interests people and businesses only when a loss-making event arises.⁹³⁰ Nevertheless, its scope is beyond other forms of civil liability such as contracts.⁹³¹ According to Gibson and Fraser, a tort is:

a civil wrong other than claim for breach of contract and for which a right of civil action for damage may arise. It is an act or omission of the defendant that creates an infringement of an interest of the plaintiff that the law will recognise and which involves the plaintiff proving on the balance of probabilities that their version of the facts is the more believable.⁹³²

Therefore, tort law revolves upon the interactive relationship between the plaintiff and the defendant, and its goal is to focus on how to correct wrongful losses between tortfeasor (wrongdoer in tort, defendant in a tortious action) and victim (plaintiff in such an action).⁹³³

The word of ‘tort’ originates from Anglo-French, and means a ‘wrongful’ or ‘illegal’ act. According to the law, a civil wrong — including in regard to the rights and obligations of an individual — can only be determined by the law of torts (in Dutch ‘tort’ is translated as ‘*onrechmatige daad*’ or ‘unlawful act’)⁹³⁴ and includes acts of omission as well as commission in the code law state of the Netherlands (the colonial source of much Indonesian law) just as it does in the law of Australia, a common law country. The law of torts itself is difficult to define succinctly since it has extensive meanings and its boundaries are indistinct. However, torts differ from other forms of civil liability such as contracts, albeit sometimes there is a degree of ‘cross over’. Tort is dynamic. Political, economic, social mores and the existence of gaps in civil liability law may affect the development of tort law.

The law of torts can be divided into three types, namely intentional (or direct) torts, unintentional (or indirect torts), and miscellaneous torts. Intentional tort is where a defendant ‘intentionally carries out a wrongful act that directly causes harm to the plaintiff’.⁹³⁵ Some examples of intentional torts include trespass to the person (assault, battery, false imprisonment), to land, and/or to goods. Unintentional torts lack the

⁹³⁰ Fuady, ‘*Perbuatan Melawan Hukum*’, above n 914, 2. See also Gibson and Fraser, above n 917, 81.

⁹³¹ Stewart and Stuhmcke, above n 912, 4.

⁹³² Gibson and Fraser, above n 917, 82.

⁹³³ Stewart and Stuhmcke, above n 912, 5.

⁹³⁴ Fuady, ‘*Perbuatan Melawan Hukum*’, above n 914, 2. The concept of tort is well-known in European civil law countries.

⁹³⁵ Gibson and Fraser, above n 917, 86. See also Makarim, above n 857, 179.

element of intention and are based on a legal concept known as ‘actions on the case’, and the best example of it today is negligence. Makarim contends that negligence per se and *res ipsa loquitur* are two kinds of negligence where the plaintiff does not need to prove his/her claim.⁹³⁶ Miscellaneous torts are neither intentional nor unintentional, and the example most relevant to business is nuisance.⁹³⁷

Agustina in her dissertation in Indonesia (as cited by Makarim) compared ‘unlawful act’ that is derived from Indonesia’s Civil Code with tort law in common law countries. In essence, she maintained that both terminologies have many things in common, with only slight differences existing. Makarim concurs with Agustina that in general ‘unlawful act’ — ‘*perbuatan melawan hukum*’ in Bahasa Indonesia and ‘*onrechtmatige daad*’ in Dutch — is basically similar to tort, and thus the terminology could be used interchangeably.⁹³⁸

In Indonesia, before 1919, tortious liability or ‘unlawful act’ only suggested the action of breaking the statute (narrow interpretation); however, since the Netherlands’ 1919 landmark case of *Lindenbaum v Cohen* (reported in *Nederlandse Jurisprudentie 1919* — which is no less remarkable than the 1932 United Kingdom (House of Lords) equivalent case of *Donoghue v Stevenson* [1932] — the Dutch Supreme Court (*Hoge Raad*) accepted a more extensive interpretation of the requirement of ‘unlawfulness’. The impact of this case was very wide: the *Hoge Raad* extended the scope of protection of the general tort so as to include, in addition to any act which breaches the statute, and any of the following actions: (1) any action that is in conflict with another party’s rights;⁹³⁹ (2) any action that is in conflict with the party’s own legal obligations;⁹⁴⁰ (3)

⁹³⁶ Makarim, above n 857, 180.

⁹³⁷ Fuady, ‘*Perbuatan Melawan Hukum*’, above n 914, 3. See also Gibson and Fraser, above n 917, 86.

⁹³⁸ Makarim, above n 857, 169–77.

⁹³⁹ Rachmat Setiawan, *Tinjauan Elementer Perbuatan Melawan Hukum* [Basic Overview of Tort] (Alumni, 1982) 17. A subject’s personal rights include the right to freedom, a good name and honour, and property rights. See also Setiawan, *Aneka Masalah Hukum dan Hukum Acara Perdata* [Various Legal Problems and the law on Civil Procedure] (Alumni, 1992) 260–2.

⁹⁴⁰ Setiawan, ‘*Tinjauan Elementer Perbuatan Melawan Hukum*’, above n 939, 18–19. Legal obligation is an obligation that derived from regulation. Hence tort in this case is any act or omission that conflicts with regulation. See also Setiawan, ‘*Aneka Masalah Hukum dan Hukum Acara Perdata*’, above n 939, 252–4. Setiawan describes further that based on current case law in the Netherlands, in order for a matter to be established as tort, several requirements must be met. Indeed for it to be held that ‘any action ... is in conflict with its own legal obligation’, several pre-requisites must be satisfied. These are: a) the plaintiff’s interest is in jeopardy because of such tort; b) the violated regulations were intended to protect the interest of the plaintiff; c) the plaintiff’s interests are included in the interests intended to be protected by the Article 1365 of the Indonesian Civil Code; d) the violation of the regulation was contrary to the

any action that conflicts with morality;⁹⁴¹ or (4) any action that conflicts with prudential principles or appropriate conduct in a good society.⁹⁴²

As described previously, tort provisions that are relevant to the unauthorised ATM/debit card transactions in Indonesia are Articles 1365 to 1367 of Indonesia's Civil Code 1848. Article 1365 is the 'umbrella' provision for tort claims in Indonesia. The tortious liabilities principle that is contained in this Article is 'at fault/negligence' liability, that is, liability based on fault/negligence.⁹⁴³ According to Article 1365, 'A party who commits an unlawful act which causes damage to another party, shall be obliged because of his/her fault to compensate the damage'. Kristiyanti concurs with this Article from the point of view of common sense. According to her, it does make sense nor is it reasonable that a guilty party not compensate their victims for losses sustained; conversely, it is not fair that innocent parties should compensate the losses suffered by others (or that the victim be recompensed by other than the guilty party).⁹⁴⁴ In fact, Kristiyanti's view on the article 1365 of Civil Code is indisputable and also reflects the view of the author and that of the vast majority of Indonesians. However with the current bank-consumer standard contract which is always favours the bank and/or with the current legislation regarding fraud liability that is too general to be implemented in regard to unauthorised ATM/debit card transactions cases, the consumer victims always have difficulties in proving bank negligence and/or fault.

Meanwhile Article 1366 of Indonesia's Civil Code further explains that the liability for such acts applies not only in relation to an intentional act by the party responsible for

proper good conduct that should be addressed to the plaintiff; e) there is no justification under the law [for the action or lack thereof].

⁹⁴¹ Unwritten rules with respect to proper conduct, which reasonably can be expected of reasonable people in their conduct within the community (objective criteria — special expertise/knowledge of the tortfeasor may aggravate criteria applicable). See Setiawan, '*Tinjauan Elementer Perbuatan Melawan Hukum*', above n 939, 19–20. According to Setiawan, what constitutes good moral conduct alter according to the place and time. See also Setiawan, '*Aneka Masalah Hukum dan Hukum Acara Perdata*', above n 939, 265–6.

⁹⁴² Fuady, '*Perbuatan Melawan Hukum*', above n 914, 6; Setiawan, '*Aneka Masalah Hukum dan Hukum Acara Perdata*', above n 939, 251–70, 266–9; Setiawan, '*Tinjauan Elementer Perbuatan Melawan Hukum*', above n 939, 17; Hermansyah, above n 683, 261–3. See also Gibson and Fraser, above n 917, 6–9, 30–3. According to Rachmat Setiawan, an act is in conflict with appropriate conduct in a good society if: (a) that act jeopardises other people's rights without any compelling reason; (b) that act is useless and endangers other people, which action according to the common people should not be done.

⁹⁴³ Kristiyanti, above n 928, 92–3.

⁹⁴⁴ Ibid 93.

the damage, but also includes any damages that occurred because of the party's negligence or recklessness ('less cautious' conduct).⁹⁴⁵

Besides tortious liability, Indonesia's Civil Code also states that each person/institution is not only liable for damage caused by their own action, but also for the damage caused by acts of the dependents (vicarious liability), or by items or infrastructure under their control (occupiers' liability).⁹⁴⁶

6.2.3. Vicarious Liability

In law, a person is liable for any of their conduct that causes harms to others. However, there is always a possibility that a person is to be held responsible for the acts or omissions of another, even though the person does not have any wrong or direct causation to the damage incurred. This is known as 'vicarious liability', which is always strict liability. Vicarious liability is liability 'that a supervisory party (such as an employer) bears for the actionable conduct of a subordinate or associate (such as an employee) because of the relationship between the two parties'.⁹⁴⁷ A common example of vicarious liability can be found in the relation between an employer and its employee or between a principal and its agent.⁹⁴⁸ In relation to agency, Gautama asserts that agency is governed by Articles 1792–1819 of Indonesia's Civil Code.⁹⁴⁹ According to him, Article 1792 of the Code concerning 'mandate' seems too narrow and refers 'only to agency contracts which involve representation, that is, ostensible mandates by virtue of which an agent is able to bind his principal directly to a third party'. The principal is liable for the torts of his agent committed while acting in his capacity as principal's agent.⁹⁵⁰

⁹⁴⁵ Indonesian Civil Code art 1366: 'An individual shall be responsible, not only for the damage which he has caused by his act, but also for that which was caused by his negligence or carelessness.' See also P N H Simanjuntak, *Pokok-Pokok Hukum Perdata* [The Civil Law Cores] (Djambatan, 2009) 353.

⁹⁴⁶ *Kitab Undang-Undang Hukum Perdata* [Civil Code] art 1867: 'An individual shall be responsible for the damage which he has caused by his own act, as well as for that which was caused by the acts of the individuals for whom he is responsible, or caused by matters which are under his supervision.' See also Makarim, above n 857, 165; Marzuki, *An Introduction to Indonesia Law*, above n 145, 259; Kristiyanti, above n 928, 93–4.

⁹⁴⁷ Garner, above n 797. See also Marzuki, *Pengantar Ilmu Hukum*, above n 155, 259; Hans Kelsen, *Teori Umum Tentang Hukum dan Negara* [General Theory on Law and State] (Nusa Media, 2011) 101–2.

⁹⁴⁸ Gibson and Fraser, above n 917, 139.

⁹⁴⁹ According to Article 1792 of the Indonesian Civil Code, the 'mandate' (*lastgeving, pemberian kuasa*) is a contract in which one person, the principal or mandating party, gives to another, the mandate, a power to execute a legal act in the principal's name.

⁹⁵⁰ Sudargo Gautama, *Indonesian Business Law* (PT Citra Aditya Bakti, 2006) 105–9.

Muhammad argues that the acknowledgement of vicarious liability is derived from Article 1367 of Indonesia's Civil Code.⁹⁵¹ Its acknowledgement by the law can be demonstrated by several Indonesian Supreme Court cases, among them, the Indonesia Supreme Court verdict in *PT Bintang v PT Indah*, dated 4 June 1973 No 558/K/SIP/1971.⁹⁵²

The principle of vicarious liability can also be found in the legislation governing electronic transactions. Article 21(2).c of *LIET* in essence states that the provider of the electronic agent shall be responsible for any legal ramifications arising from the use of it in electronic transactions. This Article is progressive, because it has provided legal certainty regarding the application of the responsibility of the principal for the agent that is not a natural person. Hence, the legal status of any electronic agent (such as ATMs, EFT-POS machines, and so on) has been equated by *LIET* with the legal status of a human agent. As a result, banks as the providers of electronic agents such as ATM and/or EFT machines (and therefore are the principals) will be responsible for any legal ramifications that are derived from electronic transactions that happen in regard to their electronic agents.

Further, sometimes it is more efficient for banks to outsource some parts of their business activities or their supporting system to other parties (outsourcing company/agent) based on outsourcing agreements. An outsourcing company could to some extent just provide workers to undertake the bank's activities, or even provide comprehensive business solutions (including provision of staff for such tasks as are covered by said agreement, for example a call centre for banking customers or ATM/EFTPOS inter-operability under similar principal and/or switching company). In

⁹⁵¹ Indonesia Civil Code art 1367: 'an individual shall be responsible for the damage which he has caused by his own act, as well as for that which was caused by the acts of the individuals for whom he responsible, or caused by matters which are under his supervisor.'

⁹⁵² Facts of the case: on 4 June 1965, Soegiono Atmodiredjo (employee of PT Star-owned bus company) caused a bus owned by PT Indah to be burned due to his negligence. When Mr Atmodiredjo was refueling the bus (itself owned by PT Bintang) in Purwokerto terminal using a bucket, a bus passenger threw cigarette butts down and ignited a fire on PT Bintang's bus. That fire also burned the PT Indah bus that was parked nearby. On 1 September 1966, the PT Indah bus owners sued the owners of the first bus (PT Bintang) for damages.

In an earlier criminal case, Mr Atmodiredjo has been sentenced on the basis of 'negligence caused the fire' (judgment dated February 4, 1966). The Tegal District Court ruled in a civil case (filed by PT Indah, on 7 March 1968) that PT Bintang pay compensation to PT Indah. Next, PT Bintang appealed, but the High Court's decision on 20 May 1970 in essence is still the same as the district court verdict. PT Bintang further filed a cassation. The Supreme Court in its verdict on 4 June 1973 rejected PT Bintang's cassation. Accordingly, the High Court's decision was final and binding.

relation to the issues of liability rules that might apply to this kind cooperation, Bank Indonesia has enacted Bank Indonesia Regulation Number 13/25/PBI/2011 Concerning the Prudential Principle for a Commercial Bank which Outsources Some Parts of Its Works to Another Party. Article 3(3) highlights that the bank, as the principal of the work, is responsible for any legal effect that occurs in relation to this outsourcing agreement, regardless of whether the outsourcing company is the one who is executing the bank business activities. Banks also are liable if the outsourcing party has caused damage to the banks' consumers.⁹⁵³

From the case law and regulations above, it can be concluded that the liability for an unlawful act or tort not only bind a bank itself (as tortfeasor) for its direct actions, but for the actions of its employees and/or agents (both electronic and natural persons) who are under its supervision and whose actions are therefore the bank's responsibility.⁹⁵⁴ Therefore, banks will always be liable for their employees' conduct that is subject to Article 1367 of Indonesia's Civil Code and causes damage to consumers or other third party. The damages themselves should be treated as a cost of business.⁹⁵⁵

6.2.4. Occupiers' Liability

Occupiers' liability is a field of tort law which concerns the responsibility of the occupiers who because of their control over the premises (through ownership or lease),⁹⁵⁶ have a duty of care to ensure that anyone (even trespassers) who comes on to their premises is not exposed to any danger or risk of harm.⁹⁵⁷ Rustard and Daftary contend that 'a property owner who invites the public onto his property for business purposes is potentially liable if those invitees are harmed by negligent or accidental (inadvertent) acts by third parties'. As indicated earlier, property in the banking context includes ATMs/EFTPOS machines and associated physical and electronic (including

⁹⁵³ See *Peraturan Bank Indonesia Number 13/25/PBI/2011 Tentang Prinsip Kehati-hatian Bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain* [Bank Indonesia Regulation Number 13/25/PBI/2011 Concerning Prudential Principle for Commercial Bank which Outsource Some Parts of Its Works to Other Party] (*BIR-Outsource to Other Party*) art 3(3).

⁹⁵⁴ Abdulkadir Muhammad, *Hukum Perdata Indonesia [Indonesia Civil Law]* (Citra Aditya Bakti, 2010) 271–2.

⁹⁵⁵ Djumhana, above n 68, 341.

⁹⁵⁶ 'Premises' include a wide range of fixed and movable structures, such as plant and machinery, as well as movables such as ships, railway carriages, and even ladders. See Gibson and Fraser, above n 917, 123.

⁹⁵⁷ *Ibid* 121.

software) infrastructure. Courts will impose liability if the risk of harm to visitors was reasonably foreseeable.⁹⁵⁸

The main element of occupiers' liability is the occupier's control over the property. The duty of care owed by the occupier/s is directed not only to the invitee, but to anyone who enters the premises including guests (those who enter by express or implied permission), and even those who are uninvited, such as trespassers. Hence liability of the occupiers will arise if an accident occurs which is caused by the defective or dangerous condition of the premises.⁹⁵⁹

When an accident occurs in or on the premises, the plaintiff must ascertain at least two elements to establish a case of 'occupiers' liability, which are: (1) 'the defendant has occupation or control of the land or structure'; and (2) 'the defendant was negligent.'⁹⁶⁰ Therefore, the plaintiff has to establish that the defendant was responsible for the harm that happened within the plaintiff's property, or that the defendant ought to have known that there was a foreseeable risk of injury and unreasonably has done nothing to remove the risk.

However, the degree of care that is to be expected from the occupiers relies on whether or not the risk is obvious. If the risk is obvious (to the plaintiff), the duty of the defendant will be minimal, and vice versa. In the High Court in *The Council of the Shire of Wyong v Shirt* (1980) 146 CLR 40, Mason J explained how to test for determining what the occupier must do to discharge the duty of care. He contended that two questions should be raised:

- Would a reasonable person in the defendant's position have foreseen that the conduct involved a real risk of injury to the plaintiff? If the risk is real, and it doesn't matter if it is remote or unlikely to happen, then;
- What would a reasonable person do in response to the risk?⁹⁶¹

These questions require some factors to be considered. These include the foreseeability (by the defendant) of the risk, information regarding the magnitude of the risk, the cost

⁹⁵⁸ Michael Rustad and Cyrus Daftary, *E-Business Legal Handbook* (Aspen Law & Business, 2001) 397–8.

⁹⁵⁹ Gibson and Fraser, above n 917, 121. See also *Australian Safeway Stores Pty Ltd v Zaluzna* (1986) 162 CLR 479.

⁹⁶⁰ Gibson and Fraser, above n 917, 121.

⁹⁶¹ *Ibid* 124.

of removal the risk, its degree of probability, whether the risk is ordinary, and whether it is obvious risk.⁹⁶²

In Indonesia, occupiers' liability is derived from Article 1367 of Indonesia's Civil Code, especially its last sentence: 'an individual shall be responsible for the damage which he has caused by his own act, as well as for that which was caused by the acts of the individuals for whom he responsible, or *caused by matters which are under his supervision*' (emphasis added).

Fuady argues that if someone suffers a damage caused by infrastructure under the occupier's control, the law obliges the owner of the infrastructure to help the victim and also to warn the user of such infrastructures regarding the risk (duty of rescue or warning). Defendants are also liable for the damages if it is established that the defendant has an obligation to control that risk in regard to its controlled party/parties (such as guests or consumers) but has done nothing to secure them from third party attack.⁹⁶³ Further Setiawan explains that the statute does not give the responsibility for monitoring just to the owner of infrastructure, but also to every person that has an obligation to secure and monitor the infrastructure, such as the tenant, user, or employee of the owner.⁹⁶⁴

6.3. Tort of Negligence

Historically, tort caused by negligence or an inadvertent form of violation of customs and proprietary conduct in public has been so regarded and unlawful in the Netherlands and Indonesia after the 1919 *Lindenbaum v Cohen* case. Meanwhile, in common law countries, a tort of negligence has been recognised since the early 19th century.⁹⁶⁵

In tort law, the tort of negligence is the most pervasive tort in practice — including in Indonesia — in providing remedy to victims who suffer loss because of the fault of another. Negligence is the most common action in tort law. Vickery and Pendleton state that '[n]egligence law is concerned with whether people have been so careless or faulty

⁹⁶² Ibid.

⁹⁶³ Fuady, 'Perbuatan Melawan Hukum', above n 914, 94. See also Sidabalok, above n 792, 107.

⁹⁶⁴ Setiawan, 'Tinjauan Elementer Perbuatan Melawan Hukum', above n 939, 55–6.

⁹⁶⁵ Fuady, 'Perbuatan Melawan Hukum', above n 914, 3. See also Gibson and Fraser, above n 917, 71–2.

[sic], or breached [a] special legal duty, that they should be liable for the loss they have caused.’⁹⁶⁶ *Black’s Law Dictionary* defines negligence as:

the failure to exercise the standard of care that a reasonably prudent person would have exercised in a similar situation; any conduct that falls below the legal standard established to protect others against unreasonable risk of harm, except for conduct that is intentionally, wantonly, or wilfully disregarding of others’ rights.⁹⁶⁷

Meanwhile, Gibson and Fraser define negligence as ‘the omission to do something which a reasonable person would do, or doing something which a prudent and reasonable person would not do. It is the failure to exercise reasonable care and skill.’⁹⁶⁸

6.3.1. Element of Negligence

In order for it to be determined that an action in negligence has occurred, the elements of negligence should be present, namely: a duty of care, and a breach of that duty, causation, and damage.⁹⁶⁹ Even though each of these elements is complex, it is essential for each to be established by the plaintiff in order to be successful in a tort of negligence case.

In the negligence claim inquiry, the court is supposed to find any relevant legal rules and concepts applicable to the specific case, whether they are well established, still being developed and/or even subject to some uncertainties.⁹⁷⁰ In *Jaensch v Coffey* (1984) 155 CLR 549 at 585–86, the ‘components’ of an action in negligence are set out by Deane J as follows:

- (i) a relevant duty owed by the defendant to the plaintiff to take reasonable care resulting from the combination of (a) reasonable foreseeability of a real risk that injury of the kind sustained by the plaintiff would be sustained either by the plaintiff, as an identified individual, or by a member of a class which included the plaintiff, (b)

⁹⁶⁶ Roger Vickery and Wayne Pendleton, *Australian Business Law: Compliance and Practice* (Pearson Education Australia, 2009) 85.

⁹⁶⁷ Garner, above n 797, 1056.

⁹⁶⁸ Gibson and Fraser, above n 917, 93. See also Sidabalok, above n 792, 107–11.

⁹⁶⁹ Zulham, *Hukum Perlindungan Konsumen* [Consumer Protection Law] (Kencana, 2013) 84; Donn B Parker, *Fighting Computer Crime: A New Framework for Protecting Information* (John Wiley and Sons, 1998) 429–30; Gibson and Fraser, above n 917, 93; Stewart and Stuhmcke, above n 912, 135. Even though the elements of torts sometimes are depicted by various writers as three or four elements, in essence the elements are placed in the same category, where sometimes the writer put two elements such as causation and damage under the same number. For instance, Stewart and Stuhmcke note that to succeed in a negligence claim, a plaintiff will have to prove three elements of tort, which are:

- (a) that the defendant owed the plaintiff a duty of care;
- (b) that the defendant has breached that duty of care by negligent conduct; and
- (c) that the defendant’s breach caused the plaintiff actual damage which is not too remote from the breach.

⁹⁷⁰ Stewart and Stuhmcke, above n 912, 136.

existence of the requisite element of proximity in the relationship between the parties with respect to the relevant act or omission and the injury sustained, and (c) absence of any statutory provision or other common law rule (e.g., that relating to hazards inherent in a joint illegal enterprise) which operates to preclude the implication of such a duty of care to the plaintiff in the circumstances of the case; (ii) a breach of that duty of care in that the doing of the relevant act or the doing of it in the manner in which it was done was, in the light of all relevant factors, inconsistent with what a reasonable man would do by way of response to the foreseeable risk.; and (iii) injury (of a kind which the law recognizes as sounding in damages) which was caused by the defendant's carelessness and which was within the limits of reasonable foreseeability.⁹⁷¹

6.3.1.1. Duty of Care

A duty of care is 'a legal relationship arising from a standard of care, the violation of which subjects the actor to liability'.⁹⁷² The plaintiff must first ascertain that the defendant owed a duty of care. In common law countries, the landmark case which shows circumstances where the defendant owe a duty of care to the plaintiff, was first described by Lord Atkin in *Donoghue v Stevenson* (1932) AC 562 in terms of the 'neighbour' principle:

The rule that you are to love your neighbour becomes in law, you must not injure your neighbour; and the lawyer's question, Who is my neighbour? receives a restricted reply. You must take reasonable care to avoid acts or omissions which you can reasonable foresee would be likely to injure your neighbour. Who in law, is my neighbour? The answer seems to be — persons *who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question.*⁹⁷³

⁹⁷¹ See *Jaensch v Coffey* (1984) in Stewart and Stuhmcke, above n 912, 136.

⁹⁷² Garner, above n 797, 523. Duty: A legal obligation that is owed or due to another and that needs to be satisfied. See also Martin Davies and Ian Malkin, *Torts* (LexisNexis Butterworths, 5th ed, 2008) 30; Zulham, Hi and Hum, above n 969, 84.

⁹⁷³ *Donoghue v Stevenson* [1932] AC 562 (emphasis added). See also Gibson and Fraser, above n 917, 94–5. See also Stewart and Stuhmcke, above n 912, 134.

[Note: To understand this passage of Lord Atkin, it is necessary to see the passage to what he is alluding. Thus, see also re the origin of the phrase and concept to which he refers: Mark 12: 30–1 and especially the parable of Luke 10: 25–36 which is in response to a question from a scribe ('lawyer' or teacher of the law referred to by Lord Atkin). Both of these expand the 'neighbour' concept from its initially narrow boundaries (of Leviticus 19:18 which refers to 'sons (children) of your people') to all persons, and create a 'duty of care' (having 'mercy' on others in their distress, and to the extent that one would like to have such consideration shown to oneself). Lord Atkin moves from this generous definition in the New Testament to a far more narrow 'legal' one (see italicised section in text above) and one far from the definition in both the Jewish *Torah* and the Christian *New Testament*.] See further below:

Donoghue v Stevenson (1932):

Facts of the case: A friend bought a bottle of ginger beer for Donoghue. The ginger beer was in an opaque glass bottle. While in the course of drinking the contents of the bottle she noticed the decomposed remains of a snail. As a result, she became sick and suffered shock. She sued the manufacturer of the ginger beer (Stevenson), alleging that he had been careless in manufacturing his product so as to allow a snail to be part of the contents.

Decision: The plaintiff was entitled to recover damages against the manufacturer in negligence. Any person who manufactures products in such a way that there is no reasonable possibility of intermediate examination before they reach the ultimate consumer, and who knows that the absence of reasonable care

In this case, a specific and a general ratio decidendi ('reason for decision') held by the court are: (1) specific ratio: 'where a product cannot be inspected prior to use, the manufacturer has a duty to take reasonable care to ensure it does not contain any harmful defect'; (2) general ratio: 'the rule that you are to love your neighbour becomes, in law, you must not injure your neighbour'. Thus the general rule from this case is: 'you must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour'.⁹⁷⁴

However, before Lord Atkin's landmark decision in *Donoghue v Stevenson* (1932), it was the judgment of Brett MR (later Lord Escher) that applied. His decisions in *Heaven v Pender* (1883) 11 QBD 503 and in *Le Lievre v Gould* [1893] 1 QB 491 relied entirely on 'reasonable foreseeability'. In the former case, however, he proposed a general rule for the imposition of duty of care which was later approved by Lord Atkin in his landmark judgment. The obiter dicta of Brett MR advised:

[W]henver one person is by circumstances placed in such a position with regard to another that every one of ordinary sense who did think would at once recognise that if he did not use ordinary care and skill in his own conduct with regard to those circumstances he would cause danger of injury to the person or property of the other, a duty arises to use ordinary care and skill to avoid such danger.⁹⁷⁵

6.3.1.2. Breach of Duty of Care

In a breach of the duty of care, the plaintiff has then to prove that the defendant has breached the standard of care owed to the plaintiff. In common law, this required consideration of two factors, namely 'the degree of foreseeable risk created by the defendant's conduct and the reasonableness or otherwise of the defendant's response'.⁹⁷⁶ An objective standard is required to test in regard to the 'reasonable person' and based on the facts of the case, how such a person would have responded to the foreseeable risk.

on their part will result in an injury to the consumer's life or property, owes a duty to the consumer to take reasonable care. See also *Goldman v Hargrave* (1967) 1 AC 645. See also *Cook v Cook* (1986) CLR 376.

Since the decision in *Donoghue v Stevenson*, the law of negligence has developed and expanded significantly so that the tort of negligence today offers a remedy in many categories of cases and new duty situations are still occasionally being recognised or extended by the courts.

⁹⁷⁴ Vickery and Pendleton, above n 966, 88. See Fuady, 'Perbuatan Melawan Hukum', above n 914, 87.

⁹⁷⁵ *Heaven v Pender* (1883) 11 QBD 503 at 509. See Stewart and Stuhmcke, above n 912, 133.

⁹⁷⁶ Gibson and Fraser, above n 917, 100. See *Kosciusko Thredbo Pty Ltd v Smith* (2001) NSWCA 355. See also Stewart and Stuhmcke, above n 912, 156.

In the tort of negligence, a defendant's conduct is gauged by the test or standard of what a 'reasonable person of ordinary prudence' would have done in the same circumstances as the defendant. Hence, on the balance of probabilities, the plaintiff must prove that the defendant omitted to do something, which a reasonable person would have done or did what a reasonable person would not have done under those circumstances. If under the test it is concluded that the defendant's conduct falls below the reasonable person's standard of care, the defendant will be deemed to have breached of their duty of care.

In common law, the meaning of negligence can be distilled from the decision by Alderson B in *Blyth v Birmingham Waterworks Co* (1856) 11 Exch 781; 156 EF 1047 at 1049: 'Negligence is the omission to do something which the reasonable man guided upon those considerations which ordinarily regulate the conduct of human affairs, would do, or doing something which a prudent and reasonable man would not do.'⁹⁷⁷

The standard of care test is basically objective, even though it has inevitably some limited subjective elements. The subjectivity elements of this standard before the court for the individual case depend on the specific attributes of the defendant, such as whether the defendant is merely a layman or a professional with knowledge specific to the area.⁹⁷⁸

6.3.1.3. Causation and Scope of Liability

There is no cause of action for negligence unless the plaintiff can prove on the balance of probabilities that the harm suffered was caused by the defendant's breach of their duty of care. Causation also has an important role in determining to what extent damages could be recoverable.⁹⁷⁹ Stewart and Stuhmcke stress that the question of causation comprises two main issues:

The first is concerned with factual causation: that is, whether the defendant's negligence was at least a partial cause of the plaintiff's damage. It needs to be established whether it was a "material cause" or a "necessary condition" of the loss. The second and more difficult question is whether the defendant should bear legal responsibility for the

⁹⁷⁷ Stewart and Stuhmcke, above n 912, 158–9. See also *Civil Liability Act 2002* (NSW) s 5B(1)(c); Rustad and Daftary, above n 958, 141.

⁹⁷⁸ Stewart and Stuhmcke, above n 912, 158–68. A court may consider evidence of the standards set by professionals to assist in the determination of the legal standard of care expected of the defendant.

⁹⁷⁹ Gibson and Fraser, above n 917, 107; Stewart and Stuhmcke, above n 912, 190. See Fuady, 'Perbuatan Melawan Hukum', above n 914, 111–12.

plaintiff's loss and whether liability should extend to all the damage suffered by the plaintiff: that is, what is the "scope" of the defendant's liability.⁹⁸⁰

In the civil liability law reforms undertaken in most Australian states and territories (for instance, in New South Wales (NSW) with the *Civil Liability Act 2002* (NSW)), general principles are drawn to determine causation in negligence. According to section 5D(1) of the *Civil Liability Act 2002* (NSW), a test for determination that negligence has caused a particular harm comprises two elements, namely 'factual causation' and 'scope of liability'. Cited in Stewart and Stuhmcke, this provision is mirrored in other Australian civil liability reform legislation. The relevant section in regard to a determination of causation states:⁹⁸¹

- (a) that the negligence was a necessary condition of the occurrence of the harm ("factual causation"), and
- (b) that it is appropriate for the scope of the negligent person's liability to extend to the harm so caused ("scope of liability").⁹⁸²

The plaintiff's harm/loss actually can be caused by so many factors. These factors could combine to produce a particular outcome. From these many possibilities, it is the task of the law to extract one or more circumstances to identify which events or factors are 'necessary conditions' of the loss, hence giving rise to liability, that is, a factor without which the loss would not have occurred (*cause sine qua non*).⁹⁸³ Fuady argues that it must be determined whether the factor that is alleged to be the cause of the damage is proximate (and therefore applicable) or too remote for consideration.⁹⁸⁴

The issue of 'remoteness' also occurs in causation and the possibility of damages. In general, the basic principle is that damages cannot be recovered if a defendant's careless act that caused the damage is considered to be too remote (beyond the scope of liability).⁹⁸⁵ Again, the question of remoteness is to be determined by judge in resolving the foreseeability test — there has to be a real (not fanciful) risk where the reasonable person could foresee the damage occurring from the action/omission.⁹⁸⁶

⁹⁸⁰ Stewart and Stuhmcke, above n 912, 190.

⁹⁸¹ For the meaning of harm, see *Civil Liability Act 2002* (NSW) s 5: "Harm" means harm of any kind, including the following: (a) personal injury or death; (b) damage to property; (c) economic loss.'

⁹⁸² Ibid s 5D(1). Other similar legislation includes: *Civil Liability Act 2003* (Queensland), *Civil Liability Act 2002* (Tas), *Civil Liability Act 2002* (WA), *Civil Law (Wrongs) Act 2002* (ACT).

⁹⁸³ Stewart and Stuhmcke, above n 912, 192.

⁹⁸⁴ Fuady, 'Perbuatan Melawan Hukum' above n 914, 103.

⁹⁸⁵ Gibson and Fraser, above n 917, 110.

⁹⁸⁶ Ibid 107. See *Overseas Tankship (UK) Ltd v Morts Dock & Engineering Co* (1961) AC 388. See also *Overseas Tankship (UK) Ltd v Miller Steamship Co. Pty* (1967) AC 617 (PC).

6.3.1.4. Damages

In regard to consumer protection, all consumer protection guidelines enacted by international organisations (such as United Nations, organisation for economic co-operation and development (OECD), Consumers International (CI) and so on) concur that one of the most important provisions that should exist in ‘a country’s consumer protection law is the availability of effective consumer redress for loss or damage sustained by consumers’ when such loss or damage is caused by the business actors’ products or services.⁹⁸⁷

Therefore, in a consumer’s claim in legal proceedings concerning a dispute between consumer and business actor, damage generally will be constructed as an actual damage or loss suffered by the plaintiff because the defendant has been in breach of his/her duty of care in the form of failure to conform with the standard of care that a reasonable person would exercise.

In the civil law, the award of damages is intended to compensate the plaintiff for the loss and/or damage caused by the defendant. In order to be successful in recovering their damage, the plaintiff should prove causation between the defendant’s breach and the loss or damage sustained by the plaintiff, and that such loss or damage is not too remote from the breach.⁹⁸⁸ However, the amount claimed by the plaintiff may not be awarded; the final amount that the defendant must pay to the plaintiff will be determined by whether or not causation is clearly demonstrated and whether or not the defendant has any valid defences that they can submit in order to dilute or even eliminate the plaintiff’s claim.

In Indonesia, the concept of damages is well accepted in the practice of law, and can be derived from breach of contract⁹⁸⁹ or because of a statutory provision, including due to unlawful act (tort as governed by Article 1365 of Indonesia’s Civil Code) that caused economic loss to consumers because the consumers’ consumption or use of the business actors’ goods or services.⁹⁹⁰ Where a plaintiff files a lawsuit based on tort (Article 1365 of Indonesia’s Civil Code), Setiawan asserts that generally consumers could claim

⁹⁸⁷ See above n 920.

⁹⁸⁸ Gibson and Fraser, above n 917, 107.

⁹⁸⁹ The damages that derive from breach of contract will not be discussed in this thesis.

⁹⁹⁰ Fuady, ‘*Perbuatan Melawan Hukum*’, above n 914, 134. See LCP 1999 art 19(1). See also Sidabalok, above n 792, 145–7, 156–7; Makarim, above n 857, 165.

several types of restitution, including: (1) damages in the form of cash for pure economic loss; (2) damages in the form of non-cash or restoration (for example, of premises) to its original state; (3) a statement that the act conducted was an unlawful act/tort; or (4) the prohibition of certain acts.⁹⁹¹ The damages themselves can be divided into three categories, namely: (1) nominal damages; (2) compensatory/actual damages; and (3) punitive damages,⁹⁹² which include material and/or immaterial damage.⁹⁹³ In Indonesia's Civil Code, the general provision for the type of damages are governed by Articles 1243–1252 (more in relation to the contractual default), which include several types of damages as follow: (1) costs (expenses actually incurred and become the burden of plaintiff); (2) damages sustained as a direct and immediate result of the default; (3) loss of potential profit due the default; and (4) statutory interest of 6 per cent annually as of the date the lawsuit is submitted. Even though this provision is not directly related to the damages in the field of tort, however, by analogical interpretation — this provision is deemed applicable to the tort situation (Article 1365 of Indonesia's Civil Code), or even in the situation of a violation of consumer protection legislation.⁹⁹⁴ In the determination of damages, as long as the amount is not specified in the regulation, a judge has the freedom to define the sum of damages based on their opinion of the merits of the case.⁹⁹⁵

6.3.2. Defences in Tort of Negligence

Generally, the plaintiff can only claim damage if the defendant is proved to be at fault and there is no defence accepted by the court. The most common defences in the civil

⁹⁹¹ Setiawan, '*Tinjauan Elementer Perbuatan Melawan Hukum*', above n 939, 39.

⁹⁹² Fuady, '*Perbuatan Melawan Hukum*', above n 914, 134–5, 142–5. Nominal damages are awarded to the victim even though there was not actual loss or injured incurred. Judges can determine a sum of money based on fairness or sense of justice to the victim. Compensatory damages are a compensation payment to the victim for damages that actually incurred and suffered by the victim due to the existence of an unlawful act. This includes compensation for various losses arising due to the mental distress caused by the unlawful act. Punitive damages may be awarded to punish parties for intentional or excessive unlawful act. Hence, damages for the lattermost normally amount to a sum that is greater than the actual loss suffered by the victim.

⁹⁹³ Ibid 142–3. Immaterial damages normally could not be gauged by using normal mathematical calculations, since they are based on the judge's wisdom and on reasonableness. For reasonableness, it will depend on the victim's specific situation such as natural condition of premise and atmosphere of tort, background of tort, type of tort (gross or ordinary negligence) and so on. See also Makarim, above n 857, 176.

⁹⁹⁴ Sidabalok, above n 792, 160–1. See also Makarim, above n 857, 175–6; Setiawan, '*Tinjauan Elementer Perbuatan Melawan Hukum*', above n 939, 28–32.

⁹⁹⁵ See Sidabalok, above n 792, 157–9.

liability claim are contributory negligence, comparative negligence, and assumption of risk.⁹⁹⁶

6.3.2.1. Pure Contributory Negligence

Pure contributory negligence is probably one of the most common defences raised by the defendant to address claims for damages by a plaintiff.⁹⁹⁷ If the defendant pleads this defence, then the onus of proof lies with them to show that the plaintiff has demonstrated pure contributory negligence that has enabled the damage to occur.⁹⁹⁸

According to *Black's Law Dictionary*, contributory negligence is: 'a plaintiff's own negligence that played a part in causing the plaintiff's injury and that is significant enough (in a few jurisdictions) to bar the plaintiff from recovering damages'.⁹⁹⁹ Originally, the pure contributory negligence doctrine was 'the principle that completely bars a plaintiff's recovery [of damages] if the damage suffered is partly the plaintiff's own fault'.¹⁰⁰⁰ Hence, in former times in common law countries, pure contributory negligence acted as a complete defence.¹⁰⁰¹ In order to use this doctrine, the plaintiff or victim of an unlawful act could not contribute in any way to the occurrence of damages (the 'clean hands' doctrine). Therefore, in pure contributory negligence, the redress principle was an 'all or nothing' approach.¹⁰⁰² However, pure contributory negligence not only applied to the brick-and-mortar world, but also to transactions in cyber-world. For instance, an on-line commerce provider could defend against a claim for Internet security issues on the grounds that plaintiff also contributed for the damaged by losing their password.¹⁰⁰³ An early United Kingdom (UK) example of this doctrine can be seen

⁹⁹⁶ Fuady, 'Perbuatan Melawan Hukum', above n 914, 3. See also Gibson and Fraser, above n 917, 79–81; John W Bagby, 'Cyberlaw Handbook for E-Commerce' in Makarim, above n 857, 180.

⁹⁹⁷ Stewart and Stuhmcke, above n 912, 242–3.

⁹⁹⁸ Gibson and Fraser, above n 917, 111.

⁹⁹⁹ Garner, above n 797, 1134.

¹⁰⁰⁰ Stewart and Stuhmcke, above n 912, 243.

¹⁰⁰¹ e-lawresources.co.uk, *Contributory Negligence* (e-lawresources.co.uk <<http://www.e-lawresources.co.uk/Contributory-negligence.php>>; Stewart and Stuhmcke, above n 912, 244.

¹⁰⁰² See Fuady, 'Perbuatan Melawan Hukum', above n 914, 79–80. See also Gibson and Fraser, above n 917, 79–80. *Butterfield v Forrester* (1809) 103 ER 926: The plaintiff was riding his horse very fast. The pole was visible from a long distance away and the plaintiff, through his own failure to take care, was held responsible for the accident.

¹⁰⁰³ Rustad and Daftary, above n 958, 308.

in *Butterfield v Forrester* (1809) 103 ER 926.¹⁰⁰⁴ It should be noted that today such a doctrine is not universally applied in common law countries.

Stewart and Stuhmcke argue that the doctrine of pure contributory negligence only created unfairness especially for the plaintiff by failing to recognise the different level of the degree of fault between the parties involved: '[t]he unfairness of this rule operating as a complete defence was that a plaintiff who had been even slightly careless would be completely prevented from recovering any damages as the result of an injury caused mainly by the defendant's negligence'.¹⁰⁰⁵

6.3.2.2. Comparative Negligence

According to *Black's Law Dictionary*, comparative negligence is 'a plaintiff's own negligence that proportionally reduces the damages recoverable from a defendant.'¹⁰⁰⁶ Therefore, the comparative negligence doctrine is 'the principle that reduces a plaintiff's recovery proportionally to the plaintiff's degree of fault in causing the damage, rather than barring recovery completely.'¹⁰⁰⁷ Hence, the degree of negligence of the defendant is compared to that of the plaintiff.¹⁰⁰⁸

Comparative negligence is a doctrine that arose as a reaction to 'unfairness' found in the application of the doctrine of pure contributory negligence.¹⁰⁰⁹ As a consequence, several common law countries have abolished pure contributory negligence and have superseded it by statute and adopted the 'comparative negligence' doctrine.¹⁰¹⁰ This statute rule, instead of common law, is generally known as 'apportionment legislation'. Apportionment legislation was introduced in England and its introduction has been followed in Australia to enable damage to be apportioned in a more just and equitable

¹⁰⁰⁴ See Fuady, 'Perbuatan Melawan Hukum', above n 914, 3. See also Gibson and Fraser, above n 917, 79–80. *Butterfield v Forrester* (1809) 103 ER 926: In this case, a plaintiff failed to redeem damages from a defendant where a plaintiff demonstrated contributory negligence when he rode his horse into a pole which the defendant had wrongly placed across the highway, despite the pole being visible from a distance. Indeed the plaintiff have shown a 'slight' carelessness when he rode the horse too fast. Meanwhile, the defendant apparently had greater fault when he wrongly placed the pole across the highway. Even though the plaintiff had shown negligence, the accident would never have occurred if the defendant had not wrongly placed the pole on the highway.

¹⁰⁰⁵ Stewart and Stuhmcke, above n 912, 244.

¹⁰⁰⁶ Garner, above n 797, 1056.

¹⁰⁰⁷ Ibid 1134.

¹⁰⁰⁸ Rustad and Daftary, above n 958, 398. See also Fuady, 'Perbuatan Melawan Hukum', above n 914, 80–1.

¹⁰⁰⁹ See Fuady, 'Perbuatan Melawan Hukum', above n 914, 80. See also Gibson and Fraser, above n 917, 79–80. *Butterfield v Forrester* (1809) 103 ER 926.

¹⁰¹⁰ See *Wynbergen v Hoyts Corporation Pty Ltd* (1997) 149 ALR 25.

way between the plaintiff and defendant. According to Stewart and Stuhmcke, the aim of apportionment legislation is ‘to adjust compensation according to degrees of fault’; they add that it now operates in cases of contributory negligence to reduce the amount of damages awarded to a plaintiff ‘to the extent that the plaintiff’s carelessness contributed to the damaged suffered.’¹⁰¹¹ The *Civil Liability Act 2002* (NSW) is an instance of apportionment legislation pertaining to pure contributory negligence.¹⁰¹² In England, the *Law Reform (Contributory Negligence) Act 1945* (UK) is an instance of reform involving the comparative negligence doctrine, where judges apportion liability (and hence damages) according to the degree of culpability of the tortfeasor and plaintiff for the injury/damage sustained by the latter.¹⁰¹³

Nowadays, pure contributory negligence still survives in some jurisdictions; however, for countries that have already reformed their liability law, contributory negligence (of the plaintiff) will be treated as ‘comparative negligence’ and no longer constitute a complete defence. Thus, if a defendant’s defence of plaintiff contributory negligence is accepted by the court, the plaintiff’s damages may be reduced according to the degree of negligence of the plaintiff. For instance, if the plaintiff is deemed 20 per cent responsible for the event that caused the damage, then the defendant will only be responsible for 80 per cent of the plaintiff’s damages.

¹⁰¹¹ Stewart and Stuhmcke, above n 912, 246–50.

¹⁰¹² Ibid 254; *Civil Liability Act 2002* (NSW). However, instead of using comparative negligence, the term used in the legislation is still ‘contributory negligence’ with a ‘new’ definition that is closer in meaning to that of ‘comparative negligence’. See *Civil Liability Act 2002* (NSW) s 5R:

(1) The principles that are applicable in determining whether a person has been negligent also apply in determining whether the person who suffered harm has been contributory negligent in failing to take precautions against the risk of that harm.

(2) For that purpose:

(a) the standard of care required of the person who suffered harm is that of a reasonable person in the position of that person, and

(b) the matter is to be determined on the basis of what that person knew or ought to have known at the time.

¹⁰¹³ Stewart and Stuhmcke, above n 912, 246–7. See *UK Law Reform (Contributory Negligence) Act 1945* (UK) s 1(1):

Where any person suffers damage as the result partly of his own fault and partly of the fault of any other persons, a claim in respect of that damage shall not be defeated by reason of the fault of the person suffering the damage, but the damages recoverable in respect thereof shall be reduced to such extent as the court thinks just and equitable having regard to the claimant’s share in the responsibility for the damage.

See also 5S of the *Civil Liability Act 2002* (Contributory negligence can defeat claim):

In determining the extent of a reduction in damages by reason of contributory negligence, a court may determine a reduction of 100% if the court thinks it just and equitable to do so, with the result that the claim for damages is defeated.

Apportioning damages in percentage terms between the plaintiff and the defendant in real cases is not an easy task for the courts. Basically, the courts have to compare the negligence of the plaintiff and that of the defendant, and transform it into a percentage. Hence, in the apportionment of fault, ‘the damages will be reduced to an amount which the court considers to be fair having regard to the extent of the plaintiff’s responsibility for the damage’.¹⁰¹⁴ However, each court might have different opinion regarding the degree of fault attributable to the plaintiff and the defendant.¹⁰¹⁵ As evidence of this, in *Pennington v Norris* (1956) 96 CLR 10, the trial judge reduced the plaintiff’s damages by 50 per cent for contributory negligence, while the High Court judge argued that damages should only be reduced by 20 per cent.¹⁰¹⁶

Nevertheless, very valuable guidelines about how to gauge the parties’ responsibility for the damage can be distilled from the Tasmanian High Court decision in the *Pennington v Norris*, as follows:

The only guide which the statute provides is that it requires regard be had to “the claimant’s share in the responsibility for the damage” ... What has to be done is to arrive at a “just and equitable” apportionment as between the plaintiff and the defendant of the “responsibility” for the damage. It seems clear that this must of necessity involve a comparison of culpability. By “culpability” we do not mean moral blameworthiness but degree of departure from the standard of care of the reasonable man. To institute a comparison in respect of blameworthiness in such a case as the present seems more or less impracticable, because, while the defendant’s negligence is a breach of duty owed to other persons and therefore blameworthy, the plaintiff’s “contributory” negligence is not a breach of any duty at all, and it is difficult to impute moral blame to one who is careless merely of his own safety... Hence in our opinion, the negligence of the defendant was in a high degree more culpable, more gross, than that of the plaintiff. (at 16)¹⁰¹⁷

From the case above, we can conclude that unlike negligence that depends on a breach of duty to another, contributory negligence is only concerned with the failure of a person to take care of his or her own safety and interests. Therefore, in order to use contributory negligence as a defence in a tortious liability claim, the defendant is required to establish that:

¹⁰¹⁴ Stewart and Stuhmcke, above n 912, 246.

¹⁰¹⁵ See *Pennington v Norris* (1956) 96 CLR 10 where the plaintiff, a pedestrian, was struck by the defendant’s car while crossing a road at night in Tasmania.

¹⁰¹⁶ Stewart and Stuhmcke, above n 912, 247–8.

¹⁰¹⁷ See summary of the case in Stewart and Stuhmcke, above n 912, 247–8. See also judgment by Lord Danning in *Froom v Butcher* (1975) 3 All ER 520 at 523:

Negligence depends on a breach of duty, whereas contributory negligence does not. Negligence is a man’s carelessness in breach of duty to others. Contributory negligence is a man’s carelessness in looking after his own safety. He is guilty of contributory negligence if he ought reasonably to have foreseen that, if he did not act as a reasonable prudent man, he might hurt himself.

- (a) the plaintiff failed to take the precautions a reasonable person would have taken for their own protection (that is, the standard of care applicable to the plaintiff's act) and;
- (b) the damage was reasonably foreseeable (that the injury is within the risk) and was partly caused by the plaintiff's negligent act.¹⁰¹⁸

In most states of Australia, a finding of contributory negligence by the court will focus on only the plaintiff's conduct according to the standard of what a reasonable person would have done in the same situation. Regarding the plaintiff's standard of care, the statutory standard of care in Australia is that which is stated, for example, in section 5R(2) of the *Civil Liability Act 2002* (NSW): 'the matter is to be determined on the basis of what that person knew or ought to have known at the time'.¹⁰¹⁹ Thus, common knowledge by a reasonable person in the same circumstances is a benchmark to be tested by the court.

As in pure contributory negligence so in modified contributory negligence or comparative negligence, the onus of proof rests with the defendant who pleaded this defence in order to defend him/herself against a claim from the plaintiff over damages. If the defendant is successful in proving their defence, there will be a reduction in damages to be paid to the plaintiff, based on the comparison of the plaintiff's degree of lack of standard of care that a reasonable person would observe in the plaintiff's position, 'and the matter will be decided on the basis of what the person knew or ought to have known at the time'.¹⁰²⁰ The standard of care test that the defendant must pass to evade claims of contributory negligence/comparative negligence is basically similar to the standard of care that is owed by the defendant to the plaintiff. In relation to the amount of the reduction, Gibson and Fraser state that, 'the reduction is calculated on the basis of the damages that would have been awarded to the plaintiff if there had been no fault on their part, and then reduced by the percentage of their negligence.'¹⁰²¹

In Indonesia, Article 1365 of Indonesia's Civil Code obliges the tortfeasor/defendant to redress the damage to the victim/plaintiff in full; however, if the loss incurred is attributed to the tortfeasor and also to the victim's own fault/negligence (joint fault/negligence), then the tortfeasor need only to pay partial compensation. In other words, the victim in such circumstances should also bear part of the damages suffered.

¹⁰¹⁸ Stewart and Stuhmcke, above n 912, 252–3.

¹⁰¹⁹ This provision is duplicated in *Civil Liability Act 2003* (Qld) s 23; *Civil Liability Act 2002* (Tas) s 23; *Wrongs Act 1958* (Vic) s 26; *Civil Liability Act 2002* (WA) s 5K.

¹⁰²⁰ Gibson and Fraser, above n 917, 112.

¹⁰²¹ Ibid 111–12.

This condition has existed in the Netherlands since 1916 and is acknowledged in Dutch case law.¹⁰²² In general, plaintiff fault or negligence will reduce the liability of the defendant. Both plaintiff and defendant should bear the damages based on their degree of fault/negligence.¹⁰²³ The division of liabilities between plaintiff and defendant is known in the civil law, and also in tort under customary law (as can be seen from Indonesia's Supreme Court Verdict on 10 January 1957 No 206 K/Sip/1955).¹⁰²⁴

6.3.2.3. Voluntary Assumption of Risk

As explained above, the defendant may be able to avoid liability for the claim for damages from the plaintiff, if that defendant can raise a defence that the plaintiff has assumed and consented to the possibility of risk existing in their activities, and such a defence is accepted by the court. In *Scanlon v American Cigarette Company (Overseas) Pty Ltd* (No 3) [1987] VR 289, Nicholson J asserted that there are three elements that must be established in raising the defence of voluntary assumption of risk by the plaintiff. These elements are:

- precise knowledge of the risk by the plaintiff;
- understanding and appreciation of the risk by the plaintiff; and
- voluntary participation.¹⁰²⁵

With the development of civil liability reforms, defence using a voluntary assumption of risk generally can now be raised in regard to a general action (previously this defence typically was only used in sporting situations). The plaintiff will not recover any damages if the defendant successfully submits the defence of voluntary assumption of risk. However, this defence only can be raised if the plaintiff has obviously not paid attention to the obvious risk,¹⁰²⁶ and hence ignored their own safety, where another reasonable person in their position would have acted differently to avoid it.¹⁰²⁷ Therefore, the plaintiff cannot recover damages for harm, even if the defendant is at fault, if the plaintiff voluntarily assumes a known risk. For instance, if a web site warns

¹⁰²² See *Arrest Hoge Raad* dated 4 February 1976 in Setiawan, 'Tinjauan Elementer Perbuatan Melawan Hukum', above n 939, 17.

¹⁰²³ Ibid 37–9.

¹⁰²⁴ Ibid 38–9.

¹⁰²⁵ Gibson and Fraser, above n 917, 112–13.

¹⁰²⁶ See ibid 113. An obvious risk is 'a risk that, in the circumstances, would have been obvious to a reasonable person in the position of the defendant and includes risks that are patent or matters of common knowledge, risks that may have a low probability of occurring and risks that are not prominent, conspicuous or physically observable.'

¹⁰²⁷ Ibid.

the user that it does not in use the most current standard security software, a plaintiff may have voluntarily assumed a known risk.¹⁰²⁸

Nevertheless, using this defence in circumstances other than sporting or recreational activities might be difficult. A cause of difficulty in using such a defence is the problem of establishing whether 'the plaintiff had a precise knowledge of the risk, a full and free understanding and appreciation of the particular risk, and voluntarily accepted the risk.'¹⁰²⁹ In relation to the defence, a plaintiff is deemed to be aware of the risk if they are aware of the type or kind of risk in general (not necessarily to understand the risk in detail, such as knowing its precise nature, extent or manner of occurrence).

6.3.2.4. *Novus Actus Interveniens*: ('A New Intervening Act')

In a tortious liability case, especially in data security breaches such as happens in unauthorised ATM/debit card transactions, it is very common for the defendants to argue that their acts were not the cause of the plaintiff's loss because there was an event which intervened between the defendant's conduct and the plaintiff's harm, such as the intervening criminal acts of third parties who steal the consumer's data to commit identity theft and fraud.¹⁰³⁰

In this regard, a defendant usually asserts that the intervening incident might be said to be the 'real' cause of the plaintiff's loss. Hence, it is commonly argued that the later conduct severs or breaks the chain of causation between the defendant's negligence and the plaintiff's damage. This condition is sometimes dubbed a *novus actus interveniens*: a new intervening act. If the court finds that on the balance of the probabilities that an intervening act indeed severed the causal link to the accused, then the defendant's conduct would not be a cause of the loss and the defendant would not be liable for the damage.¹⁰³¹

The problem for the court in cases where an intervening act is said to exist is whether that intervening event is sufficient to break the chain of causation between the negligent act of the defendant and the plaintiff's loss. Several approaches have been acknowledged in determining whether a particular act can constitute an intervening act

¹⁰²⁸ Rustad and Daftary, above n 958, 398.

¹⁰²⁹ Gibson and Fraser, above n 917, 113.

¹⁰³⁰ See *Nasruddin v PT Bank Mandiri Tbk* case. See also Jennifer A Chandler, 'Negligence Liability for Breaches of Data Security' (2008) 23(2) *Banking and Finance Law Review* 263.

¹⁰³¹ Stewart and Stuhmcke, above n 912, 201–2.

that breaks the chain of causation between a defendant's act and the plaintiff's loss. These include voluntary acts, the 'very risk' created by the defendant, and coincidence:

(1) voluntary acts:

Smith J in the *Haber v Walker* (1963) VR 339 stated that:

[T]he intervening occurrence, if it is to be sufficient to sever the connection, must ordinarily be either:

(a) human action that is properly to be regarded as voluntary; or

(b) a causality independent event the conjunction of which with the wrongful act or omission is by ordinary standards so extremely unlikely as to be termed a coincidence.¹⁰³²

Hence defendants can basically escape liability if they can prove that a voluntary act of the plaintiff was actually the main cause of the damage sustained by the plaintiff, and so severed the causal link between defendant's negligence and the plaintiff's loss. If this cannot be demonstrated, liability remains.

(2) The 'very risk' created by the defendant:

Pertaining to *novus actus interveniens*, Stewart and Stuhmcke noted that '[i]n some circumstances, it may be that such an action is the very thing against which a defendant has a duty of care to protect the plaintiff's loss notwithstanding a subsequent act'.¹⁰³³ In many cases where the defendant owed a duty of care to the plaintiff and the risk can be categorised as 'reasonable foreseeable', the second act or event that occurs and is claimed by the defendant to be the 'real' cause of the plaintiff's loss and thus is used by the defendant as the intervening act to escape liabilities, such a claim is mostly rejected by the courts on the basis that the causal link persists and the damage or harm sustained by the plaintiff was actually facilitated by the negligence of the defendant. Hence, it cannot break the chain of causation as can be seen from various judgments in cases such as *Chomentoski v Red Garter Restaurant* (1970) 92 WN (NSW) 1070, *March v Stramare* (1991) 171 CLR 506, and *Medlin v SGIC* (1995) 182 CLR 1.¹⁰³⁴

¹⁰³² Ibid 203–4. See also Fuady, 'Perbuatan Melawan Hukum', above n 914, 124–5. Stewart and Stuhmcke note the facts pertaining to a 'voluntary act' in *Haber v Walker*:

the plaintiff's husband had been very severely injured in a car accident which led to a serious depressive illness and eventual suicide. The defendant negligent driver argued that, as the deceased had voluntarily taken his own life, that act severed the causal link between the defendant's negligence and the death of the deceased. The Victorian Court of Appeal found that the conduct of the deceased was not really a voluntary act as it was the result of the severe depressive illness caused by the defendant's negligence. Therefore, the causal link was not broken and the defendant was liable for the death.

¹⁰³³ Stewart and Stuhmcke, above n 912, 192.

¹⁰³⁴ Fuady, 'Perbuatan Melawan Hukum', above n 914, 125. See also Stewart and Stuhmcke, above n 912, 192.

(3) Coincidence:

A coincidence is a circumstance where the defendant can build a defence against a damage claim by the plaintiff by using *novus actus interveniens*, where the condition that causes a plaintiff's loss was actually a fortuitous event which is causally unrelated to the act of the defendant. Stewart and Stuhmcke summarise the judgments in cases such as *March v Stramare* (1991) 171 CLR 506 at 516 and *Canterbury Bankstown RLFC Ltd v Rogers* (1993) Aust Torts Reports ¶81–246, observing that:

A tortfeasor will not be liable where injury is caused by a coincidence, even where the tortfeasor's actions might have resulted in the plaintiff being in the place at the time when the coincidence occurs, so long as the risk to the plaintiff has not been increased by the actions of the tortfeasor.¹⁰³⁵

In Indonesia, Fuady states that in general in cases where it can be proven that there is no 'reasonable foreseeability', the intervening act will be deemed a 'superseding cause'. Consequently, the defendant's act will not be treated as the necessary proximate cause for the damage that occurred, and the defendant will not be liable for damages (that is, the relationship between the damage to the plaintiff and the defendant's act is too remote as it was 'unforeseeable' and so no risk prevention could have been adopted by the defendant in relation to such risk). However a defendant will not be liable for the damages, if the victim also contributed to the occurrence of damages, such as when the victim does nothing to prevent losses.¹⁰³⁶ In other words, in cases where the defendant owes a duty of care to the plaintiff and the risk can be categorised as one of 'reasonable foreseeability', the *novus actus interveniens* that occurs and becomes the 'real' cause of the plaintiff's loss will render the defendant liable for damages to the plaintiff (with restitution in the form of monetary compensation as the most likely outcome, as indicated earlier).

Nevertheless, in the area of e-banking in Indonesia, legislation invalidates the *novus actus interveniens* principle. Its invalidation in Indonesia can be seen from (among

¹⁰³⁵ Stewart and Stuhmcke, above n 912, 206. In *March v Stramare*, Mason CJ said that 'a factor which secures the presence of the plaintiff at the place where and at the time when he or she is injured is not causally connected with the injury, unless the risk of the accident occurring at that time was greater.' While in *Canterbury Bankstown RLFC Ltd v Rogers*:

the plaintiff had suffered an injury to his jaw as a result of a battery by the defendant's player. The plaintiff, having recovered from his injury, went to England to recover his match fitness. Whilst playing in England, he suffered an injury to his leg. The plaintiff would not have been in England had it not been for the tort of the defendant but that was not sufficient to establish a causal link between the defendant's tort and the subsequent injury. The subsequent injury was a coincidence and therefore a *novus actus interveniens*. The defendant was not liable for that injury.

¹⁰³⁶ Fuady, 'Perbuatan Melawan Hukum', above n 914, 124–6.

others) Article 21(3) of *LIET*, which states that: ‘if the damage [to] electronic transactions occurred because of the failure of an electronic agent due to the direct acts by third party/ies against the electronic system, then all legal consequences will be the liability of the provider or owner of an electronic agent.’ This creates a statutory ‘proximity’ for the ‘provider or owner of the electronic agent’ that is not broken by the ‘intervening acts’ of third parties and thus appears to eliminate any defence based on such ‘new intervening acts’ that may be perpetrated by fraudsters. However, as Article 21(4) of *LIET* makes clear, such liability is void ‘if damage [to] electronic transactions is occasioned by failure of the operation of the electronic agent due to negligence of service users’; in such instances ‘any legal consequences shall become the responsibility of the service users.’

6.4. Consumer Protection for Unauthorised ATM/Debit Card Transactions: Concept and Practice of Dispute Resolution and Redress in Indonesia

6.4.1. Unauthorised ATM/Debit Card Transaction: Consumer as a True Victim

Typically, payment fraud (such as unauthorised payment card transactions) will cause losses of actual consumers’ funds in their banks.¹⁰³⁷ For consumers, besides the direct financial cost (the defrauded amount that is not reimbursed by banks), they also suffer indirect financial costs or consumer costs (the out-of-pocket costs or lost wages) incurred by the victim in order to resolve a fraud case, such as postage, copying, notarising documents, and legal fees associated with investigation and prosecution. These costs may also include the expense generated by any fraudulent debts, with such expenses including interest on loans, credit cards and so on, paid in order to avoid further problems.¹⁰³⁸ Some consumers also suffer from privacy infringement,¹⁰³⁹ mental distress, trauma and frustration regarding uncertain situations related to whether or not their money will be reimbursed by the card issuer bank. An example of the experiences (including economic and psychological damages and stresses) of a victim comes from

¹⁰³⁷ See UNCITRAL, ‘UNCITRAL Legal Guide on Electronic Funds Transfers’, above n 189, 48; Rusch, above n 106, 561. See also Roberds, above n 265, 42; Sullivan, ‘The Changing Nature of US Card Payment Fraud’, above n 262, 103.

¹⁰³⁸ Javelin Strategy & Research, ‘2010 LexisNexis True Cost of Fraud Study’, above n 334, 10.

¹⁰³⁹ Malphrus, above n 338, 35.

Mr Panggabean, a 55 year old public high school teacher and the victim of an ATM card-trapping fraud.¹⁰⁴⁰

The Example of Mr Panggabean Case:

On 19 May 2012, Mr Panggabean conducted an ATM transaction at a Bank DKI ATM booth in Cibubur Square Mall. Instead of the normal transaction occurring, his ATM card became stuck inside the ATM slot. Panicking because he had never had such an experience, he followed the suggestion of a ‘good Samaritan’ who had stepped into the booth and suggested to him that he call the Bank DKI call centre number as shown on the sticker attached to the body of the Bank DKI ATM, in order to get help and overcome the problem (the sticker was fake but had been made with such precision as to make it indistinguishable from the genuine one). The ‘call centre officer’ — who was actually one of the ‘con artists’ in this fraud — then pretended to help and asked him to make several attempts to retrieve the card from the ATM, such as by pressing some combinations of the buttons on the ATM keyboard. However, none of the attempts succeeded. The ‘officer’ then asked him to verify his identity by supplying his name, PIN, date of birth and so on in order to cancel the card and issue the new one. Because of the stressful situation and believing that he was speaking with an authorised bank officer, he then revealed all the information demanded and left the ATM, believing the bank would be securing his card. Something that Mr Panggabean didn’t know was (because, as he later argued, he had never had consumer education about ATM risk from his bank) that the ‘good Samaritan’ was actually a con artist and the call centre was actually fake.

Soon after Mr Panggabean left the ATM, the fraudster pulled out the consumer’s ATM card using special devices (such as metal clip or customised screwdriver) and withdrew Mr Panggabean’s money using the correct consumer PIN. As result, all Mr Panggabean’s money —as much as IDR45,698,000 or around AUD4500 — was drained from his account. Sadly, this was not the end of his misery. Instead, this was just the beginning of his ordeal.

Following the loss, he wrote of his experience to more than 10 newspapers and magazines, asking for help since Bank DKI itself refused to recognise any liability as he had willingly supplied his information and the correct PIN and number had been used in the transaction. After his demand for the bank to reimburse his loss was rejected by the bank, he then approached mediation for his loss at the Banking Mediation Agency in Bank Indonesia (the central bank of the Republic of Indonesia) on November 2012.

Unfortunately, after several meetings, by December 2012 no agreement had been concluded and the bank still refused to be liable on the ground that the loss was due to Mr Panggabean’s own mistake in revealing his PIN (the bank blamed the perpetrators for their success in attaching card-trapping device and fake call centre number to the bank’s ATM booth, and did not perceive this situation as at all due to any negligence on

¹⁰⁴⁰ Interviews with Mr Samuel Panggabean, a 55 year old public high school teacher and the victim of an ATM card-trapping fraud (Jakarta, 2 August 2012) revealed how poor the condition of the ATM fraud victim is, both economically and psychologically. For an instance of his writing to media, see *Waspada Kejahatan di ATM [Beware on Crime at the ATM]* (15 July 2012) *Harian Terbit* <<http://www.harianterbit.com/2012/07/15/waspada-kejahatan-di-atm/>>.

the bank's part). Moreover, the bank also requested that Mr Panggabean pay the monthly instalment and interest on the loan from which he would never benefit.

As a result of the fraud, Mr Panggabean's son failed to continue his university studies and Mr Panggabean spent most of his free time (including weekends) giving tutorials for extra cash to compensate for his loss. Sad, frustrated, angry, regretful and mentally distressed are just some of words that can now give some semblance of his condition.

The only hope and avenue left now is to launch a civil suit in the court or go to the Consumer Disputes Resolution Body. But the very negative stigma of court proceedings (which often involve many 'phantom' expenses, the lack of knowledge on the part of judges about e-banking transactions, and the prolonged trial process from District Court, High Court and Supreme Court (a process that may take years) combined with a great uncertainty as to the result (on top of the costs involved), the court process is deemed a difficult (if not altogether impossible) option for Mr Panggabean.

His is by no means a unique experience for, as described in the background to this study given in the Chapter 1, in Indonesia many unauthorised ATM/Debit transactions that have caused money to be lost from consumer bank accounts ended up with banks refusing to redeem the money. The most common defence supplied by the banks is either that the alleged transactions are deemed valid due to the use of the correct card number and PIN or to some extent the consumers have been deemed to have been negligent and so enabled fraudsters to carry out unauthorised ATM/Debit card transactions.

As a consequence of weak consumer protection in Indonesia, the loss of customers' money from their banks due to fraud can create a severe crisis. The loss of money for some consumers who have been unable to obtain remedies from their banks not only creates harsh economic hardship, but also varying degrees of psychological distress (such as frustration, sadness, loss of hope, depression, and indeed, mental distress). However, fraud not only affects individual consumer victims (and their immediate families) monetarily but also alters their perceptions and behaviours (consumer confidence) which can have a significant impact on the issuer bank and retail merchant, particularly if this experience — or knowledge of such experiences — becomes widespread.¹⁰⁴¹

¹⁰⁴¹ Javelin Strategy & Research, '2010 LexisNexis True Cost of Fraud Study', above n 334, 11, 20. According to the results of this study, fraud victims demonstrate a mixture of both positive and fear-driven reactions as a result of their experience. Approximately 36% of victims report the intent to avoid certain merchants; 17% will change financial institutions (both issuers and primary banks). There is also non quantifiable loss because of customer attrition resulting from frustration with the fraud resolution process; 27% report they will spend less money; and 31% will switch payment methods. See also Diebold

Levi and Burrows argue that consumers and other individuals ('public at large') are 'ultimately the victims of most fraud, as they generally bear the costs of fraud through higher insurance premiums, reduced dividends or pensions, higher credit card fees or interest rates, higher fees for banking services, higher taxes, and so on (including psychiatric services and redundancies)'.¹⁰⁴²

Consumer protection issues in Indonesia are 'an iceberg above the sea phenomenon', that is, there are far more problems than are easily visible. Many parties, including consumers believe that there are issues regarding consumer protection in Indonesia; however, data on the number of consumers that experience pure economic loss in the use of a bank's particular products and/or services are scarce and incomplete. To this day, Indonesia does not have a data centre that actively records and stores consumer protection related cases. Many consumers who have lost money from their bank accounts prefer to be silent rather than complain to the relevant consumer organisations. This is worsened by the prevalent cultural Indonesian behavioural norm that values avoiding an open conflict, especially with one who is deemed superior in most aspects.¹⁰⁴³ Some consumers also treat a loss as a 'divine will', and hence they must bear it.

These facts are consistent with the results of research by the Indonesian National Law Development Agency (BPHN), which concluded that the majority of Indonesian people keep silent about an instance of a loss that they have experienced. They are reluctant to file a claim for compensation and report the complaint to the competent bodies. This reaction is variously motivated. The predominant reasons are that the victim consumers: (1) do not want a legal 'hassle'; (2) worry that the situation might be exacerbated if they make a complaint; (3) do not want to be involved with the police (because of the inherent stigma attached to Indonesia's police department); (4) do not know exactly where to complain about the incident and are afraid of the cost of making and processing the complaint; and (5) are pessimistic regarding whether the reported incident will be addressed properly or even that the report itself will receive any

Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 2; Hendry, above n 203, 22; Smart Card Alliance, 'Fraud in the US Payments Industry', above n 297, 5.

¹⁰⁴² Michael Levi and John Burrows, 'Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey' (2008) 48(3) *British Journal of Criminology* 293, 301–2.

¹⁰⁴³ NHT Siahaan, *Hukum Konsumen: Perlindungan Konsumen dan Tanggung Jawab Produk* [Consumer Law: Consumer Protection and Product Liability] (Panta Rei, 2005) 8.

attention.¹⁰⁴⁴ This acts in the banks' rather than the victim consumers' favour — at least in the short term in the matter of possible litigation, but is not in the long term interests of either consumers or banks.

Siahaan contends that, in fact, the lack of consumers' reports concerning their losses when consuming or using products or services from its producer (the card issuer in regard of card payment transaction) not only will be to the detriment of the rights of those consumers themselves, but also to all other relevant stakeholders. The absence of actual consumer complaints is detrimental to all parties for a number of reasons. Businesses or government authorities will not be aware of the issues regarding the problems of consumer protection when no complaints filed. The absence of consumer complaint data 'sends the wrong signal' to card issuers because they feel that there is nothing wrong with their goods or services. That same absence of consumer complaints has led not only to a lack of awareness on the part of the government in regard to the existence of problems, but consequently an inability to seek and then impose appropriate solutions. In relation to consumers themselves, any losses incurred will not be recovered if the losses are never reported and/or claims made to the court or dispute resolution body that the business actors responsible for the losses should make restitution for those losses.¹⁰⁴⁵ Given their international experience, however, it could be argued that larger businesses, major banks and government should be somewhat aware of potential problems, even with the lack of consumer reports.

6.4.2. Consumer Protection in ATM/Debit Card Transactions

In general, consumers are in a weak position compared to banks as producers of banking products and/or services.¹⁰⁴⁶ Huzna Zahir (former chief of the Indonesian Consumer Protection Agency) contends that many fraudsters are taking advantage of inherent weaknesses in the banking system and its infrastructures. She further argues that theft of a consumer's funds from their bank accounts through ATM/debit card fraud basically can be considered as violating the consumer's right to security (and privacy of

¹⁰⁴⁴ Badan Pembinaan Hukum Nasional, '*Laporan Akhir Penelitian Perlindungan Konsumen Atas Kelalaian Produsen* [Research Final Report on Consumer Protection over Producer Negligence]' (Departemen Kehakiman, 1992) 82.

¹⁰⁴⁵ Siahaan, above n 1043, 8.

¹⁰⁴⁶ Kristiyanti, above n 928.

transactions) as well as reducing the convenience of utilising the banking products and services.¹⁰⁴⁷

Beside the classic asymmetry problems concerning information about bank products and services,¹⁰⁴⁸ the absence of information about the inherent risks for consumers is probably one of the biggest issues in this regard in the banking industry. Hence, it is not surprising that Muliaman Hadad (former Bank Indonesia Deputy Governor) urges banks to educate their consumers, especially regarding payment card transactions. He further argues that good consumer education could reduce the possibility of disputes caused by the consumer's lack of understanding of fraud risk and the methods used to perpetrate such fraud.¹⁰⁴⁹ Such education is, therefore, in the interests of the bank as well as the consumers, by reducing consumer's unwitting 'cooperation' in their exposure to fraud. Its prevention through increased consumer education benefits both bank and consumer.

Disturbingly, many consumers are also unaware of their rights as consumers.¹⁰⁵⁰ Hence, most of the time, they have become objects of business activities undertaken by the business actors in pursuit of profit. Business actors (that is, businesses, including banks) typically attempt to optimise their profit through by (either or both) increasing sales and decreasing costs so as to maximise shareholder or business owner returns. In a bid to increase sales, business actors may employ advertising and other promotional activities, and various sales methods; while in a bid to decrease costs, necessary but expensive updates or repairs may be delayed or blame-shifting occur, and standard agreements/contracts be adopted. The agreements may indeed be designed to place consumers at a disadvantage compared to the business actor whose interests the contract will seek to protect.¹⁰⁵¹ The common general principle for business actors everywhere is to make the ultimate profit with the minimum capital. It is also most likely that this principle will jeopardise consumer rights, either directly or indirectly.¹⁰⁵²

It has been shown that in the complex environment of the financial sector, banking consumers are particularly vulnerable to identity theft and identity fraud related to bank

¹⁰⁴⁷ Lema, above n 120.

¹⁰⁴⁸ See Kristiyanti, above n 928, 26.

¹⁰⁴⁹ Fitri Novia Heriani, *BI Fokus Mediasi Kasus Perbankan* [BI Focus on Mediation for Banking Cases] (4 April 2012) Hukumonline.com <<http://www.hukumonline.com/printedoc/lt4f7c3e18704f3>>.

¹⁰⁵⁰ Ibid 12.

¹⁰⁵¹ Law No 8 of 1999 on Consumer Protection.

¹⁰⁵² Ibid. See Considering Section.

products and services, such as in bank payment card operations. In the event of theft or/and fraud occurring, consumers are still in a very weak position in regard to recovering their lost funds from the bank.

Bank consumers are in a weak position from the beginning of their relationship with the bank. The legal relationship between the bank and its customers is initiated when the customer and the bank enter into a deposit contract and the account is established.¹⁰⁵³ This relationship is generally governed by a bank's standard contract where often the terms and conditions have been created by the bank in the bank's favour.¹⁰⁵⁴ Although the adoption of a standard contract has itself been legitimated by the Indonesian legal system, in practice there are still many forbidden clauses such as 'liability dumping' contained in them.¹⁰⁵⁵ According to Anderson et al, liability dumping is a condition where 'firms seek to manage risk ... by externalising it on less powerful suppliers or customers'.¹⁰⁵⁶

Such liability dumping has been banned by the *LCP*. Article 18 of *LCP* explicitly prohibits the transfer of responsibility by businesses to their customers. Any violation of these provisions will cause the agreement to become null and void. Nevertheless, due to the lack of oversight of the bank agreement clauses with customers, most bank–consumer contracts still have liability dumping provisions. This causes a noteworthy inequality in the parties' rights and obligations arising under the contract, to the detriment of a consumer's rights when fraud occurs. Hence, despite the existence of prohibition of 'liability dumping,' some additional form of legal protection for bank consumers is no doubt needed in order to maintain their trust in bank operations.¹⁰⁵⁷ Otherwise it could be argued that there are less than optimal circumstances for motivating banks to reduce fraud as 'liability dumping' reduces the impetus for change by reducing impact on the banks themselves by minimising the possibility of a bank having to cover consumer fraud losses.

¹⁰⁵³ Miller and Harrell, above n 874, 413, 446. See also UNCITRAL, 'UNCITRAL Legal Guide on Electronic Funds Transfers', above n 189, 27–8.

¹⁰⁵⁴ Kristiyanti, above n 928, 12.

¹⁰⁵⁵ See Widiyono, above n 66, 73 and accompanying text.

¹⁰⁵⁶ Anderson et al, above n 338, 19.

¹⁰⁵⁷ Peter Cartwright, 'Consumer Protection in Financial Services: Putting the Law in Context' in Peter Cartwright (ed), *Consumer Protection in Financial Services* (Wolters Kluwer, 1999) 7.

6.4.3. Forum to Resolve Unauthorised ATM/Debit Card Transactions: Alternative Dispute Resolution (ADR) Body and the Court

Settlement of a civil or commercial dispute in Indonesia is generally conducted through lengthy litigation in the courts. However, out of court settlement also has been known in civil lawsuits. Article 45 of the *LCP* has opened up the possibility for any aggrieved consumer to sue business actors through institutions in charge of resolving disputes between consumers and business operators, or through judicial courts based on the voluntary choice of the parties to the dispute. Further, the *LCP* states that the settlement of disputes should be conducted outside the court in order to reach an agreement regarding the type and amount of compensation and/or regarding certain measures that must be taken to ensure that no such damages should occur again to consumers.¹⁰⁵⁸

During its development, the current settlement of a lawsuit outside the court system through a variety of arbitration and alternative dispute resolution (ADR) is relatively popular in Indonesia.¹⁰⁵⁹ Owen states that ADR is becoming more routine and accepted in Indonesia because it allows the disputing parties to resolve disputes quickly and inexpensively through a trusted third party.¹⁰⁶⁰ Zulham notes that ADR provides many benefits to the parties involved including: (1) greater guarantee of confidentiality; (2) involvement of expertise in the specific field; (3) simpler and more efficient procedures; (4) final and binding decision; and (5) no publication of the verdict without the parties' consent.¹⁰⁶¹ It could be argued that while the final provision reduces overall transparency and reporting of disputes, it could also make it attractive to various parties (especially defendants) and thus increase willingness to participate.

The exercise of arbitration and ADR has been practised from ancient times in Indonesia and is based on customary law in many communities in Indonesia. This traditional type of dispute resolution had been widely practised throughout the archipelago of Indonesia and ultimately became institutional and formalised by the enactment of the Law

¹⁰⁵⁸ See *LCP 1999* art 47.

¹⁰⁵⁹ Romli Atmasasmita, *Pengantar Hukum Kejahatan Business* [Introduction to the Law on Bisnis Fraud] (Prenada Media, 2003) 37. See also Mas Achmad Santosa, *Development of Alternative Dispute Resolution (ADR) in Indonesia* (2003) ASEAN Law Association (ALA) - Indonesia <http://www.aseanlawassociation.org/docs/w4_indo.pdf>

¹⁰⁶⁰ Owen et al, above n 64, 22. See also Alexander H Bevan, *Alternative Dispute Resolution* (Sweet and Maxwell, 1992). Note: re ADR, *LAADR* art 6(5) states that mediation must begin within 7 days of a mediator being agreed upon, and conclude within 30 days (art 6(6)).

¹⁰⁶¹ Zulham, Hi and Hum, above n 969, 88.

Number 30 of 1999 concerning Arbitration and Alternative Dispute Resolution (*LAADR*).¹⁰⁶²

LAADR principally encourages people to use arbitration or alternative dispute resolution to resolve civil disputes between parties. According to this law, an ‘arbitration institution’ is the governing (decision-making) body, and arbitrators are selected (and mutually agreed upon) by the parties to the dispute to give a verdict on a particular dispute. This process has been previously agreed upon, usually prior to any dispute arising, although an arbitration agreement can also be made subsequent to disputes arising (Article 1(3)). The institution is also able to give a binding opinion on a particular legal relationship in a case where no conflict has yet arisen.¹⁰⁶³ Where parties cannot agree on the choice of arbitrators, the Chairman of the District Court can select an arbitrator or arbitration panel (the various permutations of this process are covered in detail in chapters II and III of the Act).

ADR, on the other hand, is a mechanism that is used to resolve the dispute or difference of opinion through the procedures agreed upon by the parties of a settlement which explicitly state that disputes are to be settled out of court by way of ‘consultation, negotiation, mediation, conciliation, or expert opinion’.¹⁰⁶⁴ According to *LAADR*, every dispute in the private law area that can be filed with the court can also be settled through ADR. Besides *LAADR*, *LIET* also provides opportunity for disputant parties to settle their disputes by ADR.¹⁰⁶⁵

6.4.3.1. Bank Indonesia Banking Mediation Agency

Customer dispute settlement regulation as stipulated by Bank Indonesia in 2005¹⁰⁶⁶ is in practice, however, still far from successful. Much consumer dissatisfaction and many

¹⁰⁶² Santosa, above n 1059.

¹⁰⁶³ See art 1(8) of *Undang-Undang Republik Indonesia Nomor 30 Tahun 1999 Tentang Arbitrase dan Alternatif Penyelesaian Sengketa* [Law of Republic of Indonesia No 30 of 1999 on Arbitration and Alternative Disputes Resolution] (Indonesia) (*LAADR*1999).

¹⁰⁶⁴ See art 1(10) of *LAADR* 1999.

¹⁰⁶⁵ See art 39(2) *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik* [Law No 11 of 2008 on Electronic Information and Transactions] (Indonesia) (*LIET*)

¹⁰⁶⁶ *Peraturan Bank Indonesia Nomor: 7/7/PBI/2005 Tentang Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor: 10/10/PBI/2008* [Bank Indonesia Regulation Nomor: 7/7/PBI/2005 Concerning Resolution of Customer Complaints as amended by Bank Indonesia Regulation Number 10/10/PBI/2008] (*BIR RCC*). See also *Surat Edaran Bank Indonesia Nomor 7/24/DPNP Perihal Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Surat*

complaints are still emerging regarding the way in which banks resolve consumer problems. Consumer's disappointment is mostly caused by a bank's rejection of a consumer's claim, either in full or in part.

In accordance with *LAADR* and due to the existence of many prolonged disputes between banks and consumers, Bank Indonesia in 2006 stipulated the Bank Indonesia Regulation Concerning Banking Mediation to facilitate the resolution of unsettled disputes between banks and their customer as set out in the Bank Indonesia Regulation on Resolution of Customer Complaints. The goal of this regulation is to maintain the banks' good reputation and also to create an alternative dispute resolution venue for customers when their claims are rejected by their banks.¹⁰⁶⁷

Mediation in this regulation means a dispute settlement process involving a mediator to assist disputing parties to reach a settlement in the form of a voluntary agreement for some or all aspects of the problem under dispute.¹⁰⁶⁸ It is expected that this mediation process could provide a simple, efficient and fast mechanism for customers that are willing to settle their disputes with banks. Moreover, Bank Indonesia anticipates that the existence of the Banking Mediation Agency (of Bank Indonesia) will provide better protection to small consumers in the resolution of disputes against their own bank.¹⁰⁶⁹

Following this enactment, every consumer that has unsettled disputes with banks, and with the financial claim in such dispute being no more than IDR500 million,¹⁰⁷⁰ can file

Edaran Bank Indonesia Nomor 10/13/DPNP [Bank Indonesia Letter Number 7/24/DPNP Concerning Resolution of Customer Complaints as amended by Bank Indonesia Letter Number 10/13/DPNP].

¹⁰⁶⁷ See Bank Indonesia Regulation Number: 8/5/PBI/2006 Concerning Banking Mediation as amended by Bank Indonesia Regulation Number: 10/1/PBI/2008. See also Sembiring, above n 694, 184–6.

¹⁰⁶⁸ Bank Indonesia Regulation Number: 8/5/PBI/2006 Concerning Banking Mediation as amended by Bank Indonesia Regulation Number: 10/1/PBI/2008 art 1(3). Bank Indonesia will perform as a mediation agent until the Indonesian Banking Association can form an independent banking mediation institution. See Garner, above n 797, 1071. 'Mediation' is defined as a method of non binding disputes resolution involving a neutral third party who tries to help the disputing parties reach a mutually agreeable solution.

¹⁰⁶⁹ Bank Indonesia Regulation Number: 8/5/PBI/2006 Concerning Banking Mediation as amended by Bank Indonesia Regulation Number: 10/1/PBI/2008 arts 4, 5 and their elucidation. See also Heriani, above n 1049. In performing its banking mediation function, Bank Indonesia will assist customers and banks to review the dispute at its core in order to reach an agreement. In this regard, Bank Indonesia shall facilitate dispute settlement by way of summoning, bringing to meet, hearing, and motivating the customer and the bank to reach an agreement without giving a recommendation or a decision. In doing this, Bank Indonesia shall appoint an independent mediator that fulfils some qualifications such as having knowledge in banking, finance and/or law.

¹⁰⁷⁰ See Bank Indonesia Regulation Number: 8/5/PBI/2006 Concerning Banking Mediation as amended by Bank Indonesia Regulation Number 10/1/PBI/2008 arts 1s(4), 6. See also art 6 and its elucidation. In this regulation: 'Dispute' means a complaint submitted by the customer or customer representative to a banking mediator, after the dispute had undergone a dispute settlement process by the bank as stipulated in Bank Indonesia Regulation Concerning Customer Dispute Settlement. Meanwhile, the meaning of

their dispute with Bank Indonesia for alternative dispute resolution by way of a mediation process. Sondang Martha Samosir (former chief of Bank Indonesia's Banking Mediation Agency) concluded that cases related to the payment system are the type of cases that mostly arise. Further, the former Bank Indonesia Deputy Governor, Muliaman Hadad, has explained that the payment system's problems are dominated by ATM/debit and credit card cases.¹⁰⁷¹

However, although the BI banking mediation process is free of charge,¹⁰⁷² relatively rapid compared to judicial settlements,¹⁰⁷³ and should be promoted and published by banks to their consumers,¹⁰⁷⁴ its existence is still not recognised by most bank customers, as is shown in the results of the survey conducted by the author. Of the 30 consumer interviewees (including 6 consumers who had experienced unauthorised ATM/debit card transactions) from 6 respondent banks in Jakarta, Denpasar and Yogyakarta from July to August 2012, only 5 of had any knowledge about the BI banking mediation section as an alternative disputes resolution body in Indonesia.¹⁰⁷⁵

Furthermore, the mediator provides neither recommendations nor decisions binding on either party; the mediator is there to encourage the parties to reach agreement and not provide them with a solution. However, under Article 6(7) the successful conclusion of a mediation process involves a 'written agreement resolving the dispute or difference of opinion'. Such agreement 'will be *final and binding* on parties for execution in good faith' (emphasis added) but it must be registered at the District Court within 30 days of signing. If the disputing parties reach no mutual agreement, the parties must then bring

'financial claim' here is the customer's potential financial loss that is considered as being caused by the Bank's mistake or negligence. The financial claim value shall cover direct damage/loss and/or expenses already paid by the customer in the effort to settle the dispute, but not immaterial loss or consequential damages such as damage or loss due to defamation and misdemeanour.

¹⁰⁷¹ Heriani, above n 1049.

¹⁰⁷² However, in the event that customer or bank has the initiative to present expert witnesses, then the customer and bank have agreed to cover the expert witness expenses.

¹⁰⁷³ Bank Indonesia Regulation Number: 8/5/PBI/2006 Concerning Banking Mediation as amended by Bank Indonesia Regulation Number: 10/1/PBI/2008 art 11: 'to avoid excessive time frame on the dispute resolution process, the process of mediation shall have been completed in no more than 30 (thirty) working days, with option to extend for another 30 (thirty) working days'.

¹⁰⁷⁴ *Surat Edaran Bank Indonesia Nomor 7/24/DPNP Perihal Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Surat Edaran Bank Indonesia Nomor 10/13/DPNP* [Bank Indonesia Letter Number 7/24/DPNP Concerning Resolution of Customer Complaints as amended by Bank Indonesia Letter Number 10/13/DPNP]. According to this regulation, banks should publicise banking mediation as an alternative dispute resolution to its customers by providing the information in the form of leaflets, pamphlets, posters, booklets, website, or other means of publicity in each branch, or send such information along with the results of any customer's complaint by letter to the customer's address.

¹⁰⁷⁵ See, eg, interviews with bank consumers C-1–C-30.

the case to either arbitration or a court of law in order to secure a binding decision. In practice, Samosir has argued that not all of the cases brought to Indonesia's Banking Mediation Agency can be settled smoothly and a consensus reached.¹⁰⁷⁶

As Bevan argues, 'where there is a wide disparity between the parties in terms of power, then mediation may not be suitable'.¹⁰⁷⁷ In fact, many cases that are brought to Indonesia's Banking Mediation Agency by consumers are the same cases that have failed to be resolved on the first attempt at resolution within a bank's internal dispute resolution unit. In such instances, it is obvious that a bank generally has far much more power and knowledge than consumers, and greater control than consumers. All payment card system infrastructure is created by or decided upon by the bank and ultimately under the control of the bank. For instance, by examining the CCTV footage record (if any), transaction records, a consumer's transactions pattern and so on, the bank is the one who most probably knows whether the unauthorised transactions claimed by the consumers were indeed done by third party fraudster or someone else. Banks are also the ones who know almost everything about the type of identity theft and identity fraud that might jeopardise their payment card system and/or their consumers' funds.

Therefore, technically, it is very easy for a bank that lacks a commitment to fairness and does not have act in good faith to conceal the facts about unauthorised ATM/debit card transactions as such revelations may be feared to weaken the bank's position.

By way of contrast, it is very difficult for most consumers to articulate their position since in general consumers have limited knowledge about the banking system and it is almost impossible for them to access knowledge about that system or access 'back room' knowledge of a bank's operations. Consumers remain vulnerable to this day. Bank Indonesia still does not openly publish on its payment system website any ATM/debit card fraud figures (which are reported regularly by banks) nor details about the results of Bank Indonesia's supervision of the banks' ATM/debit card systems.

¹⁰⁷⁶ Heriani, above n 1049. In light of Bank Indonesia Regulation Number 8/5/PBI/2006, dated 30 January 2006, on Banking Mediation (State Gazette of the Republic of Indonesia Number 7/2006, Supplement to State Gazette of the Republic of Indonesia Number 4601), BI thought it 'necessary to set forth the implementation regulation in a Bank Indonesia Circular with the provisions as follows:

2(11).The Agreement reached in the Mediation process shall be contained in a Deed of Agreement, which shall be final and binding on the Customer and the Bank. Being final shall mean that the Dispute cannot be submitted to the executives of the Banking Mediation function for Mediation reprocess.'

¹⁰⁷⁷ Bevan, above n 1060.

Although there are some payment card fraud figures disclosed in the Bank Indonesia's payment system yearly report that are also posted in the Bank Indonesia's website, these figures could not be easily retrieved by using Internet search engines (the layperson's usual method of finding material). This makes these fraud figures unreachable by the vast majority of people unless they know to read the Bank Indonesia's report and are aware of how to source it.¹⁰⁷⁸

In general, banks commonly state that their systems are infallible. In practice however, there is much evidence to the contrary. The classic 'trump card' for banks in the disputes with their consumers over unauthorised ATM/debit card transactions is the liability dumping clause in the bank–consumers standard contract. In this contract, there are provisions that transfer bank liabilities to the consumer. Such a provision can include that if a consumer's ATM/debit card data is compromised and used by fraudsters, regardless of whether the consumer has or has not contributed to the crime, the bank will be deemed to have no liability for the consumer's damage (loss, injury).

As a result, in most cases, disputes between banks and consumers over unauthorised ATM/debit card transactions have to be escalated to arbitration or litigation in the court, because the mediation process has failed to achieve an agreement or the expected dispute resolution result.¹⁰⁷⁹ Even if the mediation is entirely successful or even partially in terms of a bank finally having agreed to redress the consumers' losses, often the reason behind these decisions could not be treated as a legal guidance for common consumers. Very often the basis of the agreed mediation decision was not a legal fact but mostly at the discretion of bank management and achieved by a direction from bank's management concerning the consumer's status. For instance, the consumer victims tend to have redress if they are old (to avoid 'karma'), have a favourable affiliation to a political party or religious organisation, a high ranking police/military official, the central bank, and so on. This was revealed by a number of banking mediation body interviewees.¹⁰⁸⁰

¹⁰⁷⁸ No consumers volunteered knowledge of such material in the interviews conducted.

¹⁰⁷⁹ Heriani, above n 1049.

¹⁰⁸⁰ Interview results from several Bank Indonesia Banking Mediation Body officers who requested anonymity. See, eg, BI-MBO-1; BI-MBO-2 (BI banking mediation body officer).

6.4.3.2. Consumer Dispute Settlement Body (CDSB)

6.4.3.2.1. Brief Overview

LCP establishes an independent body — the National Consumer Protection Agency — to regulate consumer protection and a dispute settlement body (the Consumer Dispute Settlement Body (CDSB)) in each district in Indonesia to function as a type of ‘small claims court’ (without being a court) for resolving disputes between business actors and consumers in Indonesia.¹⁰⁸¹ A CDSB can be used by disputant parties to resolve disputes that generally only involve relatively low amounts that are not worth settling in court in terms of expected length of time to be taken and proceedings cost that would be involved.¹⁰⁸² CDSBs are also chosen by consumers who are reluctant to file a lawsuit in the court because of their inferior position in terms of social and financial resources compared to those of business actors.¹⁰⁸³

Based on interviews with six consumers that had been victims of unauthorised ATM/debit card transactions as explained previously, most of the consumers’ claims for unauthorised ATM/debit card damages failed either in the banks’ internally provided dispute resolution processes and then in the alternative dispute resolution (ADR) venues provided, such as the Bank Indonesia Banking Mediation Agency. Accordingly, the opportunity to file a lawsuit at a CDSB as a ‘last resort’ for out of court settlement becomes the preferred choice for few banking consumers to settle their dispute with banks.

Article 49 of *LCP* introduced CDSBs to handle business actor/consumer disputes and to serve as a mechanism for out of court settlement of such disputes.¹⁰⁸⁴ CDSB members

¹⁰⁸¹ *LCP* 1999 art 45(1). CDSB has been established in several cities in Indonesia with the enactment of Presidential Decree No 90 Year 2001 Concerning the Establishment of CDSB at city of Medan, Palembang, Jakarta Pusat, Jakarta Barat, Bandung, Semarang, Yogyakarta, Surabaya, Malang and Makasar.

¹⁰⁸² Sidabalok, above n 792, 148–9. See also Adrian Sutedi, *Tanggung Jawab Produk Dalam Hukum Perlindungan Konsumen* [Product Liability in Consumer Protection Law] (Ghalia Indonesia, 2008) 22–3; Zulham, Hi and Hum, above n 969, 140–8; Shofie, ‘*Kapita Selekta Hukum Perlindungan Konsumen di Indonesia*’, above n 683, 123–6; Susanti Adi Nugroho, *Proses Penyelesaian Sengketa Konsumen Ditinjau Dari Hukum Acara Serta Kendala Implementasinya* [Consumer Dispute Settlement Process from Procedural Law Perspective and its Implementation Constrains] (Kencana Prenada Media Group, 2006) 15.

¹⁰⁸³ Nugroho, above n 1082, 75, 85.

¹⁰⁸⁴ *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen* [Law No 8 of 1999 on Consumer Protection] (Indonesia) (*LCP*) art 1(18).

consist of representatives of government, consumer and business. The CDSBs' functions among others are:

- (a) to handle and settle consumer disputes through mediation,¹⁰⁸⁵ arbitration¹⁰⁸⁶ or conciliation;¹⁰⁸⁷
- (b) to provide consultation for consumer protection;
- (c) to undertake supervision regarding the inclusion [and nature] of a standard clause;
- (d) to report to the public investigator if there are any violations to the provisions of the *LCP*;
- (e) to receive written or oral complaints from the consumers regarding violations of consumer protection;
- (f) to investigate and examine the consumer protection disputes;
- (g) to summon the business actors who are accused to have violated consumer protection;
- (h) to summon and bring witnesses, expert witnesses and/or each and every one considered to have known that there has been violation of the *LCP*;
- (i) to request assistance from investigators to bring the business actors, witness, expert witness, or each and every one intended by points (g) and (h) above who are not willing to fulfil the summons issued by the CDSB;
- (j) to obtain, examine and/or evaluate the letters, documents or other evidence to be used for investigation and/or examination;
- (k) to decide and determine if the consumer has suffered any damages or not;
- (l) to notify the decision to the business actors who have violated consumer protection;
- (m) to impose administrative sanctions against the business actors who have violated *LCP*.¹⁰⁸⁸

In accordance with this provision and in order to develop an effort for consumer protection, the CDSB shall establish a committee that must be uneven in numbers and consists of representatives of all elements (government, consumers, and business actors)

¹⁰⁸⁵ See Garner, above n 797, 1071. 'Mediation': a method non binding disputes resolution involving a neutral third party who tries to help the disputing parties reach a mutually agreeable solution.

¹⁰⁸⁶ Ibid 119: 'Arbitration: a method of dispute resolution involving one or more neutral third parties who are usually agreed to by the disputing parties and whose decision is binding.'

¹⁰⁸⁷ See ibid 329: 'Conciliation: 1. a settlement of disputes in an agreeable manner; 2. a process in which a neutral person meets with the parties to a dispute and explores how the dispute might be resolved; 3. A relatively unstructured method of dispute resolution in which a third party facilitates communication between parties in an attempt to help them settle their difference.'

¹⁰⁸⁸ See *LCP 1999* art 52. See also Santosa, above n 1059; Sidabalok, above n 792, 148–9; Sutedi, above n 1082, 24.

and shall be assisted by a registrar.¹⁰⁸⁹ The decision by such committee shall be final and binding and has to be enacted within 21 days of the case having been received.¹⁰⁹⁰ Within seven days of receiving the CDSB's decision, the business actors are obligated to implement the said decision.

Each consumer who has suffered damages when consuming an business actor's products and/or services may file a lawsuit against the business actor that is believed liable for the damages, through either an ADR forum or the court. If the disputants agree to choose an ADR or out-of-court institution as the forum to settle their dispute,¹⁰⁹¹ civil lawsuit in the trial court can only be made if the ADR failed to satisfy one or both disputants. In regard to ADR, the *LCP* has obliged the Indonesian government to establish CDSBs to settle consumer disputes outside the court. However, even though CDSB's decision is final and binding,¹⁰⁹² if the parties are not satisfied with its decision, they may appeal to the District Court and further to the Supreme Court to obtain a final decision.¹⁰⁹³ The party may submit an appeal to the trial court (District Court) within 14 working days of receiving the notification of the CDSB decision.¹⁰⁹⁴ Once the court accepts the appeal, the dispute settlement mechanism will be referred to ordinary court regulation.¹⁰⁹⁵

Nevertheless, many substantive laws in Indonesia also provide specific procedural law that differs from the ordinary procedural law mentioned below, such as proceeding law mechanism in *LCP*.¹⁰⁹⁶ For instance, in the *LCP* every consumer that has experienced damages may file charges against the business actors through ADR or in an ordinary

¹⁰⁸⁹ See *LCP 1999* art 54.

¹⁰⁹⁰ See *ibid* arts 54, 55. See also elucidation of art 54(3): What is meant by the expression 'the CDSB's decision is final' is that there is no appeal and cassation in the CBDS mechanism.

¹⁰⁹¹ *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen* [Law No 8 of 1999 on Consumer Protection] (Indonesia) ('*LCP*') art 47. This provision states that out of court settlement process only can be conducted in order to reach an agreement regarding the type and amount of compensation and/or regarding certain measures that must be taken to ensure that no such damages should again occur to the consumers in the future.

¹⁰⁹² *LCP 1999* art 54(3).

¹⁰⁹³ *Ibid* arts 56(2), 58(2). See also MVT/Yoz, above n 137. This is an online report concerning discussion at an international seminar on Commercial Arbitration (Gadjah Mada University, Yogyakarta (Indonesia)) regarding controversy about the CDSB final and binding decision that can still be appealed to the District Court and then the Supreme Court.

¹⁰⁹⁴ *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen* [Law No 8 of 1999 on Consumer Protection] (Indonesia) ('*LCP*') arts 45(1) and (2), 47, 56(2). See also Sidabalok, above n 792, 149.

¹⁰⁹⁵ *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen* [Law No 8 of 1999 on Consumer Protection] (Indonesia) ('*LCP*') art 48.

¹⁰⁹⁶ Mertokusumo, '*Hukum Acara Perdata Indonesia*', above n 152 8.

court of justice. In regard to settlement through ADR, if one of the disputant parties is not satisfied with the decision of the ADR process, the *LCP* provides opportunity for the party to make an appeal to the ordinary court of justice.

However, the procedural law in the court for cases arising from a complaint that has moved from a CDSB to the court is regulated differently by the *LCP*. Unlike in the ordinary trial court mechanism under regulations that in principle do not limit the length of the trial process, the time allowed for the process in trial court under *LCP* for CDSB appellate is limited (those regulations being the *Herziene Inlandsch Reglement* (HIR) for people living in Java and Madura areas or *Rechtsreglement voor de Buitengewesten* (RBg) for those living outside those areas). According to Article 58 of *LCP*, the District Court that examines a CDSB appellate case has to finish its examination and conclude its decision on the case within 21 days of receiving the appeal. A party that does not favour the District Court decision may submit a cassation to the Supreme Court of the Republic of Indonesia within a period of 14 days of the handing down of the appellate decision. The Supreme Court of the Republic of Indonesia is then obliged to render a decision within 30 days of receipt of the cassation petition. All in all, the whole dispute resolution process through the CDSB plus its appeal mechanism to the courts (District Court and Supreme Court) will only take approximately 100 proceeding days between initial lodgement of complaint with the CDSB and the final Supreme Court verdict. This is a far shorter period than that of the average length of process of civil lawsuit in the ordinary court, which can take approximately six to eight years from its inception in the 256-District Court until its final verdict in the Supreme Court.¹⁰⁹⁷

6.4.3.2.2. Unauthorised ATM/Debit Card Transaction Cases in CDSB (Which Are Then Appealed to the Court)

From the Supreme Court of Republic of Indonesia's website, CDSB proceedings, and mass-media, it can be seen that there have been several civil lawsuits concerning unauthorised ATM/debit card transactions cases that have begun in the CDSB and which have been finalised at the cassation stage or after civil law review in the Supreme Court. These cases are:

¹⁰⁹⁷ See n 141.

1. *Evi Yulisna br Harahap v Bank Mandiri (Card Trapping Case)*

Facts of the case:

On 13 October 2012, the plaintiff withdrew some money from the defendant's ATM in Tanjungsari (Simpang Pemda) Gas Station (Medan, West Sumatra). The withdrawal failed but the card was 'swallowed' by the ATM, as indicated by the ATM's monitor. The plaintiff claimed that she called the call centre number that appeared on the ATM to ensure that everything was under control. The plaintiff also claimed that she never revealed her PIN during the conversation. On 15 October 2012, the plaintiff attended the defendant's branch in Taman Setia Budi Indah Medan, the branch where the plaintiff had opened their account, just to find that she had losses totalling IDR78 million (from funds that she had previously deposited with the defendant's bank). The fraud was then reported to the defendant, Police Department, and Bank Indonesia, but there was not an outcome acceptable to the consumer. In the meeting with the defendants, Taman Setia Budi Indah Branch Head Mr Zulkarnaen Lubis and Mr Syahrudin Dalimunthe (the defendant's ATM Head) admitted that someone had compromised their ATMs, but they refused to be liable for the plaintiff's loss. The CCTV footage at the site was not up date and could not be used to confirm the transactions.

– The plaintiff then filed a lawsuit with the CDSB. On 14 February 2013, the CDSB judges in verdict number 77/Pen/BPSK-Mdn/2012 concluded in favour of the plaintiff and instructed the defendant to make redress for the plaintiff's damages within 14 days of the decision. However, the defendant refused to make redress and submitted an appeal to the District Court of Medan (the case was still in proceeding).¹⁰⁹⁸

¹⁰⁹⁸ See Sarsin Siregar, *Perlindungan Nasabah Jangan Sekedar Retorika* [Consumer Protection Should Not be just Rhetoric] (26 March 2013) MedanBisnis <http://medanbisnisdaily.com/news/read/2013/03/26/20104/perlindungan_nasabah_jangan_sekadar_retorika/#.Ux70NoXInxA>; See also Sarsin Siregar, *Evi Yulisnawati Minta Putusan BPSK Medan Direalisasikan* [Evi Yulisnawaty Asked CDSB-Medan's Verdict to be Fulfilled] (27 March 2013) MedanBisnis <http://medanbisnisdaily.com/news/read/2013/03/27/20328/evi_yulisnawaty_minta_putusan_bpsk_medan_direalisasikan/#.Ux72UoXInxA>; Far, *Uang Rp76 Juta Raib di Bank Mandiri* [Rp76 Million Disappears from Bank Mandiri] (14 May 2013) SumutPos <<http://sumutpos.co/2013/05/58129/uang-rp76-juta-raib-di-bank-mandiri>>.

2. *Mr Bahari v PT Bank Negara Indonesia (Persero) Tbk (Card Trapping Case)*¹⁰⁹⁹

Facts of the case:

- The plaintiff is the defendant's consumer. On 15 December 2007, the plaintiff withdrew money from the defendant's ATM at Gunung Pamela Hospital (Medan), but the card was trapped by the machine. A stranger then stepped into the defendant's ATM booth and encouraged the plaintiff to press the cancel button on the keypad. Because all efforts failed and the ATM card was still trapped inside the ATM slot, the plaintiff immediately visited the defendant's branch at Tebing Tinggi to report the incident. The plaintiff met with the defendant's security officer who told him that if the card was swallowed by the ATM, it meant that the card was safe. Later, it was revealed that on 15 and 16 December 2007, several unauthorised withdrawals and transfers had been made from the plaintiff's account and drained his funds, with a total loss of IDR60 million.
- The plaintiff filed the arbitration lawsuit with the CDSB of Medan. In verdict number 5/PEN/BPSK-Mdn on 12 March 2008 the CDSB ordered the defendant to pay damages of IDR60 000 000 to the plaintiff, this amount being equivalent to restitution of the funds lost.
- Following this decision, the defendant submitted an appeal to the District Court of Medan, with defences listed as follows: (1) Bank Indonesia Circular Letter No 7/60/DASP dated 30 December 2005 which urged banks to provide consumer protection, prudential action, and enhancement of bank payment card security, but never obliged banks to provide security officers or police to safeguard bank ATMs (as interpreted by the CDSB of Medan). Further the defendant contended that the security enhancement that is encouraged by Bank Indonesia circular only obliges banks to provide chip-based payment card technology, security enhancement on EDC or ATM machines and their supporting infrastructure, and the use of six digit PIN for ATM/Debit cards; (2) The defendant argued that they could not be punished by having to provide redress to the consumer, because the damage incurred was due to the consumer's own fault; (3) The defendant also argued that they had already educated consumers about the benefits and risks of payment cards such ATM cards, and the procedures that have to be taken by consumers if they experience difficulties with ATM

¹⁰⁹⁹ See Supreme Court decision No 718 K/Pdt.Sus/2008 dated 10 December 2008.

transactions. Such consumer education had been undertaken using various means such as using brochures, in writing, and in verbal conversation between the defendant's officer and the consumer when the bank gave the card to the consumer in person. This included the information that a consumer should not share the PIN information with anybody. Further, the defendant stated that *LCP* Article 5(a) obliges consumer to read and follow instructions issued by a party (in this case the defendant) when using that party's products and services; (4) The defendant alleged that the plaintiff had allowed a stranger to step into the defendant's ATM booth to help him with the trapped ATM card, and followed his instruction to press the PIN in the keypad which might have caused the PIN to be captured by the fraudsters; (5) The defendant argued that the damages incurred were not only because of the ATM used by the consumer swallowing their card (and then being retrieved from the ATM), but also because other people also knew the consumer's PIN. Therefore, based on Article 19(5) of *LCP*, business actors are not liable to the consumer if the damages occurred are due to a consumer's own fault. Hence, the defendant considers themselves as an business actor of good faith and, therefore, do not owe an indemnity obligation to the consumer. Following this appeal request, the District Court of Kisaran in their verdict number 06/PDT.G/2008/PN.KIS dated 15 May 2008 overturned the CDSB decision, and released Bank BNI from any obligation to pay the damages on the basis that the consumer's damage was due to the consumer's own fault.

– Following the District Court decision, the plaintiff submitted a cassation to the Supreme Court, and argued that his loss was due to a lack of security features as follows: (1) The defendant had not yet implemented chip-based payment card by 31 December 2008 as as required by Bank Indonesia Circular Letter No 7/60/DASP; (2) The payment card issuer was obliged to implemented six digit PIN for transaction security by 31 December 2006, but was still using four digit PINs for its consumers at the time of the offence, in breach of Article 8 of *LCP*, which forbids an business actor to produce and/or transact products and services that are not in conformity with the relevant standards as required by the regulation; (3) Bank Indonesia Circular Letter No 7/60/DASP obliged the issuer of a payment card to improve security features on payment cards in order to minimise the crime rate and improve consumer confidence in payment cards. This provision is similar to that of Article 4 of *LCP*, which gives consumers the right to convenience, security and safety in consuming an business

actor's products and services. As a consequence, even though the BI Circular Letter indeed does not specify in great detail what sorts of security features have to be implemented in payment card infrastructures, the plaintiff contended that because of the fact that there were so many fraud incidents that involve ATM infrastructure, the existence of security officers and CCTV cameras in an ATM booth is deemed to be necessary. Therefore, if there are some malfunctions and/or interference with ATM infrastructure in the absence of such precautions, the bank as the ATM owner should be deemed responsible and liable; (4) In regard to interference by a 'stranger' (that is, unknown party) in regard to ATM booths which jeopardised the consumer's transaction, the absence of bank security officers at ATM booths is the main cause of the incident as it also permitted the trapped card to be seized by the fraudsters; (5) Following the chronology of the above event, the Supreme Court judges posits that Bank BNI has not demonstrated good faith as it failed to secure its ATM transactions (as demanded by the applicable legislation and regulations) whereas the plaintiff had acted in good faith. Therefore, the Supreme Court verdict overturned the District Court decision on the ground that the District Court has incorrectly applied the right law. This was based on the fact that: (1) The consumer's claim — that he had never revealed his PIN to the fraudster and instead only pressed the 'cancel button' — was believed by the court; (2) The consumer had reported the card-trapping incident to the bank branch within 15 minutes of the incident having occurred; (3) Bank BNI was deemed to have not abided by Bank Indonesia Circular No 7/60/DASP as it had failed to safeguard its consumer's transactions at the ATM by the fact that card-trapping devices had been installed in the ATM and there was no bank security officer to secure the ATM booth; (4) The ATM card issued by Bank BNI only employed a four digit PIN instead of six digits PIN and thus bank practice conflicted with Bank Indonesia's circular letter. Overall, the Supreme Court decision was to order Bank BNI to pay damages equal to the consumer's losses, that is IDR60 million.

– Following this decision, the defendant submitted the case for civil case review to the Supreme Court on the following basis: (1) Bank Indonesia Circular Letter No 7/60/DASP does not oblige the bank to safeguard and guarantee that ATMs can continuously work properly, and/or provide a security officer to safeguard ATMs; (2) The defendant also alleged that the Supreme Court exhibited gross negligence or even a gross error when it accused Bank BNI of having not fulfilled Bank Indonesia

Regulation Number 7/60/DASP in regard to the use of a four instead of six digit PIN for ATM transactions, as this obligation will only be applied after 2016.¹¹⁰⁰ Following this case review, the Supreme Court civil case review judges rejected the civil case review submitted by Bank BNI,¹¹⁰¹ and so the judgement for the plaintiff stands.

3. *Muhajidin Tahir, SE v PT Bank Mandiri (Persero) Tbk and PT Advantage CSM (Card Trapping Case)*¹¹⁰²

Facts of the case:

– Plaintiff is the defendant's consumer and holds an ATM Card issued by the defendant. On 16 October 2010 around 6.30am, the plaintiff authorised his wife to use his ATM card to make a transaction at an ATM booth located in the District Court of Gowa (Makasar). Unfortunately, the card was swallowed by the ATM, and an apparent 'good Samaritan' walked into the ATM booth to offer the use of a mobile phone so that the plaintiff's wife could contact bank consumer call centre (whose number was displayed at the ATM) to resolve the ATM problem. The plaintiff's wife then spoke to the person on the phone who claimed to be an officer of the defendant bank, and due to this deception, the consumer then revealed her husband's ATM PIN. The plaintiff's wife then left the ATM with the ATM card still inside the ATM. On 17 October 2010 around 8pm, the plaintiff received a short message on his mobile from the defendant (automatic alert notification), notifying him that there had been an ATM withdrawal on his account. The plaintiff then called defendant's call centre to block his account. Unfortunately, several unauthorised ATM transactions in the form of cash withdrawals had occurred between 16 and 17 October 2010 and had drained his account. Total losses amounted to over IDR45 million. However, from the defendant's viewpoint, all those unauthorised transactions were deemed valid because of the use of the plaintiff's own ATM card and PIN, whereby the plaintiff had violated the bank–consumer agreement by surrendering his ATM and PIN to his wife. Therefore, the defendant argued that all plaintiff losses were the plaintiff's liability.

– Following this unresolved dispute, on 16 March 2011, the plaintiff submitted the dispute to the CDSB of Makasar City. CDSB verdict number 04/BPSK/III/2011 dated

¹¹⁰⁰ Author's note: In fact, Bank Indonesia Circular No 7/60/DASP was amended by Bank Indonesia Circular Letter No 8/18/DASP dated 23 August 2006, which has delayed the use of six digit PIN for ATM card until a date that will be determined by a Bank Indonesia special regulation.

¹¹⁰¹ See the Supreme Court Civil Case Review Decision No 122 PK/Pdt.Sus/2009 dated 3 March 2010.

¹¹⁰² See the Supreme Court Decision No 769 K/Pdt.Sus/2011 dated 27 February 2012.

26 April 2011 was made in favour of the plaintiff. Among the reasons for the decision were: (1) Once a consumer's ATM card is swallowed by a bank's ATM, then all responsibility and liability in relation to the ATM card and its associated accounts should lie with the bank; and (2) The use of an ATM card by a family member is not violating the law, since this practice was covered by customary law in Indonesia. Makassar City CDSB then concluded that the defendant has jeopardised consumer protection law and that caused damages for the plaintiff, and therefore, ordered that the defendant pay the consumer an amount in excess of IDR45.1 million (and thus exceeding the amount lost by IDR7700 million).

– Following the verdict, the defendant lodged an appeal with the District Court of Makasar City, on the basis that Makassar City CDSB incorrectly implemented the law. Bank Mandiri submitted that: (1) For transactions on an ATM to occur, every consumer has two devices, namely the ATM card and PIN. Hence, even if an ATM card is inserted into the ATM but the PIN is incorrect, then the ATM will automatically reject the transaction. Since consumers have an obligation to keep their PIN secret (including from their family), all consequences of the use of a consumer PIN will fall on the shoulders of consumers themselves as highlighted in the bank–consumer agreement; (2) Article 5(1) of *LCP* states that to ensure consumer safety, consumers should read and follow the procedures for use of an business actor's products and/or services. Hence, by giving his PIN to other people, the consumer had violated Article 5(1) and should be responsible for the consequences; (3) The defendant contended that they had already provided consumer education as obliged by the Act in regards to the consumer's obligation to safeguard their PIN as any unauthorised use of it would make the consumer liable. The defendant also submitted that it had disseminated their legitimate call centre number through various means, such as at bank branches, in brochures, via electronic media and at ATM booths. Therefore, consumers should know the defendant's legitimate call centre number, which is 1400 (and also (021) 52997777).

– Following this appeal from the defendant, the District Court of Makassar City in the verdict number 03/Pdt.BPSK/2011/PN.MKS dated 28 July 2011 made a decision in favour of the plaintiff and rejected the appeal from the defendant. The District Court decision also confirmed that the defendant's standard clause that contained a liability

dumping clause) in the bank–consumer agreement (shifting liability from the bank to consumers) breached Article 18 of *LCP* and therefore should be deemed null and void.

– Following the District Court rejection, the defendant then submitted a cassation to the Supreme Court on 8 August 2011 on several grounds: (1) It was not disputed that the defendant had to abide by the law, including civil law and Bank Indonesia Regulation such as Bank Indonesia Circular Letter No. 11/10/DASP dated 13 April 2009 concerning the Implementation of Payment Card, which obliged banks to operate their payment card infrastructure by implementing consumer protection principle, prudential action, and security enhancement in regard to payment cards. The defendant, however, argued that they had implemented Bank Indonesia’s regulation on payment cards, such as by providing consumer education on the importance of PIN secrecy (for example, by instructing cardholders not to write down the PIN on an ATM card, to regularly change PIN, and so on); (2) The defendant also argued that the standard clause on the defendant’s agreement did not violate the *LCP* because it only regulated something that is commonly implemented in the payment card system; (3) The damages that resulted in regard to the consumer ATM transaction were not incurred due to a weakness in the bank’s ATM infrastructure, but because of the plaintiff’s own negligence in revealing the ATM PIN to his wife who then further revealed it to other people. Based on Article 19(5) of *LCP*, business actors are not held liable for the damage to consumers if that damage occurred because of the consumer’s own fault.

– The Supreme Court in decision number 769 K/Pdt.Sus/2011 conversely favoured the defendant and rejected the District Court and Makassar City CDSB decisions on the grounds that: (1) *judex factie* (CDSB and the District Court of Makassar City) had wrongly implemented the law because they had provided an administration sanction with general provision (Article 4(a) of the *LCP*)¹¹⁰³ without linking it to other normative provisions that have sanction provisions in the *LCP*. In addition to that, the CDSB does not have the authority to punish an business actor with administrative sanctions as regulated by Article 60 of *LCP*;¹¹⁰⁴ (2) the damages incurred by the plaintiff were the

¹¹⁰³ *LCP 1999* art 4.a: ‘The rights of the consumer are to obtain comfort, security and safety in using or consuming the goods and/or service.’

¹¹⁰⁴ *LCP 1999* art 60: (1). The consumer dispute settlement body shall be authorised to impose an administrative sanction on the business actors who violate Article 19 Section 2 and Section 3, Article 20, Article 25 and Article 26; (2) The administrative sanction shall be determined in maximum amount of Rp.200,000,000.00 (two hundred million rupiah); (3) Procedure for determining an administrative sanction as intended by Section 1 above shall be further regulated by the law.

consumer's own fault, by giving the ATM card and PIN to his wife, which allowed the information she (unwittingly) gave to be communicated to other people.

– Following this cassation decision, the plaintiff filed a request for a civil law review with the Supreme Court on 5 October 2012, on the grounds that: (1) The use of Article 4 of *LCP* by the District Court and Makasar CDSB in relation to Article 60 of *LCP* was very relevant since both of the articles are contained in the same legislation and are interdependent; (2) It is very obvious that the damages sustained by the consumer were due to his ATM card having been swallowed as a result of inherent weaknesses of bank's ATMs. Hence, the use of Article 4(a) of *LCP* by the consumer to show that his right to convenience, security and safety while using bank products or services (as regulated by that Article) had not been fulfilled; and (3) Article 18(1), (2) and (3) of *LCP* clearly states that every standard clause in the agreement that contains liability dumping will be deemed null and void. Following this review, the Supreme Court with their decision number 190 PK/Pdt.Sus/20012 dated 20 February 2013 rejected the application by the plaintiff for a civil case review on the grounds that: (1) *Judex juris* or the Supreme Court's cassation decision did not make an incorrect decision according to the law and there was no new evidence (*novum*) that could justify the review; (2) The plaintiff's wife is the party that caused the damages and because of this damages could not be awarded against the defendant.

6.4.3.3. Under Court Litigation

6.4.3.3.1. Brief Overview of Court Structures and Its Procedural Rules

In Indonesia, judicial power is deemed very important and explicitly regulated under the Indonesian Constitution. Article 24 of the amended 1945 Constitution states that judicial power is an independent power to administer juridical proceedings in order to uphold law and justice. This judicial power is exercised by one Supreme Court and other subordinate judicial bodies in the ordinary court jurisdiction, religious court jurisdiction, military court jurisdiction, and administrative court jurisdiction, and by the Constitutional Court.¹¹⁰⁵ The judicial bodies consist of the Courts of First Instance

¹¹⁰⁵ *Undang-Undang Dasar Republik Indonesia 1945* [Constitution of the Republic of Indonesia 1945] art 24 (1) and (2). See also *Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman* [Law Number 48 of 2009 on Judicial Power] art 18. Nevertheless, this thesis only discusses litigation that happened in civil lawsuits before the public court.

(District Courts) and the High Court.¹¹⁰⁶ Most notable is the position of the Supreme Court. In Indonesia, the Supreme Court is critical because of its function as the ultimate upholder of justice in the state.¹¹⁰⁷

In an ordinary civil lawsuit, if one or more of the disputant parties are dissatisfied with the Court of First Instance's decision,¹¹⁰⁸ it can be appealed (*banding*) to the High Court.¹¹⁰⁹ Cassation (*kasasi*) may also be requested to the Supreme Court if an appellate court decision is considered unfair, or did not satisfy the interests of one of the disputants.¹¹¹⁰ The Supreme Court is the highest state court and has authority to process the cassation against the verdict given by the final level of the court beneath the Supreme Court.¹¹¹¹ In this regard the Supreme Court acts as a last resort of appeal from its subordinate court or other judicial bodies.¹¹¹² In principle, the Supreme Court verdict is final and binding, except if there is a request from the unsuccessful party to the Supreme Court for a writ *certiorari* for that Court to conduct a civil case review (*peninjauan kembali*). However, a case review only can be conducted for the disputant parties if there is a 'case or particular circumstances' such as the discovery of new

¹¹⁰⁶ Mertokusumo, '*Hukum Acara Perdata Indonesia*', above n 152, 32.

¹¹⁰⁷ Marzuki, '*An Introduction to Indonesia Law*', above n 145, 121. See also Mertokusumo, '*Hukum Acara Perdata Indonesia*', above n 152, 8.

¹¹⁰⁸ Marzuki, '*Pengantar Ilmu Hukum*', above n 155, 126. Under Indonesian law, the court of first instance (also called a trial court) is the only court that is able to issue subpoenas and examine witnesses and where the disputant parties appear before the court, conducts discovery proceedings, and reaches a decision. If both parties accept the trial court judgment, then the court's verdict will be final and binding. However, if one of the parties to the dispute does not accept the trial court verdict, the party may appeal to the appellate court (the High Court).

¹¹⁰⁹ Ibid 126–7. The appellate or High Court when examining the appellate case only deals with the case's documents concerning the case. Hence, it neither does issue subpoenas nor examine witnesses. The appellate court decision generally either may establish, reserve, or uphold the trial court judgment. See also *Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman* [Law Number 48 of 2009 on Judicial Power] art 27.

¹¹¹⁰ See *Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman* [Law Number 48 of 2009 on Judicial Power] art 23. See also Mertokusumo, '*Hukum Acara Perdata Indonesia*', above n 152, 238–9. See also Marzuki, '*An Introduction to Indonesia Law*', above n 145, 127:

In this last resort of proceeding, the Supreme Court will examine whether or not appellate court has taken proper procedures as prescribed by law and whether or not it has applied law accurately. The Supreme Court may rule out the appellate court judgment and at the same time support the trial court decision or confirm the appellate court verdict or overrule the appellate court decision and at the same time make its own decision over the appealed case.

¹¹¹¹ *Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman* [Law Number 48 of 2009 on Judicial Power] arts 20, 23. See Marzuki, '*An Introduction to Indonesia Law*', above n 145, 127. In Indonesia, following the Latin terminology, 'trial court and appeal court are called *judex facti* [which] means "the institution that judges the fact", while the Supreme Court is called *judex juris* [which] means "the institution that decides whether or not its subordinate judiciaries apply law properly".'

¹¹¹² See Amended *Undang-Undang Dasar Republik Indonesia 1945* [Constitution of the Republic of Indonesia 1945] art 24A (1). See also Marzuki, '*An Introduction to Indonesia Law*', above n 145, 127.

evidence (*novum*) and /or the presence of an oversight or mistake by the judge in applying the law.¹¹¹³

For the courts' procedural law, which is based on Article 5(1) of Emergency Law Number 1 of 1951,¹¹¹⁴ Indonesia is still basically using regulations which were adopted from the Dutch colonial system: the *Herziene Inlandsch Reglement* (HIR) for people living in Java and Madura areas, and *Rechtsreglement voor de Buitengewesten* (RBg) for people living outside of those areas.¹¹¹⁵

6.4.3.3.2. Unauthorised ATM/Debit Card Transaction Cases in Court

Unlike other settlement disputes in the CDSB, a dispute between a bank and a consumer over unauthorised ATM/debit card transactions that is directly submitted to the court is quite rare. This dearth of cases is likely to discourage potential plaintiffs from lodging a case. The lengthy period of time for the process and the relatively high cost of litigation are also deterrents.¹¹¹⁶ Many people also consider the courts unprofessional in handling business disputes, unfair, and unresponsive to the needs of the plaintiff. As a result, courts are considered less effective and efficient in the examination and resolution of business disputes when these are filed.¹¹¹⁷

In addition, there is a lack of legal certainty related to trial results. This is produced by reports of past cases where a degree of unpredictability of outcome, and lengthy procedures are often made public. This contributes to a reluctance to resolve the dispute with the bank in the ordinary court, especially for a consumer that lacks of resources compared to a bank. Judges are also accused of having knowledge that is too generalist,

¹¹¹³ *Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman* [Law Number 48 of 2009 on Judicial Power] art 24. See also Marzuki, 'An Introduction to Indonesia Law', above n 145, 127; Mertokusumo, 'Hukum Acara Perdata Indonesia', above n 152, 244–5.

¹¹¹⁴ *Undang-Undang Darurat Nomor 1 Tahun 1951 Tentang Tindakan-Tindakan Sementara Untuk Menyelenggarakan Kesatuan Susunan Kekuasaan dan Acara Pengadilan-Pengadilan Sipil* [Emergency Law Number 1 of 1951 on Temporary Actions to Perform the Unity of Ordinary Courts' Jurisdiction Power and Proceeding].

¹¹¹⁵ Mertokusumo, 'Hukum Acara Perdata Indonesia', above n 152, 7. However for a civil case appeal in the High Court, based on Emergency Law number 1 of 1951, the specific regulation for it is Law Number 20 of 1947 for Java and Madura areas, and RBg arts 199–205 for areas beyond Java and Madura. See also Sidabalok, above n 792, 149.

¹¹¹⁶ Sutedi, above n 1082, 27.

¹¹¹⁷ Zulham, Hi and Hum, above n 969, 141.

which makes it difficult for them to resolve complex or specific problems related to banking.¹¹¹⁸

6.4.3.3.3. *Nasruddin v PT Bank Mandiri Tbk (Card Trapping Case)*¹¹¹⁹

Albeit the existence of many disadvantages of utilising the court (as mentioned above), there was a case in which a consumer (Mr Nasruddin), a victim of card-trapping fraud, filed a lawsuit against his bank (PT Bank Mandiri Tbk) in the Jakarta District Court (*Nasruddin v PT Bank Mandiri Tbk*).

Facts of the case:

– The plaintiff was the defendant’s consumer and possessed an ATM card issued by the defendant. Based on the information supplied by the plaintiff, on 6 July 2010 around 6.50am in Jakarta, he went to the defendant’s ATM booth at Gonzaga High School (at Pasar Minggu, south of Jakarta) to withdraw some money. Because he incorrectly typed the total amount of the money to be withdrawn, the plaintiff then cancelled the transaction by pressing the ‘cancel button’. Surprisingly, instead of simply cancelling the transaction and expelling the card, the card was trapped inside the defendant’s ATM (and failed to come out). To resolve the problem, the plaintiff called defendant’s call centre number (52889777) that was listed on a sticker attached to the ATM (above the ATM slot). When the call was connected, the plaintiff related his ATM card problem to the person he believed to be a bank officer named ‘Iskandar’ at the defendant’s call centre. The ‘bank officer’ then asked several questions that are commonly asked by a call centre officer (for example, bank ATM card numbers, consumer account number, and mother’s maiden name and so on). After the consumer had answered all these questions, the bank officer told the plaintiff that his account had been blocked. Later, the plaintiff was encouraged by a friend to confirm the incident by calling 1400 (the defendant’s official call centre number) and ensure that his account was truly blocked. The plaintiff then made a visit to the defendant’s South Kemang branch to report the incident to Mrs Wildany F Kinana, a consumer service relation officer for the bank. She informed him that there had been a withdrawal of IDR8.9 million from the plaintiff’s

¹¹¹⁸ Shofie, ‘*Kapita Selektta Hukum Perlindungan Konsumen di Indonesia*’, above n 683, 30–2; Nugroho, above n 1082, 127–8. See also Bevan, above n 1060, 17; Yusuf Shofie, *Perlindungan Konsumen dan Instrumen-instrumen Hukumnya* [Consumer Protection and Its Legal Instruments] (Citra Aditya Bakti, 2009) 359–62; Nurdin, above n 155, 237–60.

¹¹¹⁹ See Distric Court of South Jakarta Verdict No 632/Pdt.G/2010/PN.Jkt.Sel dated 30 June 2011.

account. The plaintiff claimed that this was an unauthorised transaction. Further, according to the plaintiff, Mrs Kinana has admitted that there had been many card-trapping incidents and fake call centre stickers had been involved in a number of incidents where other bank consumers had also been defrauded. This information was also confirmed by Mr Suroso, the Gonzaga High School security officer, who also claimed that consumers had already frequently asked the defendant to improve security at ATM booths and place bank security officers on site. Following these requests, the defendant allegedly failed to secure ATMs, doing nothing to improve the security of the ATM system/booth. Among other things it failed to put security officers in place and regularly monitor ATMs. Such inaction had caused many consumers' ATM cards to be trapped and consumers subsequently defrauded.

– In accordance with these facts, the plaintiff alleged that the defendant committed a tort action by: (1) violating the law — among other things Article 1365 of the Civil Code (tort article), Bank Indonesia Regulation Number 11/11/PBI/2009 which obliges banks to safeguard and improve security on payment card technology, and Article 4(a) of *LCP*, which guarantees consumer rights to comfort, security, and safety in the consumption of goods and/or services; (2) violating the subjective right of the plaintiff whose deposit has been placed in the bank with an expectation that such funds should be maintained properly and safely; (3) failing to carry out its legal obligations as a bank that is responsible for managing its system and network of ATMs and ensuring that an effective disaster recovery plan is in place to address and minimise problems that might arise and interfere with the smooth operation of the ATMs. Further, it is the defendant's obligation to fulfil consumer protection principle and the prudential principle, and improve the security of their payment card system and network; (4) their tort action having triggered the damage suffered by the consumer, the defendant should be liable for the damages. Article 1365 of Indonesian Civil Code regulates that 'every unlawful act that harms another obliges the actor who causes the damage to pay damages due to his/her fault.'

Further, Article 1366 of the same Act states that: 'Each person is responsible not only for the loss caused by his actions, but also for the loss caused by his negligence or lack of care'. Because of the causal link between the tort action of the defendant and the actual damage suffered (a loss of IDR8.9 million), as well as the damage suffered in

terms of lost opportunity as regards the enjoyment and utilisation of lost funds, the bank is obliged by law to pay all such damages to the plaintiff.

– Judges urged the disputant parties to mediate their disputes as governed by the Supreme Court Regulation Number 1 of 2008. However, the disputant parties failed to reach an agreement. A civil lawsuit examination therefore proceeded.

– The defendant in its defence stated that the loss of the plaintiff's funds was a result of fraud committed by 'Mr Iskandar' as a 'stranger' falsifying the defendant's call centre numbers and claiming to be the defendant's officer. Therefore, the plaintiff should have reported any fraud committed by 'Mr Iskandar' to the police; and pursuant to Article 137(7) of HIR, the defendant also argued that the District Court was not authorised to examine and adjudicate cases before offences of counterfeiting and fraud that were here referred to the District Court had been proven in criminal court decisions, which are final and binding. The defendant also argued that because the plaintiff had contacted 'Mr Iskandar' and supplied his bank account number and PIN, which are supposed to be kept secret, and this information was later used to cause the loss of customer funds, the claim was unsupportable as the judge had to decide that the plaintiff's claim was not able to be accepted because it did not include 'Mr Iskandar' in the lawsuit. Other than that, the defendant claimed that the plaintiff had agreed to various terms and conditions as set forth in the consumer-bank agreement, including the obligation of the plaintiff to keep the PIN secret. The plaintiff was also blamed for contacting the number that was not the defendant's call centre number. Therefore, the defendant argued, the bank would not liable for the misuse of the PIN.

– In relation to the allegation that the defendant had not enhanced their security, the defendant denied this allegation by stating that all their ATMs are secure. The defendant also argued that the presence of security officers is unnecessary to secure ATM premises. As to the allegation that there was a malfunction of the defendant's ATM that caused many consumers' ATM cards to be trapped and which therefore was evidence that the defendant had violated Bank Indonesia Regulation Number 11/11/2009 and Article 1365 of the Civil Code concerning tort action, the defendant contended that the allegation was not based on facts since the appointed ATM was working properly and there were no complaints from the other consumers. The defendant also stated that they publicise their genuine call centre number quite exhaustively via print and mass media

(such as TV programs, commercials) as well as online, in brochures and leaflets at bank branches, and on billboards, on the ATM cards themselves and ATM monitors. The defendant also stated that they already give many safety tips for consumers, including warnings to secure their card and PIN, warnings not to disclose consumer PIN to anybody, suggesting that consumers cover keypad with their hand when entering their PIN, and so on. Therefore, if a consumer calls a number other than the Bank Mandiri call centre number (1400), then all damages incurred should be borne by the consumer themselves, because the damage was caused by their own fault or negligence.

– Following the dispute, the District Court of South Jakarta issued a verdict as follow: (1) The lawsuit is a civil tort filed by the plaintiff can be examined by the District Court judge without the need to wait for the criminal process, especially as there are no criminal proceedings relating to this lawsuit; (2) In a tort civil lawsuit between the plaintiff and the defendant, there is no need to add a third party fraudster as party to the lawsuit; (3) The tort lawsuit filed by plaintiff against the defendant should be rejected because there was no evidence that the defendant had violated the rights of the plaintiff subjectively, on the basis that (a) there is no obligation for the defendant to put a security guard on each of its ATMs; (b) plaintiff cannot prove the number of complaints or complaints from the public that are related to the presence of the card-trapping devices installed by criminals on the bank's ATM;¹¹²⁰ (c) The presence of a spurious call centre sticker on the ATM should have made the plaintiff more vigilant; (d) The defendant had quite clearly informed the plaintiff of the correct call centre number to the plaintiff; (e) It is the obligation of the plaintiff to maintain the confidentiality of his PIN, so he/she should be held responsible when the PIN is used by an unauthorised person; (f) The presence of a spurious call centre sticker on the defendant's ATM does not mean the defendant has violated the Bank Indonesia regulations related to the obligation of banks to increase security on its ATM system, although the defendant has the obligation to immediately remove it if it is found in ATM booths.

¹¹²⁰ See Carl and Reni, above n 141. The Indonesian Civil Procedural Law does state the broad principle that 'a person who claims to have a right, or refers to a fact to substantiate his right, or to contradict someone else's right, must evidence the existence of that right or that fact.'

6.5. Conclusion

In the absence of clear and decisive loss allocation rules for unauthorised ATM/debit card transaction, the tort law of negligence under articles 1365–1367 of Indonesia Civil Code becomes the most common legal basis for consumer lawsuits to claim redress from the bank. However, the bank liability is voided if the bank can prove that the loss was incurred due to the customer's own fault or negligence. As a result, the dispute between a consumer and bank typically revolves around the question of whether the bank or consumer is actually at fault and whose fault/negligence has caused the losses.

The liability principle is acknowledged in Indonesia's Civil Code as not only containing tortious liability principle, but also vicarious and occupier liabilities. *LIET*, which also recognises the vicarious liability principle, specifically governs the use of banks' electronic agents such as ATMs and EFTPOS machines, and also third party providers. Banks as the principals of the ATM/debit card system are responsible for any legal ramifications that are derived from ATM/debit card transactions which initiated at banks and/or banks' third party electronic agents/infrastructures (vicarious liability). Meanwhile, in theory, occupiers' liability could be drawn if the bank as the owner or controller of the ATM/EFTPOS failed to secure or control its electronic agent — which has caused damages (pure economic loss) for the user of the electronic agent. However, defences as outlined in the above situation serve to restrict liability in practice.

In tort law, whether in Indonesia or other jurisdictions, generally, the ATM/debit card consumer as the party who alleges the bank has undertaken a tortious act, has an obligation to prove the defendant bank negligence that has caused a pure economic loss. However, this is a difficult and almost impossible undertaking, since all the evidence or witnesses relating to unauthorised ATM/debit card transactions are under the control of the defendant bank as provider/owner of the ATM/debit card system (such as CCTV camera footage, detail transaction records, and so on).

Several ADR venues in Indonesia are considered not to be optimal in helping consumer to settle their disputes over unauthorised ATM/debit card transactions. Bank Indonesia's Banking Mediation Agency gives relatively little help to the disputant party, especially the victim, the consumer since it has no power to make a final decision (as a mediator only). The CDSBs although giving some hope to the victims of unauthorised

ATM/debit card transactions, in practice, all CDSB verdicts on unauthorised ATM/debit card transaction disputes that are in favour of consumers (who are awarded damages against a bank) are overturned on appeal, whether to the district and/or Supreme Court). Hence, their existence seems almost ‘useless’ for consumers.

In civil court proceedings, in theory, generally damages can be claimed by the plaintiff only if the defendant is proved to be at fault or negligent and there are no defences that are accepted by the court. However, the most common defence utilised by the defendant in a civil liability claim in Indonesia is pure contributory negligence, where the plaintiff or victim of an unlawful act should not contribute in any way to the occurrence of damages (the so-called ‘clean hands’ policy). As a result, all court verdicts in regard to unauthorised ATM/debit card transactions that are derived from identity theft methods, where the plaintiff also ‘contributed’ to the loss, such as in card-trapping fraud, are usually all in favour of the defendants. The existence of the bank’s infrastructure of various fraudulent devices, such as card-trapping devices, spurious bank call centre numbers, as well as the absence of consumer protection material about inherent risk (and genuine level of risk) of ATM/debit transactions and so on that have become the dominant factor in the occurrence of fraud — tends to be ignored (or their importance minimised) by the judges in the consideration of their decisions. Hence court verdicts were deemed to have failed to create just and sensible decisions.

In contrast, the pure contributory negligence principle has been abolished in most of western countries because it tends to be unjust to consumers. Instead, for loss allocation rules, the pure contributory negligence principle has been superseded by ‘comparative negligence’, which is deemed to be more balanced and fair.

All in all, the failure of banks to secure their ATM/debit infrastructure and operations from fraudulent activities, the incomplete consumer protection regulations that lack detailed and fair fraud liability rules (especially those that redress provisions in the event of unauthorised ATM/debit card transactions), and the many drawbacks in the implementation of consumer protection regulations for ADR institutions and courts, have generally disadvantaged payment card consumers in practice. All these unfortunate factors have also reduced the incentives for banks as providers of ATM/debit card operations to improve their security systems and provide easier, timely, and fair redress mechanisms for their consumers. Reforms in these areas are accordingly long awaited.

CHAPTER 7 – LAW REFORM ON THE LOSS ALLOCATION RULES AND DISPUTE RESOLUTION BETWEEN CONSUMER AND BANK CONCERNING UNAUTHORISED ATM/DEBIT CARD TRANSACTIONS IN INDONESIA

7.1. Introduction

The need for law reform of the loss allocation rules for unauthorised ATM/debit card transactions in Indonesia is clear and is derived from the empirical fact that almost all court verdicts concerning unauthorised ATM/debit card transactions disputes between bank and consumer favoured the bank, a result that is considered to be unjust and arbitrary. The verdicts have ignored several important facts such as the existence of inefficiency and asymmetry of information in the payment card system, the inherent risk in the ATM/debit card operations, and banks' reluctance to supply fraud risk education to the consumers (a market failure).

This chapter proposes several ways to overcome the problems. However, due to the multifaceted aspects involved in unauthorised ATM/debit card transactions/operations, multi-disciplinary approaches using economic, technological and legal aspects are deemed required to ensure that the law reform can accurately achieved its objectives.

It is argued that adjudication/litigation proceedings, which utilise the outmoded and unjust concept of pure contributory negligence and allocate the onus of proof in a manner that disadvantages consumers, should be reformed. Among the ideas proposed to ensure fairness and offer the optimum incentive for a satisfactory result are *res ipsa loquitur*, negligence *per se* doctrine, comparative negligence principle, and shifting the onus of proof onto the shoulders of the bank involved. The typology of prominent and popular identity theft and frauds is also established on the basis on their point of compromise to find the the party party or parties that could reduce fraud loss at the lowest cost (the 'least cost avoider/s') who eventually should be liable for the loss.

Nevertheless, clear, fair, detailed, and decisive loss allocation rules for unauthorised ATM/debit card transactions in Indonesia are necessary to ensure banks and consumers have appropriate incentives to secure ATM/debit card transactions. The rules are believed to ensure uniformity, predictability and a more sensible decision if a dispute

about an unauthorised ATM/debit card transaction is adjudicated in the court or ADR forum.

In order to optimise resulting law reform recommendations, in the quest of most effective, fair and appropriate loss allocation rules concerning unauthorised ATM/debit card transactions in Indonesia, both US-style strict liability regulation and the Australian fault-based liability regulation model are discussed, compared, and analysed.

7.2. Compelling Reasons for Law Reform on Loss Allocation Rules Concerning Unauthorised ATM/debit Card Transaction in Indonesia

7.2.1. Market Failure and Fraud Asymmetry Information in ATM/Debit Card Operation in Indonesia

When a n unauthorised ATM/debit card transaction occurs and a consumer loses funds from their bank account, the natural implication — which has also become the focus of this thesis — is the distributive issues, that is, the question of how to re-allocate the damages between the two or more parties to the dispute or which party that should be liable to bear the loss. Even though this is probably a very simple question, in Indonesia the answer is not.

In cases of unauthorised ATM/debit card transactions, the fraudster that is the party most deserving to be punished and liable for the loss, is usually long gone by the time the fraud is discovered by the consumer and/or bank, or if apprehended, does not have enough money to adequately compensate the loss.¹¹²¹ On which party the fraud risk ultimately rests thus probably depends on the circumstances of the payment system, such as the instrument used to commence payment, the manner used to process the payment, and the means and the point of compromise at which the identity fraud was perpetrated.

In a free market operation, private agreement is generally preferable for market participants to achieve an economically efficient result in their economic transactions. However, as has been highlighted by CPSS-BIS, an efficient and robust payment system could not entirely depend on the market alone:

[M]arket forces alone, however, will not necessarily achieve the objectives of safety and efficiency sufficiently, since operators and participants do not necessarily bear all the risks and cost. They may not have adequate incentives to minimise the risk of their own

¹¹²¹ Braun et al, above n 279, 142–4. See also Steennot, above n 47, 555; Rusch, above n 106, 561.

failure or the failure of a participant or the costs they impose on other participants. In addition, the institutional structure of the payment system may not provide strong incentives or mechanisms for efficient design and operation.¹¹²²

Basically, ADR fora and the courts can play a very important role where market failure exists, imposing justice and providing remedy. However, should ADR institutions and the courts not manage to create a resolution — due to the absence of common guidelines and the very subjective and poor judgment of the adjudicators — the legislature / government / payment system authority may do so.

Government intervention becomes necessary when the market fails to produce the expected efficiency result (market failure).¹¹²³ When market failure exists — legal rules (whether in the form of legislation or other measure) are expected by one or more market participants to enforce agreement and/or protect one or more weak or victimised parties to the contract. Legal rules are also necessary for the victimised party who probably is not a party to the contract, but suffered harm or damages when consuming or using the product or services offered by another party.¹¹²⁴

Typically, market failures occur in the payment system because of disproportionate negotiation cost or asymmetrical information between a bank and its consumer.¹¹²⁵ As Ramasastry points out, ‘consumer confusion, to the extent it exists with respect to retail payments, may indicate market failure’.¹¹²⁶ When private agreements fail to work properly and fairly, Cooter and Rubin have argued:

[I]n an operating market, private agreements between parties will generally produce economically efficient results without the need for legal intervention. Intervention becomes necessary, however, when the market fails to produce these efficient results on its own. Rules that are designed to achieve economic efficiency in payment law, therefore, should enforce agreements between private parties when no market failure has occurred. When market failures exist, legal rules can improve upon private agreements if they are designed with the goal of minimizing costs in mind.¹¹²⁷

In Indonesia, the bank–consumer relationship concerning ATM/debit card operation is regulated by a bank–consumer standard contract. In practice, there is no chance for a

¹¹²² CPSS, ‘Core Principles for Systemically Important Payment Systems’, above n 317, 4.

¹¹²³ See Jean Charles Rochet and Jean Tirole, ‘Externalities and Regulation in Card Payment Systems’ (2006) 5(1) *Review of Network Economics* 3. See also Glaessner, Kellermann and McNevin, above n 51, 6; Owen et al, above n 64, 14–15.

¹¹²⁴ Cooter and Rubin, above n 105, 67–8.

¹¹²⁵ Ibid 66.

¹¹²⁶ Anita Ramasastry, ‘Confusion and Convergence in Consumer Payments: Is Coherence in Error Resolution Appropriate’ (2008) 83 *Chi.-Kent L. Rev.* 813, 846–7

¹¹²⁷ Cooter and Rubin, above n 105, 68.

consumer to negotiate provisions within the contract. It is a ‘take it or leave it’ contract. With the enactment of the *LCP*, the contentious dispute between legal scholars and practitioners over the validity of standard contracts should have been solved. According to the *LCP*, a standard contract is a valid contract, unless it contains liability-dumping provision.¹¹²⁸ However, the problem is in practice. As has been discussed earlier, banks’ standard contracts for consumer deposit accounts and their payment system instruments such as ATM/debit cards still contain many liability-dumping provisions that weaken the consumers’ position in the event of an unauthorised ATM/debit card transaction dispute.

Concerning the banks’ standard contracts, Cooter and Rubin argue that most consumers actually do not understand and pay attention to the liability terms of a contract when opening a bank account.¹¹²⁹ This state of affairs arguably exists in Indonesia, where consumer literacy regarding financial and legal terms is very low. ‘Liability’, ‘redress’, ‘compensation legal suit’, and so on are not popular terms in Indonesia since redress claims in ADR and Court fora are difficult to win and waste many resources (such as money, time and effort). Until recently, the government authority charged with the oversight of business actors’ standard contract, namely the National Consumer Protection Body,¹¹³⁰ and the banking authority, such as Indonesia’s Financial Service Authority (OJK) and/or Bank Indonesia, apparently did not consider bank liability dumping practices as an urgent problem that requires immediate assessment and action. Court judges also do not provide one uniform verdict on whether or not a bank–consumer contract should be deemed null and void for containing liability-dumping provisions.¹¹³¹ Consequently, consumer claims over the loss of money deposited in their bank accounts due to unauthorised ATM/debit card transactions are usually rejected by the banks.

Apart from this issue, various Bank Indonesia regulations — such as those on the card-based payment system and information technology risk management — do exist but problems are still encountered in their operation. There are many directives for banks to

¹¹²⁸ Art 18 *LCP*.

¹¹²⁹ Cooter and Rubin, above n 105, 69–70.

¹¹³⁰ See art 34 *LCP*.

¹¹³¹ See art 18(3) *LCP*. According to this provision, every agreement provision that contained liability dumping provision should be declared null and void. However, in the practice most court verdicts even ignore the existence of this prohibited provision in the bank–consumer agreement.

improve their payment card security systems and safeguard consumer transactions. For instance, banks have an obligation to utilise chip card technology in the ATM/debit card operations as a replacement for magnetic stripe technology that are notoriously vulnerable. Banks have also been obligated to lengthen the payment card PIN from a four to six digit PIN, monitor the security of ATMs, encrypt the data transmitted between consumer activated terminal and host computer, and so on. Banks also have an obligation to improve consumer awareness among other things by promoting transparency and consumer education about the benefits and risks of their products and/or services.¹¹³²

Unfortunately, in regard to consumer education obligation, banks in Indonesia are reluctant to educate their consumers about the risks involved in consumer payment card transactions, that is, negative consumer education. Instead, banks are only keen to give positive consumer education, that is, just the benefits and advantages of a bank's products and services for consumers. In anecdotal opinions provided by banking personnel, giving negative consumer education could reduce consumer confidence in making payment card transactions, and thus could reduce consumer transactions volumes and eventually, the banks' fee-based income revenue.¹¹³³ Hence, on many occasions, banks boast about their state-of-the-art security and infallibility. In contrast, negative consumer education (tips about security) is very limited and not comprehensive. Banks generally only post the tips about security material either on the bank's website and/or in the sticker attached to the bank's ATM or ATM booth. From on-site interviews conducted by the author at several ATM centres with 30 bank ATM users, most of them didn't even notice existence of the bank's security tips on or near the ATM body or booth.

As a matter of a fact, many experts and payment system institutions concur that risk education and knowledge on how to avoid it are very important for consumers as this

¹¹³² Unfortunately, due to technical and preparation problems, the utilisation of chip card technology for bank ATM/debit cards that was supposed to be ready in 2015 has been re-scheduled until 2020 by Bank Indonesia.

¹¹³³ Pusat Riset dan Edukasi Kebanksentralan, '*Hasil Survey Pemetaan Kejahatan Identity Theft dan Fraud Pada Alat Pembayaran Menggunakan Kartu: Pencegahan, Mitigasi dan Perlindungan Konsumen di Indonesia* [Survey Result on Taxonomy of Identity Theft and Fraud on Payment Card Instrument: Prevention, Mitigation and Consumer Protection in Indonesia] (BI-Fraud Survey)' (Bank Indonesia, 2015). This face-to-face survey was conducted by the Central Bank Research and Education Centre—Bank Indonesia in April–May 2015 and involved 280 card holders in four prominent cities that have experienced payment card identity theft and fraud: Jakarta, Bandung, Yogyakarta and Bali.

would raise their awareness and enable them to take precautions against fraud.¹¹³⁴ In Indonesia, this observation was corroborated by the most recent BI-fraud survey.¹¹³⁵ According to this survey, 71 per cent of respondents admitted that they had never received any payment card fraud education from their bank. Further, when they were asked about what their response would be if the bank truly gave them payment card risk education, 86.2 per cent of respondents indicated that they would still conduct payment card transactions but enhance their precautions. Conversely, only 1.8 per cent of respondents said that they would probably completely stop using payment card transactions, and 11.9 per cent of respondents said that they would worry and probably reduce their transaction intensity.

As result of this lack of adequate risk education, many bank consumers actually have a false feeling of security about their bank. Given this asymmetry of information about various ATM/debit card fraud methods that could result in the loss of their ATM/debit card data or genuine card and PIN, most consumers do not even think about the possibility of fraud when conducting ATM/debit card transactions at ATMs and EFTPOS machines. In other words, consumers in Indonesia do not generally have any awareness of risk nor hence the ability to take precautions against fraud before undertaking an ATM/debit card transaction.¹¹³⁶ As consequence, even though fraudulent activities only happen intermittently,¹¹³⁷ once it has happened, most of the targeted consumers have fallen into a fraudster identity theft trap, which thus leads to further identity fraud.¹¹³⁸

Therefore, market failure has obviously become the case in payment card operation in Indonesia, where disproportionate negotiation costs, asymmetric fraud risk information,

¹¹³⁴ See Tracy Kitten, *3 Reasons Skimmers Are Winning* (10 May 2012) Bank Info Security <<http://www.bankinfosecurity.com/3-reasons-skimmers-are-winning-a-4752/op-1>>. See also BCBS, *Risk Management for Electronic Banking and Electronic Money Activities*, above n 3, 6–7.

¹¹³⁵ See BI-Fraud Survey, above n 1133.

¹¹³⁶ Ibid. The BI-fraud survey results indicated that only 13% of respondents always feel worried about identity theft risk when conducting payment card transactions at a consumer activated terminal.

¹¹³⁷ Cooter and Rubin, above n 105, 70. ATM/debit card fraud occurs intermittently; however, due to many incentives for this fraudulent activities for individual and local and international organised crime, and global interoperability of ATM/debit card infrastructures, its occurrence is certain and the exposure to damages is huge.

¹¹³⁸ Some fraudulent activities are ‘too perfect’ and/or intangible in the eye of the consumer, such as is the case with malware, skimming, and ‘man-in-the-middle’ attack. Some other fraudulent activities which are supposed to be more obvious and involve social engineering method — such as card swapping, card trapping, and alike — fail to be spotted by consumers because they have not had any exposure to or knowledge of such frauds previously.

a failure to routinely, rigorously and consistently implement the fraud liability dumping provisions, and the absence of clear, fair, detailed, and decisive loss allocation rules exist in payment system operations.¹¹³⁹

Hence, government intervention in the form of law reform on loss allocation rules for the payment card system in Indonesia is necessary immediately. In considering options for reform, other countries' loss allocation rules (such as those of Australia and/or United States) will also be considered as long as they fit with Indonesia's specific circumstances.

7.2.2. The Absence of Clear, Fair, Detailed, and Decisive Loss Allocation Rules and Presence of Unjust Court Verdicts on Disputes between Consumers and Banks concerning Unauthorised ATM/Debit Card Transactions

A safe, robust, and efficient payment system is a pre-requisite to the effective functioning of the financial system in a country. To achieve this ideal payment system, CPSS-BIS has argued that it is very important that a well-founded and robust legal basis be established. From the legal perspective, the system not only has to ensure a high degree of payment system security and operational reliability, but also should enable participants to have a clear understanding of the risk that might be incurred in their transactions. The system should also define the respective responsibility of the payment system operator and other participants in its operations with regard to various risks that are entwined in the payment system operation, such as financial risk, fraud risk, and so on, and by whom such risks are to be borne. It is also emphasised that the rules and procedures of the system should be enforceable and their consequences able to be predicted and understood by participants, thus creating incentives and capabilities to manage and contain each of the risks they bear. Poor understanding of payment system risks can give participants a false sense of security, leading them to underestimate the real threat that always haunts the payment card system.¹¹⁴⁰

In Indonesia, general loss allocation rules that are utilised in resolving disputes between banks and consumers about unauthorised ATM/debit card transactions are embodied in several pieces of legislation such as the Indonesia Civil Code, *LCP*, and *LIET*. In the Civil Law Code, basically a party or parties who commit a fault or negligent act which

¹¹³⁹ Cooter and Rubin, above n 105, 69–70.

¹¹⁴⁰ CPSS, 'Core Principles for Systemically Important Payment Systems', above n 317, 3–7.

causes damage to another party shall be obliged to compensate the damage. Meanwhile, under the *LCP* and *LIET*, banks as a provider are liable for the consumer's loss due to unauthorised ATM/debit card transaction, unless they can prove that the damage has occurred because of a consumer's own fault or negligence.

Therefore, one can assume that between a bank and consumer in an ATM/debit card fraud liability dispute, the liability would always lie with the bank as the provider of the system/owner of the products/services (presumed liability). A bank can only pass this liability to the consumer, if it can prove that the consumer's loss was actually due to the consumer's own fault/negligence (fault/negligence liability). The derivation of these liability rules in the payment card area can only be found in the Bank Indonesia Regulation.¹¹⁴¹ In this regulation, bank is encouraged to be financially ready to meet their liability that 'might arise' in the event of ATM/debit card fraud.

Unfortunately, none of this legislation further explains what constitutes 'consumer's own fault/negligence' or explains the phrase 'might arise' either in the general circumstances or in the specific circumstance of ATM/debit card identity theft and fraud. Consequently — as might be shown in the various court verdicts over unauthorised ATM/debit card dispute — there is no uniform understanding by banks, consumers, ADR adjudicator and court judges in terms of what constitutes bank or consumer negligence in ATM/debit card operations and practices. In this respect, Indonesia lags behind the United States with its *Electronic Fund Transfer Act 1978* and *Regulation E* which put all liability for fraud in ATM/debit card transactions onto the financial institution whether or not there was consumer negligence/fault (strict liability), or Australia with its ePayment Code, which has quite clearly regulated which party should liable for the losses sustained in cases of unauthorised ATM/debit card transactions.

Therefore, up until now, Indonesia's current legal and regulatory arrangements for loss allocation rules between consumers and banks in the event of fraudulent activities (fraud liability) are deemed too general and ineffective, unable to provide clear, fair, detailed, and decisive guidance in e-banking disputes caused by unauthorised ATM/debit transactions.

¹¹⁴¹ Elucidation section of art 22 of *BIR-CBPI*.

7.2.2.1. Flaws in the Bank's Internal Dispute Resolution Unit: Unjust Liability Dumping Provisions.

At the very first stage, a bank's internal dispute resolution unit typically becomes the first resort as the dispute resolution forum. Nonetheless, in this forum the consumer's position is very weak since the bank — which possesses almost all ATM/debit card resources and bargaining power — will act as 'an arbitrator' or 'judge' in the dispute and generally may find it difficult to act in a manner that an objective outsider would consider 'fair'.¹¹⁴² In most of the cases, banks rely on the bank's standard contract. This tends to give a one sided allocation of losses to the consumer (liability dumping). As long as the unauthorised ATM/debit card transaction is conducted using the correct consumer's card data and PIN, a bank will reject the consumer's claim — whether or not the bank can prove consumer negligence.

7.2.2.2. Flaws in the Banking Mediation Agency: Increasing the Disparity and Uncertainty.

Bank Indonesia's Banking Mediation/Facilitation Agency generally would be the next forum for ADR. However, although the BI banking mediation process is free of charge,¹¹⁴³ relatively rapid compared to judicial settlements,¹¹⁴⁴ and should be promoted and published by banks to their consumers,¹¹⁴⁵ its existence is still not recognised by most bank customers, as is shown in the results of the survey undertaken by the author.

¹¹⁴² Banks that don't have honesty and 'good will' will very easily conceal facts that can be of detriment to their position, such as by not giving the CCTV footage that records fraudsters' activities in the bank's ATM, or by arguing liability dumping clause in the banks-consumers agreement as an excuse, and/or accusing consumers to some extent undertaking a negligence act that enabled the phantom transaction in ATM/debit to occur. There was also the instance where one government bank refused to pay redress to the consumer even though they had confirmed the occurrence of identity theft conducted by third party that was not in any way associated with the consumer in their ATM booth. A bank may also use illegitimate reasons such as that by paying the claim the bank will trigger 'herd behaviour' by other victims, or that such a decision needs court verdicts, and that redress will be deemed by law enforcement to be corruption.

¹¹⁴³ However, in the event that customer or bank has the initiative to present expert witnesses, then the customer and bank have agreed to cover the expert witness expenses.

¹¹⁴⁴ Bank Indonesia Regulation Number: 8/5/PBI/2006 Concerning Banking Mediation as amended by Bank Indonesia Regulation Number: 10/1/PBI/2008 art 11: 'to avoid excessive time frame on the dispute resolution process, the process of mediation shall have been completed in no more than 30 (thirty) working days, with option to extend for another 30 (thirty) working days'.

¹¹⁴⁵ *Surat Edaran Bank Indonesia Nomor 7/24/DPNP Perihal Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Surat Edaran Bank Indonesia Nomor 10/13/DPNP* [Bank Indonesia Letter Number 7/24/DPNP Concerning Resolution of Customer Complaints as amended by Bank Indonesia Letter Number 10/13/DPNP]. According to this regulation, banks should publicise banking mediation as an alternative dispute resolution to its customers by providing the information in the form of leaflets, pamphlets, posters, booklets, website material, or other means of publicity in each of bank's branches, or send such information along with the results of any customer's complaint by letter to the customer's address.

From the interviews that the author conducted with 30 consumers from 6 respondent banks in Jakarta, Denpasar and Yogyakarta, only 5 of the 30 consumers had any knowledge about the BI banking mediation section as an alternative disputes resolution body in Indonesia.¹¹⁴⁶ These results are further supported by a recent payment card fraud survey by Bank Indonesia (BI-Fraud Survey).¹¹⁴⁷

Furthermore, the mediator provides neither recommendations to nor binding decisions on either party. In fact, many cases that are brought to Indonesia's Banking Mediation Agency by consumers are the same cases that have failed to be resolved on the first attempt at a bank's internal dispute resolution unit. However, again, the classic 'trump card' for banks in disputes with their consumers over unauthorised ATM/debit card transactions is the initial one-sided allocation of risk — the liability dumping clause in the bank–consumer standard contracts. Disputes were seemingly heavily resolved in favour of the banks who issued such contracts. In this contract, there are provisions that transfer a bank's liabilities to the consumer. Such provisions include, among other things, a rule that if a consumer's ATM/debit card data is compromised and used by fraudsters — regardless of whether the consumer has or has not any contribution to the fraud — the bank will have no liability for the consumer's damages.¹¹⁴⁸

As a result, in most of the cases, the dispute between banks and consumers over unauthorised ATM/debit card transactions in banking mediation agency have to be escalated to CDSB or court, because the mediation process failed to achieve an agreement or expected dispute resolution result from the consumer's perspective.¹¹⁴⁹ Even if the mediation succeeds — entirely or partially (in terms that a bank finally agreed to redress the consumer's loss) — often the reason behind the decision could not be treated as a legal guidance to resolve consumer disputes. Typically, the basis of the agreed mediation decisions was not a legal consideration but an act made at the discretion of the management of the bank involved concerning the consumer's status and/or condition. For instance, the victimised consumers that tend to have redress are those that are old or too poor (to avoid 'karma') or are prominent figures that have affiliation to the political party, religious organisation, the central bank, or are high

¹¹⁴⁶ C-1–C-30.

¹¹⁴⁷ See BI-Fraud Survey, above n 1133. From the BI-Fraud Survey on March 2015, of seven victims of ATM/debit card identity fraud, only two (29%) knew about the Banking Mediation/Facilitation Agency.

¹¹⁴⁸ See example of bank's liability dumping provisions at n 66.

¹¹⁴⁹ Heriani, above n 1049.

ranking police/military officials, and so on.¹¹⁵⁰ Therefore, banking mediation decisions have failed to establish a legal grip that can be used fairly in any bank–consumer dispute over unauthorised ATM/debit card transaction.

7.2.2.3. Flaws in the CDSB: CDSB’s Decision is not Final and Binding

The opportunity to file a lawsuit at a CDSB as a ‘last resort’ for out of court settlement has become the preferred choice for some bank consumers — who have noticed its existence — to settle their dispute with banks. The CDSB in general has been chosen by consumers that are reluctant to file a lawsuit directly with the court because of the many stigmas about launching court proceedings, and their inferior position in term of social and financial resources compared to business actors.¹¹⁵¹ In practice, all of the CDSB verdicts on unauthorised ATM/debit card transaction dispute were decided in favour of consumers. However, dispute resolution proceedings in the CDSB have their own problems for consumers.

From the author’s direct experience as an observer in the Mr Panggabean adjudication (processed in the CDSB), it has revealed that consumers are not able to force banks to settle their case in the CDSB if banks are not willing to do so.¹¹⁵² In a CDSB proceeding, arbitrators cannot unilaterally proceed and/or conclude the plaintiff’s claim, if the defendant disagrees with settling the dispute in the CDSB.¹¹⁵³ This situation differs from that of procedural law in the ordinary court of justice, where a judge can conclude the verdict in favour of claimant or plaintiff *in absentia*, even if a defendant refuse to settle the dispute in the court and/or refuse to attend the trial.¹¹⁵⁴ Hence, the CDSB dispute resolution benefits exist mostly only in theory, not in practice.

Nevertheless, apart from the flaws discussed above, another significant flaw relating to CDSB proceedings is the fact that the CDSB’s decision is not final and binding. Banks that are not satisfied with the CDSB decision have a legal basis for appealing to the

¹¹⁵⁰ Interview results from several Bank Indonesia Banking Mediation Body officers (BI-BMO) who requested anonymity: BI-BMO-1; BI-BMO-2.

¹¹⁵¹ Nugroho, above n 1082, 75, 85.

¹¹⁵² See text above n 1040 and Chapter Six / section 6.4.1 for complete story of the Mr Panggabean case.

¹¹⁵³ If one disputant party does not agree to resolve the dispute in the CDSB, the CDSB does not have jurisdiction to settle the dispute. Nowadays, there is tendency for more and more banks to refuse to settle their dispute with consumers in the CDSB forum and they prefer the dispute to be adjudicated in court. The logical explanation for this trend is that the bank is fully aware that most consumers who lack resources in terms of money, knowledge, and time will give up the case if the Court that notoriously is known as unpredictable, expensive, and corrupt becomes the forum of dispute settlement.

¹¹⁵⁴ See art 125 HIR (*in absentia/verstek*).

District Court — and this is what actually has happened in practice. Hence, all of the CDSB decisions on unauthorised ATM/debit card transaction disputes that have been decided in favour of consumers were in vain.¹¹⁵⁵ With all of these problems, the purpose of CDSB establishment — as a rapid, inexpensive, fair and final forum for alternative dispute resolution body — has unfortunately not yet been achieved.

7.2.2.4. Flaws in the Court: Unjust Contributory Negligence Principle

The resolution of disputes between banks and consumers usually end up at the court of justice as a final adjudication forum.¹¹⁵⁶ It is argued, however, that court decisions were almost always in favour of banks, contained many flaws, were inconsistent, and generally had a weak legal basis. These verdicts apparently confirm people's accusations that courts are unprofessional in handling business disputes,¹¹⁵⁷ unfair, and unresponsive to the needs of plaintiff.¹¹⁵⁸ As Shofie, Anderson and other scholars assert, many lawyers and judges mostly have a background in the humanities rather than the sciences and have knowledge that is too generalist, so when it comes to complex problems related to banking, technical evidence, and in particular of computer evidence, evaluation and decision-making are fraught with difficulties.¹¹⁵⁹ Hence, it is argued that 'misleading' decisions have occurred because adjudicators were only using 'common sense' without being supported by sufficient knowledge and empirical evidence.

The 'common sense' approach by the adjudicators and/or court judges also proves to be confusing because they do not examine nor consider the economic, technological and regulatory aspects that indeed are entwined in ATM/debit card transactions. This situation is also exacerbated by many other factors such as the adjudicators'/judges' and

¹¹⁵⁵ CDSB outcomes tend to always favour consumers. Actually, this is not surprising since the spirit of the establishment of the CDSB was to help consumers, who in general are far weaker than business actors (for example, in terms of knowledge, financial strength, and human resources). The spirit to defend consumers also is derived from the latest development of consumer protection doctrine (doctrine of *caveat venditor* — 'let the seller beware') which is employed in many countries' consumer protection regulations, including Indonesia. For more complete information about consumer protection principle and regulations in Indonesia, see Chapter 5.3.

¹¹⁵⁶ See Chapter Six / section 6.4.3.2.2.

¹¹⁵⁷ Unauthorised ATM/debit card transaction disputes are probably even more difficult for the judges because they involve more complex matters, including multifaceted and seamless bank infrastructures and technology security aspects.

¹¹⁵⁸ See explanation in Chapter Six, section 6.4.3.3.2.

¹¹⁵⁹ Shofie, '*Kapita Selektta Hukum Perlindungan Konsumen di Indonesia*', above n 683, 30–2. See also Ross J Anderson, 'Liability and Computer Security: Nine Principles' in *Computer Security—ESORICS 94* (Springer, 1994) 231; Nugroho, above n 1082, 127–8. See also Bevan, above n 1060, 17; Shofie, *Perlindungan Konsumen dan Instrumen-Instrumen Hukumnya*, above n 1118, 359–62; Nurdin, above n 155, 237–60.

payment system industry stakeholders' lack of knowledge about the taxonomy of ATM/debit card identity theft/fraud methods, trends and developments in fraud liability or loss allocation rules, and consumer protection in many developed countries. However, the most blunders from these adjudicators' decisions probably derive from the use of an old, abandoned, and unfair contributory negligence doctrine in the dispute between banks and consumers, as the way of adjudicators in articulating general loss allocation rules embodied in the existing legislation.

As a consequence, court judges always accede to a bank's defence which argues in terms of the infallibility of bank's ATM/debit card system (which actually is anecdotal),¹¹⁶⁰ the existence of consumer contributory negligence (which omits the part played by bank negligence (such as by its failure to safeguard its ATMs from interference by a fraudster's malicious software and/or devices), ready acceptance of bank assurances of the 'adequacy' of its consumer education, and/or the validity of the bank's liability dumping provision in its bank-consumer contract. In contrast, in the United States, a bank's claim that its systems were infallible, was rejected by the court since it placed 'an unmeetable burden of proof' on the plaintiff.¹¹⁶¹ It is argued that unfair approaches by banks and courts to the victimised consumers can discourage banks from developing sufficient security measures and playing their appropriate part in the development of a secure and robust payment system in Indonesia.

All in all, court rejections of consumer claims for redress where consumers probably only have made a small mistake or demonstrated slight negligence and were the true victim of the fraud are unfair for consumers and to some extent could jeopardise consumer trust in the banking industries and reduce incentives for banks to improve their security systems. Hence, there is always a risk that an inadequate and unfair legal framework in terms of loss allocation rules for unauthorised ATM/debit card transaction will come to erode consumer confidence in card-based payment in Indonesia.¹¹⁶²

¹¹⁶⁰ See Anderson, above n 1159.

¹¹⁶¹ Ibid. Anderson stated that:

In the landmark court case *Judd v Citibank* [JC], Dorothy Judd claimed that she had not made a number of ATM withdrawals which Citibank had debited to her account; Citibank claimed that she must have done. The judge ruled that Citibank was wrong in law to claim that its systems were infallible, as this placed 'an unmeetable burden of proof' on the plaintiff. Since then, if a US bank customer disputes an electronic debit, the bank must refund the money within 30 days, unless it can prove that the claim is an attempted fraud.

¹¹⁶² It is an undisputed fact that consumer confidence is vital to the success of a bank's electronic payment system and to the economy in general.

Nevertheless, it is unsurprisingly that most of these adjudicator decisions failed to shed light on how to satisfy the quest for a fair, predictable, and sensible decision in a dispute between bank and consumer over an unauthorised ATM/debit card transaction. If this situation persists, it is feared that it will not only cause pecuniary and non-pecuniary loss for innocent victimised consumers, but also will jeopardise consumer trust in the banking industry as a whole.

In light of the unfortunate situations detailed above, it is submitted that legal reform of loss allocation rules for fraud liability law in Indonesia — to resolve prolonged disputed and unjust adjudication verdicts on unauthorised ATM/debit card transaction — is undoubtedly needed and immediately relevant.¹¹⁶³ The existence of a clear, fair, detailed, and decisive legal framework for loss allocation is a very important aspect of improving legal certainty, reducing time and expenses for dispute resolution, and increasing predictability in regard to results of disputes regarding unauthorised ATM/debit card transactions. It is believed that the introduction of such a framework could encourage disputant parties to settle the dispute between them autonomously, and also improve consumer trust and reduce reputational risk for bank. Morse and Raval also argue that it could also effect better development of the payment systems in the country in question.¹¹⁶⁴

However, Indonesia does not have a formal law reform agency (such as the Australian Law Reform Commission in Australia¹¹⁶⁵ or the Institute for Legal Reform in United States),¹¹⁶⁶ hence, it is hoped that this thesis can act as an individual initiative to

¹¹⁶³ According to *Black's Law Dictionary*, law reform is the process of, or a movement dedicated to, streamlining, modernising, or otherwise improving the nation's law generally or the code governing a particular branch of the law. What is meant by law reform in this thesis is the process by which the fraud liability law — that is too general and does not really cater for banks' electronic transactions — is to be modified, modernised, and supplemented. This law reform aims to improve access for consumers to justice, remove unjust and obsolete legal doctrine utilised in the adjudication process, and eliminate defects and problems that used to occur in dispute resolution between banks and consumers on unauthorised ATM/debit card transactions. In considering options for law reform, it is argued that the proposed legal framework for loss allocation rules in Indonesia needs to be harmonised with prevailing well-known standards in other countries.

¹¹⁶⁴ Morse and Raval, above n 44, 543. See also CPSS, 'Clearing and Settlement Arrangements for Retail Payments in Selected Countries', above n 245, 11–12.

¹¹⁶⁵ See *Australian Law Reform Commission* (2015) Australian Government <<http://www.alrc.gov.au/>>. The Australian Law Reform Commission is a federal agency that reviews Australia's laws to ensure they provide improved access to justice for all Australians by making laws and related processes more equitable, modern, fair and efficient.

¹¹⁶⁶ *Institute for Legal Reform* (2014) U.S. Chamber of Commerce <<http://www.instituteforlegalreform.com/>>. The U.S. Chamber institute is an advocacy group founded in

influence the payment system authority (Bank Indonesia) and payment system industry at large (banks, switching company, consumer protection body, CDSB, courts, and so on) to undertake law reform and raise public awareness of the practices of the current poor and unjust fraud liability law and loss allocation rules on unauthorised ATM/debit card transactions in Indonesia.

7.3. Multi-Disciplinary Approaches to Law Reform on Loss Allocation Rules concerning Unauthorised ATM/Debit Card Transactions in Indonesia: Economic, Technological, and Legal Perspectives

The severity of fraudulent activities is sometimes exacerbated by consumer negligence or fault, or — probably more appropriately — the consumer’s lack of knowledge (in contrast to that of the bank) about various identity theft/fraud methods that are used to attack bank consumers in ATM/debit card transactions. This asymmetry of information typically is derived from a lack of bank consumer education about inherent vulnerabilities and common method of frauds on ATM/debit card operation. This is confirmed in the author’s interviews with the victims of unauthorised ATM/debit card transactions. All victimised consumers are consumers that typically never had received enough knowledge from their banks about identity theft/fraud methods and how to avoid them. In contrast, consumers that attempted to take measures so as to not fall prey to such crimes are consumers that to some extent noticed or have knowledge — mostly from mass-media/social media (rather than their bank) — about how the identity theft/fraud method worked and the consequences if they fall for it.¹¹⁶⁷ Nevertheless, there is always a possibility that the consumer is the fraudster itself/dishonest consumer.

In general, laws, market practices, and/or the consumer precautions can contain risk in electronic payment systems.¹¹⁶⁸ More specifically, risk containment in payment card fraud may be addressed by fairly allocating the losses among the parties involved in the transactions.¹¹⁶⁹ The existence of good fraud loss allocation rules is not only important because of their distributional consequences, but also is believed to give incentives to all parties involved in the ATM/debit card transaction to improve their precautions and

1998 by the United States Chamber of Commerce representing the nation’s business community with a focus on tort reform.

¹¹⁶⁷ See interviews with bank consumers C-1–C-30.

¹¹⁶⁸ Board of Governors of the Federal Reserve System, above n 190, 38.

¹¹⁶⁹ Hayashi, Sullivan and Weiner, above n 199, 100–101.

necessary efforts to prevent and/or mitigate the possible occurrence of identity theft and/or fraud.¹¹⁷⁰

The precaution element basically can be assigned to both parties regardless of the size and nature of the party. In order to achieve an efficient legal system, fraud loss liability should be assigned to the party under their specific payment system transactions circumstances, and be one that 'is able to take precaution against the loss at the lowest cost'.¹¹⁷¹ Financial institutions and consumers can reduce payment losses by taking precautions against fraud according to their own specific circumstances and capabilities.¹¹⁷²

Besides that, clear and fair loss allocation rules can also create a far higher degree of certainty regarding results as to who should be liable for unauthorised ATM/debit card transaction loss. Such certainty would encourage the liable party to take adequate precautions either to prevent the risk from occurring or to mitigate the risk if it still occurs regardless of the safety measures taken.¹¹⁷³ Thus, the rules can be expected to encourage behaviour from the parties involved in the ATM/debit card transaction to minimise identity theft/fraud occurrence to the ATM/debit card system as a whole.

Considering the fast and complex development of electronic fund transfer system (such as ATM/debit card transactions), inherent vulnerabilities of ATM/debit card infrastructures, rapid innovation, adaptation, and development of crime/fraud risk, asymmetry of information between banks officers/fraudsters and consumers, and weak legal protection on consumers in the event of unauthorised ATM/debit card transactions in the bank-consumer contract provisions, general fraud liability regulation, and in its adjudication practices — it is submitted that multi-disciplinary approaches to establish the fraud liability rules is necessary. These should include legal, economic, and technological aspects that are heavily involved in the bank ATM/debit card transactions.

It is submitted in this thesis that the use of multi-disciplinary approaches will benefit law reform in Indonesia in creating clear, fair, detailed, and decisive loss allocation rules for unauthorised ATM/debit card transactions, because such approaches will consider many different but relevant aspects that are involved in unauthorised

¹¹⁷⁰ Levitin, above n 114, 3. See also Gillette, above n 130, 189.

¹¹⁷¹ Cooter and Rubin, above n 105, 74, 84.

¹¹⁷² Ibid 73.

¹¹⁷³ Rusch, above n 106, 595.

ATM/debit card transactions. It is believed that by having clear, fair, detailed, and decisive loss allocation rules for unauthorised ATM/debit card transactions, incentives will be created for payment system stakeholders to improve their ATM/debit risk precautions and/or prevention and mitigation performance. It will also encourage disputant parties to settle their disputes concerning unauthorised ATM/debit card transactions more efficiently between themselves in accordance with the reformed loss allocation rules. Hence, any dispute resolution adjudicated — whether within a bank's dispute resolution unit, ADR forum and/or court in the future — can be settled faster, inexpensively, and more predictably, and could certainly reflect the presence of justice, efficiency and legal certainty for the disputant parties.

7.3.1. Economic Perspective: Facts and Principles

According to the CPSS, risks such as fraud, operational and other risks in the retail payment system 'are generally addressed through technical features of various payment instruments and system control'.¹¹⁷⁴ Even though banks as professional entities have much information about security threats to their retail payment system,¹¹⁷⁵ typically bank management generally does not take elaborate and costly security measures for retail payment system such as they would for the wholesale payment system. Bank management typically will consider that it would be far too expensive, involve longer processing times, or otherwise not be suitable for the retail payment system.¹¹⁷⁶ The retail payment system with its larger number of participants generally employs a more moderate security system (having to adapt to the technology owned by the participants who are very diverse — not only domestic but also international participants). Bank management decisions over their infrastructure and security for ATM/debit card operation always contain a trade-off between a bank's increased profit oriented economic objective and reluctance to have 'excessive' investment on bank security infrastructure (which could reduce those profits).

¹¹⁷⁴ CPSS, *Clearing and Settlement Arrangements for Retail Payments in Selected Countries*, above n 245, 1.

¹¹⁷⁵ Every bank in Indonesia has a risk management unit, one task of which is to update the information about various threats that could compromise bank security. The information can be obtained from various sources, such as various local/international conferences concerning payment system fraud/computer security risks; security risk information mailing lists from various banking security institutions, international ATM organisations, consumer fraud incident reports, the central bank, information exchange between banks, fraud reports from particular central bank/payment organisations, and so on. Most of the time, the type of identity theft and fraud that happens in one region (such as in Europe or the US), soon typically will also happen inside Indonesia.

¹¹⁷⁶ Roberds, above n 265, 43.

From the discussion in the previous chapters, some evidence is given of how a bank's economic considerations have overpowered technological and legal requirements to provide optimum security and consumer protection in the ATM/debit card operation. These include, among other things:

- Banks not having equipped all of their ATM/debit card infrastructure with state-of-the-art technology, such as chip technology capability, anti-skimmer sensor and anti-card-trapping automatic sensor;
- Banks not having equipped each of its ATMs/ATM booths with CCTV cameras. And even where CCTV does exist, some of them exhibit many issues concerning recording quality and/or retention or duration or the recording;
- Despite the fact that many instruments and incidents of fraud are present or occur at a bank's ATMs/ATM booths — including card swapping, card trapping, and card skimming, presence of fake call centre stickers, use of PIN-hole camera, and PIN-pad overlays — banks to some extent exhibit a serious deficiency in monitoring their ATMS/ATM booths either by using active surveillance technology or more frequent physical monitoring, or by placing a security guard;
- Banks having deliberately 'accepted' dangerous and illegitimate merchants double swiping practices;
- Banks only being keen to give 'positive consumer education' and reluctant to give 'negative consumer education' about inherent fraud risk methods on ATM/debit card transactions;
- Banks having adopted a liability dumping policy in their bank–consumer standard contract which reflects bank reluctance to redress consumer losses due to unauthorised ATM/debit card transactions.

The connection between law and economics has been known for quite a long time. Each impacts to a varying degree upon the other. Descriptions of the relationship can be broadly categorised into two groups namely 'law and economics' and 'economic analysis of law'.¹¹⁷⁷ In general, the term 'law and economics' focuses on economic problems, and legal rules are only utilised as a tool to resolve market failure

¹¹⁷⁷ Geoffrey P Miller, 'Law and Economics versus Economic Analysis of Law' (2011) 19(2) *American Bankruptcy Institute Law Review* 459, 459. See also Richard A Posner, 'Values and Consequences: An Introduction to Economic Analysis of Law' (The University of Chicago Law School, 1998) 1; Alain Marciano and Giovanni B Ramello, 'Consent, Choice, and Guido Calabresi's Heterodox Economic Analysis of Law' (2014) 77(2) *Law and Contemporary Problems* 97, 97.

problems.¹¹⁷⁸ Meanwhile, ‘economic analysis of law’ denotes an economic method or the tools that can be used by legal and policy practitioners to analyse in positive and normative sense any kind of problem in order to make decisions and understand the working of the legal system, including in the adjudication process,¹¹⁷⁹ or in the law reform process.¹¹⁸⁰ In short, economic analysis of law ‘is the use of economic principles and reasoning to understand legal materials’.¹¹⁸¹

In general, economic analysis of law can be used to see and predict the effect of the law on the participant’s behaviour; and/or to improve law by highlighting the negative consequences of the law in one or more aspects, such as in terms of economic efficiency, or the distribution of income and wealth, or other values.¹¹⁸² In its development, the economic analysis of law not only came to focus on areas of law which have economic objectives, but also on all areas of the law, such as family, crime, procedural, contract, tort, crime, institutions, and the payment system.

In recent times, many economists in the modern law and economic tradition have been attracted to seeing the relation of economic and law, especially in the quest to achieve efficient social goals by utilising lawmaking and judicial rulings.¹¹⁸³ Economic analysis of the law starting to emerge in 1960s and has been advocated by several prominent scholars in their seminal works. These include Ronald Coase in his article “The Problem of Social Cost”, and Guido Calabresi with his article about risk distribution and tort.¹¹⁸⁴ However, it was Richard Posner at the beginning of 1970 who formally ‘invented’ the economic analysis of law with a general text book on economic analysis of law and the establishment of the *Journal of Legal Studies*.¹¹⁸⁵ In the payment system area — especially on the loss allocation for consumer payments — Robin and Cooter’s

¹¹⁷⁸ Marciano and Ramello, above n 1177, 97–8.

¹¹⁷⁹ Sophie Harnay and Alain Marciano, ‘Posner, Economics and the Law: From “Law and Economics” to an Economic Analysis of Law’ (2009) 31(2) *Journal of the History of Economic Thought* 215, 215–26, 229. See also Miller, above n 1177, 459.

¹¹⁸⁰ Hamay and Marciano, above n 1179, 226. See also Posner, above n 1177, 2.

¹¹⁸¹ See Miller, above n 1177, 459. See also Cento Veljanovski, *Economic Principles of Law* (Cambridge University Press, 2007) 1. In his book, Veljanovski denotes economic analysis of law as the economic approach to law.

¹¹⁸² Posner, above n 1177, 2. See also Veljanovski, above n 1181, 1; Marciano and Ramello, above n 1177, 98.

¹¹⁸³ Enrico Colombatto, ‘A Free-Market View on Accidents and Torts’ (2014) 77(2) *Law and Contemporary Problems* 117, 117.

¹¹⁸⁴ Guido Calabresi, ‘Some Thoughts on Risk Distribution and the Law of Torts’ (1961) 70(4) *The Yale Law Journal* 499. In this article, the central policy issue is whether the basic criterion of liability is to be based on personal or individual fault or negligence or a wide distribution of risk and loss.

¹¹⁸⁵ See Posner, above n 1177, 1–2. See also Veljanovski, above n 1181, 3–5.

seminal article on loss allocation between consumers and financial institutions¹¹⁸⁶ stands out and has become a prominent reference for many countries' payment system loss allocation rules, including the *EFT Act 1978* in United States and the Australian ePayments Code. They believed that 'applying economic analysis to loss allocation in the payment system leads to a set of recommended rules that are fairly close to legislation championed by consumer interests'.¹¹⁸⁷

It is submitted that this thesis also advocates the use of Cooter and Rubin's loss allocation principles, namely 'loss spreading', 'loss reduction', and 'loss imposition',¹¹⁸⁸ as tools that can assist in resolving unauthorised ATM/debit card transaction disputes between consumers and financial institutions. Cooter and Rubin believed that applying economic analysis to loss allocation in the payment system is appropriate since loss allocation in the payment system is related to a technical and largely monetary subject, and also could lead to the creation of comprehensive loss allocation rules that could safeguard consumer interest.¹¹⁸⁹

The principles are believed to be able to enrich legal considerations in the fraud liability law reform process in Indonesia, either in terms of creating clear, fair, detailed, and decisive loss allocation rules in the regulations and/or by resolving disputes more fairly between banks and their consumers regarding unauthorised ATM/debit card transactions. Cooter and Rubin's work also stated that the concept encompassed a wider range of matters than the valuable concerns that were expressed in Calabresi's earlier seminal article.

7.3.1.1. Loss Spreading Principle

In this principle, Cooter and Rubin argued that in regard to pertinent risk in payment system, it is better to assign liability for a loss to a financial institution instead of to an individual consumer. Financial institutions are believed to be the most appropriate party that can achieve risk neutrality at the lowest cost by spreading the loss across the entire group of customers and consumers. However, as Rusch pointed out, 'A loss spreading

¹¹⁸⁶ Cooter and Rubin, above n 105. In this article, Cooter and Rubin argue that economic approach on payment system is justified since loss allocation in the payment system is technical and largely monetary subject, hence economic analysis will be deemed appropriate and indisputable.

¹¹⁸⁷ Cooter and Rubin, above n 105, 66.

¹¹⁸⁸ Ibid. The article deals only with losses due to fraud, forgery and error. However, for the purpose of this thesis, the Cooter and Rubin loss allocation principles are only used for losses due to fraud in ATM/debit card transactions.

¹¹⁸⁹ Ibid.

rationale would accept the level of unauthorized debits as a cost of doing business and would not necessarily foster any incentives or realistic opportunities to decrease the cost of operating the payment system as a whole'.¹¹⁹⁰

In general, financial institutions obviously have greater economic resources compared to consumers. Financial institutions can predict their revenue and exposure to loss from the intermittent occurrence of fraud. Subsequently, the loss then can be spread among their consumers in the form of a charge for their products and services. Example of such charge is the fee for the use of a bank's ATM and EFTPOS machines for a financial transaction, a fee for bank account administrative costs, a fee from interbank fund transfers using clearing or wire transfer (RTGS), credit card interest, and so on. Another reason is that a financial institution does not have a deleterious asymmetric information issue about inherent fraud risk in the payment system operation. On the other hand, most individual consumers do not have sufficient resources to bear the loss incurred and typically have taken no precautions whatsoever against fraud risk due to the problem of asymmetric information about inherent risk in the ATM/debit card operation.¹¹⁹¹ Therefore, the loss spreading principle definitely attributes liability for payment losses to financial institutions instead of consumers.¹¹⁹²

7.3.1.2. Loss Reduction Principle

Unlike the loss spreading principle that tends to place the burden of loss on the financial institution's shoulders, the loss reduction principle principally can be assigned to financial institution and/or consumers as parties involved in the payment system transaction that have ability to reduce fraud losses at the lowest cost. Liability is a useful incentive for the parties involved in the payment system transaction to induce precautions and/or innovations against fraud. Principally, both or either financial institutions and/or consumers can avoid or prevent payment losses.¹¹⁹³

This principle is considered more complex, because its purpose deals with human behaviour, which tends to change over time and probably has different standards of

¹¹⁹⁰ Rusch, above n 106, 592, 561.

¹¹⁹¹ Cooter and Rubin, above n 105, 70–3.

¹¹⁹² Ibid 66.

¹¹⁹³ Ibid. See also Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 211.

behaviour among participants.¹¹⁹⁴ Other than this, fraud methods are varied and witness different levels of parties' involvement and/or degrees of negligence/fault that enable the fraud to happen. In the event that more than one party can reduce the losses, the imposition of loss allocation rules should achieve balance and could avoid moral hazard in its implementation. Cooter and Rubin stated that the 'paradox of compensation' should be avoided. That is, '[h]olding one party strictly liable for a loss erodes the other party's incentive to take precaution and to refrain from any action that would increase the loss'.¹¹⁹⁵ As a solution to this problem, Cooter and Rubin affirm that from an economic analysis perspective, fault-based liability rules are an answer to the paradox, even better than strict liability rules:

Any fault rule, including simple negligence, negligence with contributory negligence defense, and comparative negligence, will motivate one party to satisfy the legal standard of fault in order to avoid liability, while inducing the other party to take precaution because it must bear any residual responsibility of the loss.¹¹⁹⁶

7.3.1.3. Loss Imposition Principle

While the loss spreading and loss reduction principles focus on the assignment of liability to the parties involved in the payment system transaction, the loss imposition principle's centre of attention pertains to the enforcement in the most efficient way of the assigned liability rules agreed by the payment system industry/authority. Given the inefficiency and expensive process in place for payment system participants to settle fraud liability disputes in court civil suits, criminal trials, administrative proceedings, and ADR currently, it should be noted that to achieve ultimate efficiency, the enforcement of loss allocation process should be simple, efficient, and cheap.¹¹⁹⁷

If existing loss allocation rules are unjust and/or not comprehensive (that is, tends to be inefficient and/or unfair for one or more participant in the payment system), reallocating loss with simple, clear, fair, detailed, and decisive liability rules and an efficient adjudication mechanism are undoubtedly very important. This approach is deemed necessary to improve certainty and predictability in the fraud liability dispute resolution, simplify adjudication proceedings, and discourage disputant parties from bringing their

¹¹⁹⁴ Cooter and Rubin, above n 105, 73.

¹¹⁹⁵ Ibid 74.

¹¹⁹⁶ Ibid.

¹¹⁹⁷ Ibid 78. According to Cooter and Rubin, 'the loss imposition principle [is] designed to avoid costly litigation and to overcome under enforcement, especially for small losses by consumers'.

dispute to ADR and/or court, a process that — in the case of Indonesia — notoriously exhausted parties' valuable resources such as money, time and effort.¹¹⁹⁸

Cooter and Rubin stated that selecting a basic mechanism to establish clear, fair, detailed, and decisive liability rules is not difficult: 'strict liability rather than fault-based liability, single factor standards rather than multiple factor standards, objective rather than subjective tests, and statutory liquidated damages rather than damages based on individualized determination of loss' are what they suggest.¹¹⁹⁹ However, all these choices demonstrate a trade-off, especially for an ATM/debit card payment system that relies on both banks and consumers for fraud containment. For instance, while loss allocation rules using strict liability are easy to administer compared to fault/negligence-based liability that tends to be complicated and probably more expensive in its determination process,¹²⁰⁰ there are problems. Strict liability only provides a rough allocation of liability to one party and probably discourages the other party from taking precautions against fraud risk; whereas fault-based liability provides precise loss allocation rules for both parties according to their specific circumstances and capabilities for reducing or preventing fraud losses, but this approach also has drawbacks in terms of economic costs.¹²⁰¹

7.3.2. Technological Perspective: Facts and Principles

In general, banks always anecdotally state that their systems are infallible. In reality, however, there is much evidence to the contrary. Examples of this can be seen in several unpublished Bank Indonesia documents on its payment system supervision of the banks' payment card systems. It was found that some bank systems were actually vulnerable to identity theft/fraud. For instance, the internal audit document of one bank admitted that there was no segregation of duties regarding consumer data within different bank departments; consumer data was stored as plain data without adequate security and/or encryption; and even worse, many staff could access data without a

¹¹⁹⁸ Ibid 78–83. Compared to banks that have strong and excellent resources, consumers are always intimidated by many problems such as high cost from lawyer's charges, difficulties in collecting documentary evidence, and long duration of adjudication process, especially for litigation in the court of justice. With the non-existence of small claim court in Indonesia, sometimes civil suit in the court is not a popular option for unauthorised ATM/debit card victimised consumers, since the court's litigation expenses and hassle may outweigh the monetary value of the consumer's claim.

¹¹⁹⁹ Ibid 78.

¹²⁰⁰ Ibid 85. According to Cooter and Rubin, 'the overall cost of imposing fault-based rules invariably will exceed the advantage gained in loss reduction'.

¹²⁰¹ Ibid 78–9.

password or authorisation. Other than this, data storage inside magnetic stripe in consumers' ATM/debit card are all in plain text without any security protection, and therefore very easy to copy and be subjected to abuse by internal or external fraudsters. Not to mention the threat from malware and eavesdropping method by which fraudsters can cleverly steal or intercept consumer ATM/debit card transactions by exploiting even slight vulnerabilities in a bank's system.

In order to create fair, robust, and objective loss allocation rules for payment card transactions, it is necessary for the law reformer in Indonesia to at least identify and understand — from a technological point of view — various aspects of identity theft and fraud in ATM/debit card operations. It is submitted that knowledge of how various identity theft and fraud risks may arise or be transmitted within the payment card system determine where they are borne (point of compromise) and who are the likely perpetrators is extremely important for the law reform process.

While ATM/debit card payment seems seamless to the consumer, the system itself in fact requires complex technology which most users or cardholders do not understand. Payment cards with chip and/or magnetic stripe technology as data container, consumer activated terminals such as ATM and EDC machines, a communication network that links the consumer activated terminal either directly or indirectly (via another bank's and/or switching company infrastructure) to the host bank computer and infrastructure, are some examples of the heavy involvement of information technology features utilised in the bank's ATM/debit card system.¹²⁰²

As has been described previously, in the ATM/debit transactions vulnerabilities lie almost at every transaction point from its inception until its settlement.¹²⁰³ From the basic identity theft/fraud typology on a consumer ATM/debit card transaction discussed earlier in the Chapter Four and section 7.4.1 above, generally fraudsters attack either a bank's infrastructure (technology), process/procedures, and/or the consumer. That is, a bank and its counterparts, their infrastructure computer and such infrastructure as ATM/EDC/EFTPOS machines, and networks, transaction process or procedures (where bank, merchant, switching company and other bank's counterpart owner/employee

¹²⁰² See Chapter Two for details about technology and infrastructures employed in the ATM/debit card operation such as ATM/debit card, magnetic stripe, chip, ATM/EFT machines, EFT network, and so on.

¹²⁰³ CPSS, 'Clearing and Settlement Arrangements for Retail Payments in Selected Countries', above n 245, 11–12. See also FFIEC, 'Retail Payment Systems', above n 180, 24.

could become a perpetrator of identity theft/fraud) or bank and/or its counterpart databased computer, and the consumer itself — could become ‘the weakest link in the chain’. The fraudster typically will attack the ‘weakest link’ as a point of compromise for identity theft, which typically later is transformed into identity fraud.

Pertaining to the threat of identity theft and/or identity fraud in the bank’s ATM/debit card operation, banks all over the world (including in Indonesia) have developed various risk management measures — including consumer education — to fight the occurrence of such theft/fraud. Unfortunately, unlike scheme credit card operations which are relatively advanced in terms of security features (with the implementation of chip card based on EMV standard), the ATM/debit card system in Indonesia at the moment still only relies on magnetic stripe card technology. Hence, from a technological point of view, ATM/debit card transactions are very vulnerable to various identity theft methods such as skimming at ATM/EFTPOS terminal, card trapping at ATMs, double swiping at merchants, waitress attack in the restaurant, malware in ATM/EFTPOS machines, eavesdropping in the communication line or node, and so on. From a technological point of view, expecting consumers to act vigilantly to spot the fraudster’s malicious devices are — in regard to most of the fraud occasions — absurd, due to the consumers’ false sense of security and trust in the ATM/debit card operation, and also the fact that the nature of fraudsters’ malicious devices makes them difficult or impossible to detect by untrained eyes of consumers as laypersons, especially in the absence of fraud risk education by banks.

From empirical evidence, some unauthorised ATM/debit card transactions are due to consumer negligence, but others are not. Indeed, because of a consumer’s negligence fraudsters may assume control of the consumer’s card and PIN and initiate an unauthorised ATM/debit card transaction. Anderson even contends that most frauds are due to blunders in application design, implementation and operation.¹²⁰⁴ Other than this — regardless of consumer’s negligence and given the extent and frequency of the breach of banks and their counterpart institutions infrastructure that contains consumer payment card data and PIN — unauthorised ATM/debit card transactions that occur because of hacker activity are probably far more frequent compared to instances of negligence by consumers.

¹²⁰⁴ Anderson, above n 1159.

However, even though a number of banks in Indonesia have enhanced some of their ATM/debit card operations — with the installation of various additional security features such as anti-skimmer devices and/or jitter at the ATMs, CCTV, and placement of ATM security tips stickers in several ATM booths, and so on — nevertheless, fraudsters on many occasions have succeeded in defrauding consumers' ATM/debit transactions. As evidence of this, from time to time there is news about ATM/debit card frauds that has caused significant monetary damages to consumers and/or banks. These references are found in the mass-media either in articles on fraud and/or fraud claims in a 'readers column'. Even though not very complete, Bank Indonesia's annual payment system report also confirmed the existence of identity theft and fraud on ATM/debit card transaction and the losses sustained by consumers.¹²⁰⁵

The inherent vulnerabilities in a ATM/debit card system might exist in various aspects of the ATM/debit card operation, such as people, processes, and technology. If a bank improves their security features (prevention and/or mitigation enhancement), it and its consumers may not necessarily be exempt from fraudster attack. It has been asserted by Greene in his 'balloon effect' theory¹²⁰⁶ that fraudsters almost always find new ways to circumvent and/or evade a bank's security features and steal consumer data (identity theft) to ultimately perpetrate unauthorised ATM/debit card transactions (identity fraud).

The plan of Bank Indonesia — Indonesia's Central Bank — is in the near future to oblige all banks in Indonesia to implement as standard a requirement for the introduction of domestic proprietary chip technology in their ATM/debit card system. Even though it is believed that this will reduce identity theft and fraud, it is not regarded as a universal panacea. Payment card equipped infrastructure such as ATM/debit card and its processing devices such as ATM/EFTPOS with chip capable technology could indeed now defend consumer ATM/debit cards from the risk of identity theft using skimming method.¹²⁰⁷ However, even these are still not infallible, as they are vulnerable to malware and skimming attacks that target consumer data within the ATM/debit

¹²⁰⁵ See Direktorat Akunting dan Sistem Pembayaran and Departemen Pengelolaan Uang, '*Laporan Sistem Pembayaran Dan Pengelolaan Uang 2012* [Payment System and Cash Management Report 2012]' (Bank Indonesia, 2012), 44.

¹²⁰⁶ See Chapter Three / section 3.3.1.3 to understand more about the 'balloon effect' theory.

¹²⁰⁷ Until recently, consumer data recorded in the payment card's chip was relatively secure from skimming attack thanks to many security layers, such as tamper resistant smart card design, cryptographic protocols, on-line authorisation transactions, and specific operating system.

card's magnetic stripe on the back of bank's chip card.¹²⁰⁸ Other than that, when faced by various identity theft methods that target the consumer's genuine card — such as card swapping, card trapping, lost and stolen card (including swallowed card theft in the ATM), and so on — the chip card itself is as vulnerable as old magnetic stripe card.

Like the economic principles that can be utilised as explanatory tools to rationalise or comprehend existing fraud liability rules and the adjudication decisions in the disputes between banks and their consumers over unauthorised ATM/debit card transactions, a technological perspective can also be very helpful to shed the light on the questions such as where was the exact location of the identity thefts occurred (point of compromise), what kind of fraud method and malicious devices were employed, and who was the most likely the perpetrator. Therefore, it is submitted that by knowing the answers to these questions, it is easier for the payment system stakeholders to find the party that is supposed to be responsible for safeguarding consumer ATM/debit card transactions. Professor Mann is probably one of the mostly prominent scholars in the area, and he believes that the question about who bears the risk of unauthorised transaction often should be resolved based on the nature of the underlying technology.¹²⁰⁹

7.3.2.1. Banks' Moderate Security Technology against Flaws and Vulnerabilities in ATM/Debit Card Operation

Actually, banks probably can make their ATM/debit card operation nigh 'infallible', if they implement the most recent and sophisticated security features technology. For instance, by employing chip technology for ATM/debit cards and public key infrastructure and/or biometrics as an authentication tool in place of the static and fragile PIN, and leasing line infrastructure for communication data between consumers activated terminal and bank's data centre, banks would increase their consumer data security. However, even though this approach probably enhances consumer transaction security, due to the nature of the retail payment system nature which involves a great

¹²⁰⁸ The magnetic stripe media is still provided in the chip card as a data 'back up' if the consumer activated terminal still has no capability to process chip card technology. The payment card industry actually noticed that the existence of magnetic stripe media in the chip card reduced 'the infallibility' of the state-of-the-art chip card technology. However, this decision is driven by the need of the payment card stake holder (issuer, acquirer, principal, etc) to ensure optimum fee based income to be generated from card transactions and by user demand for functionality, since not all countries has embraced chip card - EMV technology standard.

¹²⁰⁹ Ronald J. Mann, 'Making Sense of Payments Policy in the Information Age' (2005) 93 *Georgetown Law Journal*.

number of consumers, bank infrastructure such as ATM and EDC/EFTPOS machines, bank counterparts' supporting parties (that is, network, hardware and/or software vendors, and switching companies) and domestic/international inter-operability, this option probably will be difficult to implement due to an excessive time, effort, and investment requirements, and probably will be contrary to the demand for user convenience and to business requirements, especially in the short to medium term.

Therefore, up until now banks prefer to choose a business approach with only moderate security (and commensurate low/moderate costs) in ATM/debit card operations. Meanwhile, educating consumers with exhaustive fraud risk information is also not an option for many of Indonesia's banks, since it is believed (at least anecdotally) that this will reduce consumer confidence and hence bank revenue from fee-based transactions.

Therefore, in reference to all of the above situations, it is submitted in this thesis that banks in Indonesia need to be more specific, actually conscious and aware that consumer security in bank ATM/debit card operations are actually on the brink of compromise during the ATM/debit card operation, because of such several unfortunate factors detailed below.

1. Technological advances that increase a bank's dependence on information technology and computer-network environment have made transactions more complex and they now involve various nodes across various institutions and include consumer roles to initiate the payment at a bank's consumer activated terminals.¹²¹⁰ Transactions and their makers become more vulnerable to abuse if people (consumer, bank staff, and others) are not well prepared with the latest fraud risk education to consumers; and if the technology and processes involved in the ATM/debit card operations are not state-of-the-art' with up-to-date security features, good standard operating procedures, and/or robust IT risk management. In general, bank security systems in Indonesia are still poor.¹²¹¹ Consumer education is crucial.

¹²¹⁰ See FDIC, above n 254, 1–2. See also Drugs and Crime Prevention Committee, 'Inquiry into Fraud and Electronic Commerce' (Parliament of Victoria, 2004) 1; Rambure and Nacamuli, above n 32, 63. See also Bolton and Hand, above n 257, 235; Hayashi, Sullivan and Weiner, above n 199, 99; Gates and Jacob, above n 258, 7. See also Glaessner, Kellerman and McNevin, above n 51, 1; Malakedsuwan and Stevens, above n 258, 18–19.

¹²¹¹ Opinion of the Brigadier General of Indonesia's Police Department, Victor E Simanjuntak of the banking security system. See Mitra Tarigan, *Sepertiga Kasus Skimming di Dunia Terjadi di Indonesia [One Third of World Skimming Case Happened in Indonesia]* (2 July 2015) Tempo.co <<http://nasional.tempo.co/read/news/2015/07/02/063680461/sepertiga-kasus-skimming-di-dunia-terjadi->

As the Basel Committee on Banking Supervision pointed out several years ago, ‘risk may be heightened where a bank does not adequately educate its customers about security precautions’.¹²¹²

2. The deficiency in consumer fraud risk education (negative education)¹²¹³ is a situation that creates a huge asymmetry in information between that of the consumers compared to that of the bank and/or e-banking attacker, which makes consumers very vulnerable to abuse. As evidence of this, the BI-Fraud Survey results have confirmed the extent of this lack of education, where 70 per cent of banking consumers in Indonesia state that they have never received any fraud risk education from their banks. Consequently, many respondents are still utilising dangerous practices: 37 per cent of consumers use a birthday date as their ATM/debit card PIN and 13 per cent of consumers use a simple number such as 1234, 0000, 1111 as their PIN (which is very vulnerable for ‘PIN guessing’ attack). As Facciolo asserts, ‘inability to use technology safely and poor appreciation of the risks involved, makes consumers doubly vulnerable’.¹²¹⁴ The lack of fraud risk education by banks was also highlighted by a lack of comprehensive and published ATM/debit card fraud reports from the payment system authority.¹²¹⁵ As Kitten asserts, the level of consumer vigilance also depends on the quality and effectiveness of consumer education by the banks (that is, whether or not the banks have issued or had available comprehensive consumer education material and whether the material in question has been effectively delivered to consumers).¹²¹⁶
3. With the advance of technology and the innovation of ever more sophisticated methods of identity theft, many malicious devices such as skimmer tools and spy cameras have become tinier, easy to customise, and can deliver data wirelessly;

di-indonesia>. In fact, ATM/debit card operations still use old and vulnerable technology such as magnetic stripe card and static PIN. Banks also lack active monitoring on public consumer activated terminals, surveillance tools (such as CCTV), state-of-the-art e-banking, security infrastructure (such as ATMs with malicious device sensors and Anti Malware) and a neural network application. With these deficiencies, it is very difficult for banks to create deterrence, spot the occurrence of identity theft, or mitigate the fraud and immediately notify consumers who are affected by the fraud to reduce/stop consumer’s damages.

¹²¹² BCBS, *Risk Management for Electronic Banking and Electronic Money Activities*, above n 3, 6–7.

¹²¹³ United Nations, ‘International Review of Criminal Policy’, above n 267, 347.

¹²¹⁴ Facciolo, above n 293, 623.

¹²¹⁵ See Chapter Four / section 4.3.4 of this thesis.

¹²¹⁶ Kitten, *3Reason Skimmers are Winning*, above n 1134, Several experts in discussion, among them are: John Buzzard (FICO’s Card Alert Service), Carolyn Criscitiello (a vice president in M&T’s Alternative Banking and Retail Service Division) and Avivah Litan (Gartner fraud analyst). See also BCBS, *Risk Management for Electronic Banking and Electronic Money Activities*, above n 3, 6–7.

malware and eavesdropping techniques have also become more advanced and hard to detect; and even conventional methods such as card trapping using matchsticks or toothpicks which cleverly attach inside the ATM slot combined with ‘perfect’ fake call centre stickers as well as social engineering by con artist have all have proven to be very effective tools to steal consumer ATM/debit card data without the theft being immediately noticed by the consumer (as a layperson), especially if they have not had any education from their bank about the various identity theft and fraud methods. It is also argued that from empirical evidence, even trained consumers will arguably have difficulties in spotting these malicious devices. Some of them (such as malware, eavesdropping tools and some types of skimmers) are passive attacks that are ‘intangible’, out of sight, perfectly disguised, or simply unable to be distinguished from legitimate transactions/facilities (such as a bank anti-skimmer device) because of their ‘perfection’, and/or lack of bank’s information and/or disclosure.¹²¹⁷

4. In the electronic world, the original of a message is indistinguishable from a copy in an electronic environment. Hence, unauthorised transactions perpetrated by fraudsters will most probably be treated by the issuer bank as genuine or valid transactions. The potential for fraud is therefore substantial due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions.¹²¹⁸
5. Law enforcement agencies lack technical expertise as well as sufficient regulatory powers and equipment to investigate and prosecute fraudulent electronic transactions.¹²¹⁹

¹²¹⁷ Because many banks have many ATMs with different brands, the anti-skimmer attachment on the ATM’s slot also will have lots of variations in term of shape, colour, and dimensions. Hence, theoretically, consumers will never be able to judge whether the anti-skimmer device attached to an ATM’s slot is legitimate or not.

¹²¹⁸ UNCITRAL, ‘Model Law on Electronic Signatures with Guide to Enactment’, above n 337, 20. In practice, this condition is taken for granted by the bank with its bank–consumer’s liability dumping provision which states that all consumer transactions as long as they are using the correct ATM/debit card data and PIN will be deemed as valid transactions. This provision also becomes the main defence for banks in rejecting consumer claims over unauthorised ATM/debit card transactions.

¹²¹⁹ United Nations, ‘International Review of Criminal Policy’, above n 267, 347. Mitra Tarigan, *Sepertiga Kasus Skimming di Dunia Terjadi di Indonesia [One Third of World Skimming Case Happened in Indonesia]* (2 July 2015) Tempo.co <<http://nasional.tempo.co/read/news/2015/07/02/063680461/sepertiga-kasus-skimming-di-dunia-terjadi-di-indonesia>>. ATM skimming fraud in Indonesia is pervasive. In the last three years of 5500 ATM skimming cases in the world, one third or 1549 cases happened in Indonesia. However, only a few of the perpetrators could be arrested and prosecuted. However, a recent arrest that will raise awareness is that of ‘six people [who] allegedly used ATM skimmers — equipment designed to filch ATM card data and

7.3.2.2. Typology of Identity Theft/Fraud in an Unauthorised ATM/debit Card Transaction according to Its Point of Compromise

From the inherent risk and identity theft/identity fraud methods in ATM/debit card transaction in Indonesia (as has been described in Chapter Four), all those risk and identity theft/frauds can be summed up according to the circumstances of the identity theft/fraud circumstances based on the point of compromise. By knowing the point of compromise, this thesis argues that it becomes easier to determine the party that is supposed to be more vigilant, owes a duty care, and is in a better position to reduce the possible occurrence of identity theft/fraud at the lowest cost. Thus, the basic typology of identity theft/fraud in consumer ATM/debit card transactions will be outlined below:¹²²⁰

7.3.2.2.1. First Party Identity Theft/Fraud Typology¹²²¹

First party fraud occurs when cardholders use their genuine ATM/debit card to conduct legitimate or authorised ATM/debit card transactions and then repudiate having authorised the transactions or claim that the transactions were flawed.¹²²²

7.3.2.2.2. Second Party Identity Theft/Fraud Typology¹²²³

For second party fraud, an acquaintance of the cardholder has typically stolen the genuine cardholder's card temporarily or made a transaction beyond authorisation and used the PIN that has been previously shared by the cardholder or reached by guessing according to their knowledge of the cardholder's credentials or other information to make one or more unauthorised ATM/debit card transactions.

PINs — to steal a total of Rp 1.24 billion from 112 customers of Bank Central Asia, Indonesia's largest private lender by assets.' : 'Police Bust ATM Skimming Racket' *Jakarta Post*, 4 November 2015, <<http://jakartaglobe.beritasatu.com/news/police-bust-atm-skimming-racket/>> .

¹²²⁰ The identity theft/fraud typology in this section is based banking practices in Indonesia where all bank ATM/debit cards and their associated PINs are normally delivered directly to the consumer in 'face-to-face' transactions in a bank's office. Therefore, one member of the fraud taxonomy that used to be added in credit card fraud descriptions — 'card not received' — is not discussed here.

¹²²¹ First party fraud is that committed against a financial institution by one of its own consumers; second party fraud is fraud committed by someone close to or known to the victim, usually a relative or employee.

¹²²² In first party fraud, there is no a point of compromise since the consumer actually is the perpetrator and basically has conducted legitimate transactions.

¹²²³ First party fraud is fraud committed against a financial institution by one of its own consumer; second party fraud is fraud committed by someone close to or known by the victim, usually a relative or employee.

7.3.2.2.3. Third Party Identity Theft/Fraud Typology¹²²⁴

1. The Lost and/or Stolen ATM/Debit Card Which Targets Consumers as a Point of Compromise

This identity theft occurs when attackers target consumers/cardholders as a point of compromise to get their genuine ATM/debit card outside of a bank's premises/infrastructures. This fraud typology includes, among other things, the unauthorised ATM/debit card transaction performed by a fraudster using a consumer/cardholder's genuine ATM/debit card, which has been stolen directly from cardholder using identity theft methods such as 'lost and stolen card', or card swapping (social engineering). Meanwhile, a fraudster can obtain a cardholder's PIN by various PIN theft methods, such as PIN guessing, shoulder surfing, or PIN cracking etc.

2. The Lost and/or Stolen ATM/Debit Card Which Targets Consumers and Bank Infrastructures as a Joint Point of Compromise

This identity theft occurs when fraudsters target a consumer/cardholder and/or bank infrastructure and/or data network as a joint point of compromise. Fraudsters firstly compromise a bank's consumer activated terminal/ infrastructure with malicious devices to steal the consumer's genuine ATM/debit card (card trapping), and/or subsequently trick a consumer into revealing their PIN inadvertently. This identity theft/fraud typology includes among other things card trapping, or card swapping methods. There is also a possibility that the fraudsters may directly tamper with or break into a bank's ATM to steal consumer's genuine card, such as in identity theft using the 'swallowed ATM/debit card theft' fraud method. Meanwhile, the fraudster obtains the cardholder's PIN by PIN guessing, PIN cracking, 'shoulder surfing' (fake 'Good Samaritan'/con artist approach), fake bank ATM call centre, PIN hole camera, PIN-pad overlay, or other.

3. The Counterfeit ATM/Debit Card

This identity theft occurs when fraudsters target a bank and/or its counterpart's infrastructure and/or data network as the point of compromise. This identity theft/fraud typology includes among other things the unauthorised ATM/debit card transaction performed by a fraudster using a counterfeit card that uses the consumer's real data that

¹²²⁴ Third party fraud is fraud committed against an individual by an unrelated or unknown third party.

has been previously stolen from the consumer's ATM/debit's magnetic stripe card, from a communication network, data in transit in the ATM/merchant's EDC, and/or a bank / its counterpart computer and/or data centre. Included in this fraud typology are various identity theft methods such as card skimming, eavesdropping, malware, and so on. Meanwhile, a fraudster has obtained the cardholder's PIN, typically by PIN cracking, eavesdropping, the use of malware, PIN hole camera, PIN-pad overlay, and so on.¹²²⁵ Typically, a consumer will not notice about the identity theft — because the fraudster's malicious devices are not designed to halt or disturb the transaction, so the ATM/debit card operation appears to work very normally.

From these basic typologies of ATM/debit 'card present' identity theft/fraud (even though probably not exhaustive), identity theft and fraud methods, the point of compromise, type of fraudster and attacker, and probably its prevention and mitigation methods, can be enumerated and depicted in the matrix table below.

Table 3: ATM/Debit Card Point of Compromise, Attacker, Identity Theft, Prevention/Mitigation Methods and Least Cost Avider

<i>Point of Compromise</i>	<i>Goal</i>	<i>Attacker& Type of Attack</i>	<i>Identity Theft Method& PoC</i>	<i>Identity Theft Prevention/ Mitigation</i> ¹²²⁶	<i>Least Cost Avider</i> ¹²²⁷
Consumer	Genuine Card	Third Party/ Active Attack	- Lost/Stolen Card, Card Swapping outside banks premises	Lost/ Stolen Card & Card Swapping risk education: - Do's & don'ts - Awareness/ precaution about risk	Consumer

¹²²⁵ Banks typically have a defence that their system already has encryption, a firewall, or other security features. However, fraudsters typically can exploit any vulnerabilities that exist in the system with such vulnerabilities able to be triggered by poor security implementation, delays in software patch updates, absent or out of date anti malware applications, eavesdropping / 'man in the middle' attack on the bank's inter-operability nexus (where data change from encrypted format to the plain format in order to be encrypted by other different counterparty system), and so on. See Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 226.

¹²²⁶ Identity Fraud methods and the prevention/mitigation method are not discussed in this matrix because once an identity theft operation succeeds, then typically the identity fraud operation— such as unauthorised ATM withdrawal/transfer/transactions either using the victimised consumer's genuine ATM/debit card or counterfeit card — will be very difficult to avoid since it's using correct and indistinguishable data/PIN.

¹²²⁷ The 'Least Cost Avider' is a party or parties that could reduce fraud loss at the lowest cost. Theoretically, a consumer could become the party that is able to reduce fraud loss only if they previously had fraud risk education, including ways to avoid it. Conversely, without fraud risk education, this is unlikely as the consumer as a layman typically has a false sense of security about e-banking products, hence most of them take no precautions when conducting ATM/debit card transactions and become an easy target for identity theft.

	PIN	Passive Attack	- Shoulder Surfing, PIN-guessing		
ATM Machine Slot	Genuine Card	Third Party/ Active Attack	Card Trapping PoC: Bank & Consumer	- Consumer fraud risk education - ATM with sensor - Bank's active surveillance	Primary: Issuing Bank Secondary: Consumer
			Card Swapping PoC: Bank & Consumer	- Consumer fraud risk education - Personalised ATM/debit card	
			Card Swallowed Theft PoC: Bank	- ATM top fascia key/lock enhancement - Automatic disablement of card (card block)	Issuing Bank
	Card Data	Third Party/ Bank/ Vendor's Staff /Passive Attack	Skimming	- Anti-skimmer, jitter, ATM with sensor, CCTV - Active monitoring - Chip card & Chip ATM - Skimming risk education	Issuing Bank Acquiring-Bank Bank's-Vendor
			Malware PoC: Bank	- Anti malware - OS patch update - Know your employee - Better encryption	
			Eavesdropping	- Better encryption and data management; IDS	
	PIN	Passive Attack	-PIN-Hole Camera -PIN-Pad Overlay -Shoulder Surfing -Malware, Eaves-dropping, Social Engineering	- PIN shield - Active monitoring - Consumer education - Anti PIN-pad overlay - Anti malware IDS	
Merchant EDC/EFT-POS	Card Data	Third Party/ Merchant Owner/ Staff / Passive Attack PoC: Bank	- Malware -Eaves-dropping	- Anti malware - Strong encryption - Merchant & user risk education - EDC physical & logical security - EDC with bar & facing consumer - PIN shield	Issuing Bank Acquiring-Bank Merchant
	PIN		- Malware -PIN-cracking -PIN-guessing -Shoulder Surfing		
Merchant Cash Register	Card Data	Third party / Merchant Owner/ Staff /Passive Attack PoC: Bank & Merchant	-Hacking - Malware -Double Swiping	- No double swiping policy & regulation - Consumer boycott	Issuing Bank Acquiring-Bank Merchant
	PIN		-Shoulder Surfing - Malware		
		Merchant	Skimming	- EDC secure position	Issuing Bank

Merchant/ Restaurant, etc	Card Data	Owner/ Staff / Passive Attack PoC: Bank & Merchant		- Consumer swipe	Acquiring- Bank Merchant
	PIN		Shoulder Surfing	PIN Shield	
Data Network	Card Data	Third Party/ Bank/ Vendor's Staff/ Passive Attack PoC: Bank	Eavesdropping	<ul style="list-style-type: none"> - IDS - Strong encryption - Hash - etc 	Issuing Bank Acquiring- Bank Merchant
	PIN		<ul style="list-style-type: none"> -PIN-guessing -PIN-cracking 		
Bank &/or Counter- part Host Computer	Card Data	Third Party/ Bank/ Vendor's Staff / Passive Attack	<ul style="list-style-type: none"> - Malware - Pin-cracking 	<ul style="list-style-type: none"> - Firewall - IDS - Anti malware - Strong encryption - etc 	Issuing Bank Acquiring- Bank Banks- Vendor
	PIN		<ul style="list-style-type: none"> -Malware -PIN-cracking -PIN-guessing 		
Personalized Identified Information Database (PII): facebook, office, civil register database, & so on)	PII	Third Party/ Bank / Vendor's Staff / Passive Attack	<ul style="list-style-type: none"> -Data Gathering -Dumpster Diving -Social Engineering 	<ul style="list-style-type: none"> - Do not share PII - Card and PIN delivery in a separated envelope - Activated card with secret information - Consumer education 	Issuing Bank Acquiring- bank Consumer

7.3.2.3. PIN as an Electronic Signature Has Not a Non-Repudiation Value

In ATM/debit card operations, the validity of cardholder is identified by their ATM/debit card. As an attribution, instead of digital signature, the PIN has become a primary choice by bank as an authentication feature in order to secure cardholder ATM/debit card transactions.¹²²⁸ In other words, a PIN basically is a cardholder's electronic signature¹²²⁹ as it replaces a written signature.¹²³⁰

¹²²⁸ CPSS, *Retail Payment in Selected Countries*, above n 187, 5. See also Marco Gercke, 'Legal Approaches to Criminalize Identity Theft' in United Nations Office on Drugs and Crime (ed), *Handbook on Identity-related Crime* (United Nations, 2011) 12. See also Australian Payments Clearing Association, above n 195; Hendry, above n 203, 76; Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 208.

¹²²⁹ Electronic signatures are a broader notion of signature in the electronic form. Among others are digital signatures, biometric signatures (such as finger print, iris or retina), PINs, digitised versions of handwritten signatures, and other methods, such as clicking an 'OK-box'. See UNCITRAL, 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment', above n 337, 21.

¹²³⁰ Meyer and Matyas, above n 72, 430–1. See also Madan and Reid, above n 205, 48.

In an electronic environment, the genuine electronic data is indistinguishable from a copy. With the development of various PIN theft techniques,¹²³¹ the ease of intercepting and altering information in electronic form without detection, and so on, the possibility of fraud occurring is considerable.¹²³² Because a PIN does not have something unique that is closely identifiable only with the individual cardholder (such as is the case with the manual or handwritten signature,¹²³³ or a given biometric (for example the cardholder's retinal image), or a digital signature,¹²³⁴ then it is actually impossible for an issuing bank to distinguish an unauthorised PIN entry from an authorised one.

Geva has canvassed an important remark about the concept of electronic authentication and its legal value, as follows:

...electronic authentication is carried out by means of compliance with an agreed-upon security procedure, which can be entered into a terminal by anyone to whom it becomes available. Electronic authentication is a means of legitimizing the action of that person, or of attributing it to him or her, but not of identifying him or her. It is very much like a door key facilitating entry to the system, or better, a seal affixed to an instrument, authenticating it, but not identifying the one who actually placed it. Consequently, any technologically effective entry of an access code, even when it is carried out by an unauthorized person to whom it may have become available unlawfully, appears to the financial institution as a valid authentication. *Prima facie*, the electronic authentication would thus justified the account institution debiting the customer's account. In this sense, the authentication by means of compliance with a security procedure is not an electronic equivalent to a manual signature; rather, it is more analogous to the placement of an "electronic seal". The financial institution is unable to distinguish between an authorized and unauthorized authentication and is likely to be inclined to

¹²³¹ As has been described in the Chapter Four / section 4.2.2, a PIN is static and consists of a simple four or six digits, and is very easily stolen or revealed using various methods such as PIN-guessing, PIN-cracking, shoulder surfing, discovered from a written record kept by the consumer in their wallet or bag, obtained with a PIN-hole camera, PIN-pad overlay, malware, and so on.

¹²³² UNCITRAL, 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment', above n 337, 20.

¹²³³ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 36–7.

¹²³⁴ See UNCITRAL, 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment' above n 337, 22. According to UNCITRAL:

Digital signatures are created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form. Digital signatures use what is known as "public-key cryptography", which is often based on the use of algorithmic functions to generate two different but mathematically related "keys" (i.e. large numbers produced using a series of mathematical formula applied to prime numbers). One such key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other one for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively referred to as "cryptosystems" or, more specifically, "asymmetric cryptosystems" where they rely on the use of asymmetric algorithms. In addition to generation of key pairs (public key and private key), a "hash function" is used in both creating and verifying a digital signature which creates a digital representation, or compressed form of the message ("message digest" or "finger print"). Any change to the message invariably produces a different hash result when the same hash function is used. It is virtually impossible to derive the original message from knowledge of its hash value.

pass the risk of an unauthorized but properly authenticated transfers onto the customer.¹²³⁵

Typically, a bank always says that PINs were generated and verified with secure cryptographic hardware which is impossible for its staff or a third party to know. Hence, the consumer as the owner of the PIN should always be responsible for its use and secrecy. As Anderson asserts, '[p]eople who complain are therefore routinely told that they must be lying, or mistaken, or the victim of fraud by a friend or relative (in which case they must be negligent).'¹²³⁶ This is also the situation in Indonesia.

However, in practice blunders in application design, implementation and operation has rendered PIN secrecy able to be compromised.¹²³⁷ The other problem with PIN technology is that it is an old and outmoded technology.¹²³⁸ PINs are also static and normally consist of a four or six digit number and have been chosen by financial institutions as a cost-effective mass-distribution authentication method.¹²³⁹ The combination of PIN and magnetic stripe card is considered a weak and inherently insecure authentication method compared to other methods such as a manual signature or a strong electronic authentication method such as a biometric and digital signature, the purpose of which is to ensure non-repudiation.¹²⁴⁰

According to Kondabagil, non-repudiation is:

the assurance that a neutral third party can be convinced that a particular transaction or event did (or did not) occur. It involves creating proof of the origin or delivery of electronic information to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent.¹²⁴¹

¹²³⁵ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 228–9.

¹²³⁶ Anderson, above n 1159.

¹²³⁷ Ibid. See also Nick Gifford, *Information Security: Managing the Legal Risk* (CCH Australia Limited, 2009); Nicholas Bohm, Ian Brown and Brian Gladman, 'Electronic Commerce: Who Carries the Risk of Fraud?' (2003) (3) *Journal of Information & Technology*; Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 226–7.

¹²³⁸ Mohammed, above n 195, 214. See Hendry, above n 203, 37. See also Meyer and Matyas, above n 72, 475. See also Radu, above n 210, 388; Pipkin, above n 226, 130.

¹²³⁹ White, above n 111, 33.

¹²⁴⁰ Administrator, *Thursday Thinkpiece: Mason on Digital Signatures* (August 22 2013) Slaw Canada's Online Legal Magazine <<http://www.slaw.ca/2013/08/22/thursday-thinkpiece-mason-on-digital-signatures/>>. See also White, above n 111, 33; Andrian McCullagh, 'Legal Aspects of Electronic Contract and Digital Signatures' in Anne Fitzgerald et al (eds), *Going Digital 2000* (Prospect Media, 2nd ed, 2000) 198. According to McCullagh, a PIN comprising only a four digit number is far less strong compared with digital signature where its private key consisting of two large prime number that are so large that the ordinary person will not be able to remember them.

¹²⁴¹ Kondabagil, above n 194, 70–3.

There is a difference in the use of the term ‘non-repudiation’ in its crypto-technical and legal contexts. According to McCullagh and Caelli, in the legal sense ‘the signatory to a document is always able to repudiate a signature that has been attributed to him or her’; whereas in the crypto-technical sense:

Non-repudiation is a property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection or authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).¹²⁴²

In this regard, as long as a digital signature’s private key has not been stolen by a fraudster and the digital signature is verified, it can be treated as an electronic equivalent to a manual signature. The owner of the private key is then prevented from repudiating the digital signature.¹²⁴³ In other words, a digital signature provides a ‘non-repudiation’ function — that is, it has the ability to identify the author and whether the document has been changed since it was digitally signed.

The evidence shows that when the correct PIN is used to authenticate ATM/debit card transactions, then from a technological point of view it does not automatically prove that the transaction was authenticated and authorised by the purported cardholder.¹²⁴⁴ For instance, when a fraudster manages to skim and steal a consumer’s ATM/debit card magnetic stripe data and obtain its PIN using the PIN-hole camera/PIN-pad overlay method, technically he/she can create a counterfeit card to make an unauthorised withdrawal which drains the consumer’s money from their bank. The transaction itself will be deemed valid according to the bank’s system because it used the correct ATM/debit card data and PIN. The problem with current banking technology is that it cannot distinguish whether the ‘valid withdrawal transactions’ were generated or keyed-in by the real consumer with his/her genuine magnetic stripe card and PIN, or by an unknown fraudster with a counterfeit card and the (illegally obtained) correct consumer PIN. Hence, referring to this scenario example, it is argued that PIN as an authentication method in ATM/debit card transactions has no non-repudiation aspect at all.

¹²⁴² William Caelli, Dennis Longley, and Michael Shain, *Information Security Handbook* (Macmillan, 1991) cited in Andrian McCullagh and William Caelli, ‘Non-Repudiation in the Digital Environment’ (2000) 5(8) *First Monday*, *Peer-Reviewed Journal on the Internet*. In this definition, the authors using the Australian Federal Government’s Electronic Commerce Expert Group adopted a technical meaning of non-repudiation in its report to the Australian Federal Attorney General.

¹²⁴³ Ibid.

¹²⁴⁴ Geva, ‘Consumer Liability in Unauthorized Electronic Funds Transfers’, above n 107, 228–30, 233–4, 239–41.

7.3.3. Law Perspective: Facts and Principles

Indonesia, as a civil law country, does not have the doctrine of precedent. Hence, the rule of law which is implemented by adjudicators in various ADR fora and ultimately by the judges in the court, is often only based on the regulations themselves and not on previous judgements. As has been previously discussed, in the absence of clear, fair, detailed, and decisive fraud liability regulation, court decisions over disputes between banks and consumers concerning unauthorised ATM/debit card transactions are commonly only resolved based on too general fault/negligence liability regulations.

The unclear definition of unauthorised ATM/debit card transactions, of consumer and/or bank fault/negligence in such transactions (to name but a few evidences of lack of sufficient detail) combine with adjudicators/judges' lack knowledge about the relevant and update economic, technological and ATM/debit card regulation aspects, the existence of inherent risk in the ATM/debit card operation, and the asymmetry of information suffered by consumers to ensure that ADR and/or court verdicts tend to be varied, inconsistent, unpredictable and, it is argued, unjust.

The main issue of this thesis — and one that has also become the central issue in consumer protection implementation in payment card operation in Indonesia and other countries as advocated by many scholars and prominent institutions — concerns fraud liability and the loss allocation rules for unauthorised electronic fund transfers/ATM/debit card transactions.¹²⁴⁵ A key point with this issue is that that all the ATM/debit card transactions that were claimed as unauthorised by the consumers are — from a technological point of view — all conducted using correct consumer ATM/debit card data and PIN or agreed-upon security procedures to allow the bank to debit the consumer's fund.

From the many instances of unauthorised ATM/debit card transactions disputes in Indonesia (as has been reported by consumers and/or adjudicated in the ADR body / court of justice), the most intriguing questions pertaining to fraud liability rules that should be reformulated to assure fairness for both parties are: how to formulate fair loss allocation rules between banks and their consumers for unauthorised ATM debit card transactions, especially when: (1) there is no clear evidence in regard to who actually

¹²⁴⁵ See nns 107–17.

perpetrated the unauthorised ATM/debit card transaction and whether there is fault or negligence on the part of the bank's and/or consumers; and (2) both banks and customers exhibit negligence that enabled the fraudsters to conduct unauthorised ATM/debit card transactions (joint liability).

In regard to the very important questions above, it is submitted that ADR and court verdicts at various levels have been shown to be unpredictable, inconsistent and arguably unjust decisions. While CDSB as an ADR institutions tend to make decisions that always favour the consumer/cardholder, conversely, the Supreme Court of Justice, as an appeal court, tends to have verdicts that favour the banks.

In most of the Supreme Court decisions concerning unauthorised ATM/debit card transactions, it is submitted that generally the verdicts were based on the contributory negligence principle and/or probably the wrong 'common sense' valuation by the court's judges due to their lack of knowledge on payment card regulation, the typology of ATM/debit card identity theft and fraud, and economic and technological aspects that are intertwined with unauthorised ATM/debit card transactions. These court decisions were deemed unjust to consumers and as such could hinder the development of electronic payment in Indonesia.

Therefore, in the current circumstances where there is no specific regulation for fraud risk and/or negligence liability in ATM/debit card transactions and to assure fairness on each adjudications' verdict on unauthorised ATM/debit card disputes between bank and its consumers, it is submitted that resolution of disputes should involve progressive, up to date and relevant legal, economic and technological facts and principles that are pertinent to the specific unauthorised ATM/debit card transaction.

7.4. Proposed Law Reform Implementation on Loss Allocation Rules concerning Unauthorised ATM/Debit Card Transactions in Indonesia

In general, banks have more power and resources compared to consumers in an unauthorised ATM/debit card dispute. Since most consumers are laypersons that do not have much knowledge about the economic, technical and legal aspects related to the unauthorised ATM/debit card transactions and a bank's ATM/debit card system and operation, and often lack other resources, in many instances the consumer as plaintiff finds it difficult to prove that the bank as defendant was negligent and that negligence

has caused damages to the plaintiff. Conversely, banks usually succeed. They boast of their ATM/debit card infallibility (which is actually merely anecdotal) and maintain that the plaintiff was guilty of contributory negligence — at least in terms of the definitions supplied by the banks themselves.

In several unauthorised ATM/debit card transaction cases that ended up at court as the final adjudication forum, almost all of the verdicts favoured the bank on the basis that the consumer's losses were due to consumer's own contributory negligence. The problem with these court verdicts are is that they have many flaws that contribute to making the verdicts able to be considered unjust to the consumers involved. In this regard, it is submitted that in the adjudication proceeding, judges deny several economic, technological and legally important legal facts about the nature of the identity theft/fraud and the bank's contributory negligence in failing to secure its infrastructure and provide adequate fraud risk education to the consumer. Arguably, the bank's contributory negligence was the main enabler or dominant contributing cause that facilitated the occurrence of unauthorised ATM/debit card transaction.

These misleading verdicts could, if they continue, on one hand reduce consumer confidence and hinder development of the electronic payment system which is actually very good for the country's economic efficiency and development. On the other hand, it could also discourage banks — as the owners of electronic banking systems (including as issuers of ATM/debit cards) — from improving security of bank's electronic banking infrastructure and giving comprehensive and adequate fraud risk education to their consumers.

The principal objective of any resolution on an unauthorised ATM/debit card transaction dispute between a bank and consumer is to make a decision that will implement and enhance fairness to disputant parties. The desired fairness is to be attained in the context of creating incentives for banks and consumers so that ATM/debit card fraud precautions are improved and benefits are maximised for society as a whole. The question of who should bear the loss on unauthorised ATM/debit card transactions requires the availability of good and fair rules to provide a sensible answer. It is believed that the fair distribution of losses among market participants could affect

the incentives to commit fraud.¹²⁴⁶ As Levitin has asserted, ‘The greater a party’s liability for fraud losses, the greater incentive the party will have to take care to avoid fraud’.¹²⁴⁷

Therefore, it is believed that the law reform objective for fraud liability law/loss allocation rules for unauthorised ATM/debit card transactions in Indonesia can be achieved by synthesising multi-disciplinary approaches such as legal, economic, and technological principles into several actions concerning unauthorised ATM/debit card transaction disputes, as follow:

- 1). In civil liability adjudication/litigation proceedings, law reform can be achieved by:
 - a). promoting the movement to shift the burden of proof from the plaintiff (consumer) to the defendant (bank), such as utilising the negligence *per se* doctrine as a legal basis for a plaintiff to claim damages from a defendant. Hence, the defendant is the party that should prove that they had no fault/negligence,¹²⁴⁸ and/or the plaintiff’s negligence was the actual cause of the occurrence of the unauthorised ATM/debit card transaction. If a defendant fails to prove at least one of these two defences, the defendant is obliged to remedy the consumer’s loss; and/or
 - b). replacing the unjust and obsolete pure contributory negligence doctrine (which is commonly used in ADR/Court adjudication proceedings in Indonesia) with the comparative negligence doctrine which is deemed more fair and widely used in many developed countries. This replacement is considered important to achieve a fair and more predictable legal adjudication in cases in ADR and/or Court. With the adoption of a judge-made law role (as played by judge in the common law countries), judges in Indonesia could reform the law by setting new precedents in the unauthorised ATM/debit card transaction cases that come before them.¹²⁴⁹ This option is deemed valid and timely, since the

¹²⁴⁶ Roberds, above n 265, 43. See also Roger Clarke and Alana Maurushat, ‘Passing the Buck: Who Will Bear the Financial Transaction Losses from Consumer Device Insecurity’ (2007) 18 *JL Inf. & Sci.* 8, 39; Levitin, above n 114, 3; Rusch, above n 106, 595; Gillette, above n 130, 185–6.

¹²⁴⁷ Clarke and Maurushat, above n 1246, 39.

¹²⁴⁸ For instance, because ‘act of God’ was the cause of the consumer’s loss. However this defence is arguably cannot be used in the event of unauthorised ATM/debit card transactions but only where bank infrastructure malfunctions, such as in a natural disaster (earthquake etc).

¹²⁴⁹ Law reform of fraud liability law and loss allocation rules by modifying and/or supplementing tort law in the Indonesian Civil Code is not recommended in this thesis, since the legislation process for amending Civil Code law can be very long and full of uncertainty. As a reference for this pessimistic view, see as an example one pertaining to the amendment process of Indonesia Criminal Code that was

movement of the appointment of progressive judges is on the way in Indonesia;¹²⁵⁰ and/or

- 2). creating clear, fair, detailed, and decisive fraud liability rules for unauthorised ATM/debit card transactions. It is believed that a simple set of clear, fair, detailed, and decisive fraud liability rules would create more uniform results in fraud liability dispute resolution between consumers and their banks, regardless of which adjudication forum is used. It is believed if such rules existed, they could be treated as a common guideline and probably could remedy an adjudicator's lack knowledge on the relevant economic, technological and legal aspects that are intertwined specifically with unauthorised ATM/debit card transactions. Therefore, the existence of these rules not only will avoid prolonged disputes between banks and consumers concerning unauthorised ATM/debit card transactions that have caused damages to consumers, but also create incentives for banks and consumers to enhance their vigilance against identity theft and fraud in ATM/debit card transactions.

7.4.1. Law Reform in Civil Liability Adjudication/Litigation Proceedings

7.4.1.1. Civil Lawsuit Based on Tortious Liability: Breach of Statutory Duty (Negligence Per Se)

Generally, in a common law country a breach of statutory duty differs from ordinary negligence under tort. Breach of statutory duty can arise without negligence because the statute may impose a strict and particular standard of care. Nevertheless, a failure to abide by a statutory duty of standard of care can constitute negligence.¹²⁵¹ In Indonesia, the action of breaking a statute can be considered an unlawful act. Makarim states that in Indonesia, *negligence per se* or breach of statutory duty can be used to claim damages for which the defendant is liable.¹²⁵² By way of a comparison, in Australia when a plaintiff wants to establish a tort breach of statutory duty against a defendant that is not a statutory authority, he or she must establish that:

- (a) the statute intended to confer a civil remedy for its breach;

started in the 1980s and has not yet finished when this thesis was written. See Zainal Abidin, *Menelisik Pembahasan RUU KUHP [Investigating the Criminal Code Bill Process]* (no date) <<https://docs.google.com/document/d/1.../edit?usp=sharing>>.

¹²⁵⁰ Satjipto Rahardjo, *Penegakan Hukum Progresif [Progressive Law Enforcement]* (Kompas, 2010) 55–69.

¹²⁵¹ Stewart and Stuhmcke, above n 912, 428. Gibson and Fraser, above n 917, 117.

¹²⁵² Makarim, above n 857, 167.

- (b) the defendant breached the duty imposed upon it by the statute;
(c) that this breach caused the loss or injury to the plaintiff and that damage was of a kind the statute was intended to prevent; and
(d) the plaintiff was within the protection of the statute.¹²⁵³

From various regulations that are relevant with bank ATM/debit card operation as described in the Chapter Five and various identity thefts and frauds as described in Table 4, the relation of the occurrence of identity theft/fraud and the possibility of breach of statutory duty by the bank, is as follows (see below).

Table 4: ATM/Debit Card Point of Compromise, Identity Theft Methods and Bank Statutory Duties

Point of Compromise	Goal	Identity Theft Method&	Bank’s Statutory Duties	Statutes
Consumer	ATM/ Debit Genuine Card	- Lost/Stolen Card, Card Swapping outside bank premises	Obligation to give fraud risk education to consumer	<ul style="list-style-type: none">- Constitution- LIET- GR-OEST- LBI- BIR-CBPI- BIR-Risk Management- BIR-TBPI & UBCPD- BIR-RMUITCB- BID-CP & Security- BID-Chip & PIN- BIR-CPPSS
	PIN	- Shoulder surfing, PIN-guessing		
Bank ATM Machine Slot	ATM/ Debit Genuine Card	Card Trapping	<ul style="list-style-type: none">- Obligation to protect consumer from loss caused by the bank’s electronic agent;- Obligation to secure and protect electronic system infrastructure or any data transferred through a bank’s electronic system;- Obligation to safeguard the confidentiality, integrity, availability, authenticity, accessibility, traceability, and non-repudiation of consumer data;- Obligation to provide payment system instrument that meets security requirements, international standard and best practice;	
		Card Swapping		
		Card Swallowed Theft		
	Card Data	Skimming		
		Malware		
		Eavesdropping		
	PIN	<ul style="list-style-type: none">-PIN-Hole Camera-PIN-Pad Overlay-Shoulder Surfing-Malware, Eaves-dropping, Social Engineering		
Merchant EDC/EFT-POS	Card Data	<ul style="list-style-type: none">- Malware-Eaves-dropping	<ul style="list-style-type: none">- Obligation to implement fraud prevention devices such as IDS, anti-skimming, anti malware, firewall, and so on;- Obligation to provide Chip	

¹²⁵³ Stewart and Stuhmcke, above n 912, 428, 430–1. Gibson and Fraser, above n 917, 430. See also Restatement (Second) of Tort s 286 (1965).

	PIN	- Malware - PIN-cracking - PIN-guessing - Shoulder Surfing	technology & PINs with at least 6 digit characters; - Obligation to implement physical security control on bank's equipment and rooms such as at ATM/EFT-POS to protect consumers and their transaction from danger of theft, sabotage, and other criminal action;	
Merchant Cash Register	Card Data	- Hacking - Malware - Double Swiping	- Obligation to secure data transmission from EFT terminal to host computer from risks of network disturbance, unauthorised access, and so on;	
	PIN	- Shoulder Surfing - Malware	- Obligation to perform routine monitoring to ensure the security and consumer comfort using e-banking services;	
Merchant/Restaurant, etc	Card Data	Skimming	- Obligation to give fraud risk education to consumer;	
	PIN	Shoulder Surfing	- Obligation to provide compensation, redress and/or substitution for the damages caused by the use of the bank's services;	
Data Network	Card Data	- Eavesdropping - Malware	- and so on.	
	PIN	- PIN-guessing - PIN-cracking		
Bank &/or Counter-part Host Computer	Card Data	- Malware - Cracking		
	PIN	- Malware - PIN-cracking - PIN-guessing		
Personalized Identified Information (PII): Facebook, Office, Civil Register Database, & so on)	PII	- Data Gathering - Dumpster Diving - Social Engineering	Obligation to give fraud risk education to consumer	

In Indonesia, the *Tuan Bahari v PT Bank Negara Indonesia (Persero) Tbk* verdict has indicated that *negligence per se* can be implemented to claim redress in a dispute between a bank and a consumer concerning unauthorised ATM/debit card transactions. In principle, a bank as a prudential and fiduciary institution should always abide by the regulations in conducting their business to ensure that they will only provide robust and secure products/services to their consumers. In this case, PT Bank Negara Indonesia has been punished by the Supreme Court's judges and ordered to redeem the consumer's loss due to third party identity theft and fraud, on the basis that the defendant failed to comply with Bank Indonesia's security regulation that obliged the bank to have Chip

technology and a six digit PIN in ATM/debit card operation, and that it had also been negligent in failing to provide a security guard to improve ATM security and safeguard the consumer's transaction. In this case, the court also argued that bank also failed to prove the existence of consumer negligence that could have caused the PIN to be inadvertently revealed to the fraudster.¹²⁵⁴

Therefore it is submitted that consumers in Indonesia that have lost their funds (deposited previously in the bank) due to an unauthorised ATM/debit card transaction which was enabled by the breach of one or more elements of the bank's statutory duty (as obliged by one or more regulations described in the Chapter Five) can have their civil lawsuit adjudicated based on the *negligence per se* principle. Theoretically, what a consumer should have proved in this lawsuit is just the gap between the bank's ATM/debit card operation and the specific infrastructures, standard or procedures it was obliged to provide under the regulations.¹²⁵⁵

7.4.1.2. Civil Lawsuits Based on Tortious/Negligence Liability: Comparative Negligence instead of Contributory Principle on Unauthorised ATM/Debit Card Transaction Disputes in ADR/Court Proceedings with Multi-Disciplinary Approaches: Economic, Technological and Legal

7.4.1.2.1. Burden of Proof: Plaintiff v Defendant

When a cardholder experiences one or more 'phantom' ATM/debit card transactions and reports it to the bank, in most cases such claims are rejected by the card issuer bank. The cardholder then has to bring the unauthorised ATM/debit card transaction case to the ADR or court to redeem their losses. However, one classic problem when a plaintiff brings a civil dispute before the law concerns the burden of proof. In this regard, is it the consumer who has to prove that the ATM/debit card transaction was unauthorised, or is it the bank that has to prove that the transfer was authorised? In circumstances where both consumer and bank probably have contributed to the loss, who has to prove the existence of fault or negligence that enabled the fraud to happen?

¹²⁵⁴ See explanation of *Mr Bahari v PT Bank Negara Indonesia (Persero) Tbk* in Chapter Six / section 6.4.3.2.2

¹²⁵⁵ For reference case, see *Tuan Bahari v PT Bank Negara Indonesia (Persero) Tbk* [Supreme Court of Republic of Indonesia], 718 K/Pdt.Sus/2008, 10 December 2008..

In the law of torts — whether in Indonesia or other jurisdictions — it is very common that the onus of proving negligence lies with the party who alleges it.¹²⁵⁶ Nevertheless, in order to avoid liability the bank — as the provider of the system — should also prove the soundness of its security procedures and its lack of negligence in performing the authentication procedure in the payment transaction.¹²⁵⁷

Therefore, at the proceedings stage the plaintiff has to prove, by a predominance of evidence, that the defendant to some extent has been negligent and that this negligence has caused damage to the plaintiff.

However, in most cases plaintiffs usually have difficulty in providing evidence to support their allegation, since unauthorised ATM/debit card cases normally involve very technical matters and all necessary evidence and/or relevant information are not in the plaintiff's hand. This difficulty becomes two fold when a plaintiff does not bring an expert witness to reveal — either from theory or empirical evidence — that the bank's system is not infallible and that the possibility of identity theft and/or fraud is huge and pervasive.¹²⁵⁸ In an identity theft and fraud case where the fraudster probably may have unlawfully acquired a consumer's ATM/debit card data by various 'passive' identity theft/fraud methods,¹²⁵⁹ in most of the cases a consumer cannot provide information about where, when, how, and by whom their ATM/debit card data was compromised. Instead, all relevant evidence or witnesses (such as CCTV footage and audit trail of transactions) may be under the control of the defendant, and thus evidence (including that from witnesses) may be very difficult or impossible for the consumer to obtain by

¹²⁵⁶ See Article 163 HIR /Article 283 RBg : 'They who say they have the right, or they mention something that works to strengthen their rights or to deny the right of another person, that person must prove the existence of such rights or that event',;and Article 1865 BW (Indonesia Civil Code): 'Anyone who argues that they have right, or in order to enforce its own right or denied the rights of others, which refers to an event, required proving the existence of such rights or event'. See also Andrian McCullagh and William Caelli, 'Non-Repudiation in the Digital Environment' (2000) 5(8) *First Monday, Peer-Reviewed Journal on the Internet*; Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 235–6; Clarke and Maurushat, above n 1246, 48–9.

¹²⁵⁷ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 235–6.

¹²⁵⁸ Expert witness testimony from the police department or central bank might also be necessary to corroborate the allegation that the identity theft and/or fraud on ATM/debit card operation are actually classic foreseeable risks. As can be seen from several unauthorised ATM/debit card transaction related civil suits in the Indonesian courts discussed earlier, it is argued that one of the probable causes of the failure of plaintiff claims is their ignorance of the importance of expert testimony and/or their inability to bring expert witnesses before the court.

¹²⁵⁹ For an example of passive attack on ATM/debit card operations, see Chapter 4 / section 4.2.1.3 of this thesis.

the consumer and so prove that the ATM/debit card transaction was indeed unauthorised.¹²⁶⁰

However, to overcome the burden of proof problem for consumers, it is submitted that the adjudicators actually can shift the burden of proof from the plaintiff to the defendant, based on the most current legislation that indicates that rule on the onus of proof is more on the side of the defendant (*LCP* and *LIET*), and/or by using a maxim in the law of tort known as the doctrine of *res ipsa loquitur* as the principle of evidence.¹²⁶¹ For that reason, the burden of proof should lie with the defendant (bank), the institution that owns all the payment infrastructure and information about the consumer's ATM/debit card transactions.

1. Onus of Proof Lies with the Defendant Based on LCP & LIET

It is argued that instead using the old law that lays the burden of proof on the plaintiff who asserts the claim (such as in HIR, RBg or Civil Code), the adjudicator should utilise *LCP* and/or *LIET* which contain newer, more specific, and better provisions on consumers protection in regard to disputes concerning unauthorised ATM/debit card transactions. The *LCP* and *LIET* both are specific regulations that implicitly shift the burden of proof from the consumer as the user of the payment card system to the bank as the provider of the payment card system. In these regulation, in principle a bank will always be deemed to be at fault or negligent (presumption of negligence) and liable for any damages incurred by a consumer in the use of bank infrastructures and/or products or services. Banks can shift the liability to a consumer only when the bank can prove that the consumer is the one who is at fault or has demonstrated negligence that enabled the occurrence of the damages.¹²⁶² Thus the onus is on the bank to prove the consumer is at fault or negligent in order to avoid liability; the onus is not on the consumer to prove the bank is negligent or at fault. This regulation's purpose is to give more protection to consumers, who are generally in a weaker or disadvantageous position compared to that of banks or producers. This approach is also deemed appropriate due to the fact that the determination of security features on ATM/debit cards, adoption of

¹²⁶⁰ Fuady, 'Perbuatan Melawan Hukum', above n 914, 99–101.

¹²⁶¹ Fred E Heckel and Fowler V Harper, 'Effect of the Doctrine of *Res Ipsa Loquitor*', (1928) 22 Illinois Law Review 724, 727.

¹²⁶² Samsul, 'Perlindungan Konsumen', above n 795, 145–6. See also arts 19(1) and 19(5) *LCP*. See also art 21(2)c and 21(5) *LIET*.

state-of-the-art technology and security features within the bank's infrastructure, procedures, and the provision of a fraud risk education policy are all in bank's exclusive hand.

2. Onus of Proof Lies with the Defendant Based on Res Ipsa Loquitur Doctrine

Res ipsa loquitur is Latin for 'the thing speaks for itself.' According to the Legal Information Institute, *res ipsa loquitur* in tort law is:

a principle that allows plaintiffs to meet their burden of proof with what is, in effect, circumstantial evidence. The plaintiff can create a rebuttable presumption of negligence by the defendant by proving that the harm would not ordinarily have occurred without negligence, that the object that caused the harm was under the defendant's control, and that there are no other plausible explanations.¹²⁶³

So in this case, the plaintiff's obligation is merely to describe the situation, the facts and nature of the damages that he/she suffered (the circumstantial evidence). The plaintiff does not need to prove his/her claim.¹²⁶⁴ In regard of circumstantial evidence, Heckel and Harper argue that 'circumstantial evidence is made sufficient, as a matter of law, to sustain a recovery in the absence of explanation by [the] defendant'.¹²⁶⁵ However, the facts related to damages should always be accompanied with a statement of the circumstances in which the damage occurred, which must make negligence a reasonable inference. Other than that, the circumstances, which became the cause of the damage, must be exclusively within the defendant's knowledge and/or that the instrumentality must have been under the defendant's exclusive control both at the time of incident and at the time of the negligent acts that are presumed to have caused the injury/damage.¹²⁶⁶

It is argued that the *res ipsa loquitur* doctrine suits unauthorised ATM/debit card transactions where the point of compromise of the identity theft method is within the bank's and/or its counterpart infrastructures — such as where malware or eavesdropping is used at an ATM/EFTPOS machine or network, or card skimmers,

¹²⁶³ Legal Information Institute, *Res Ipsa Loquitur* (<http://www.law.cornell.edu/wex/res_ipsa_loquitur>. See also Vickery and Pendleton, above n 966, 90.

¹²⁶⁴ Makarim, above n 857, 180.

¹²⁶⁵ Heckel and Harper, above n 1261, 727. See *Mayes v Kansas City Light & Power Co* (1926) 121 Kan 648, 249 Pac 599; *Eaton v New York Cent. & HRRR Co* (1990) 195 NY 267, 88 NE 378. See also Fuady, 'Perbuatan Melawan Hukum', above n 914, 100.

¹²⁶⁶ Heckel and Harper, above n 1261, 725–6. See *Mardo v Valley Smokeless Coal Co* (1924) 279 Pa 209, 123 Atl 779; *New v Bradshaw* (1922) 89 Okla 205, 214 Pac 557; *Carter Oil Co v Independent Torpedo Co* (1924) 107 Okla 209, 232 Pac 419; *Lakey v North McAlester Coal Co* (1924) 98 Okla 130, 224 Pac 309; *Goldman, etc., Bottling Co v Sindell* (1922) 140 Md 488, 117 Atl 866; *National Biscuit Co v. Wilson* (Ind 1906) 78 NE 251. See also Fuady, 'Perbuatan Melawan Hukum', above n 914, 99.

card-trapping devices, and a PIN-hole camera at an ATM. Banks as the ‘owners’ of the ATM/EFTPOS machines and their networks, obviously have full control over such infrastructure.

In Indonesia, Fuady states that the *res ipsa loquitur* doctrine can be used in tort cases as long as several conditions are fulfilled, namely that:

- (1) [such] an event usually does not occur in the absence of negligence (or intention) of the perpetrator (the perpetrator in this case is the bank);
- (2) the losses incurred are not caused by the actions of the victim;
- (3) [the] instrument which causes a loss is in the exclusive control of the party that is accused of negligence;
- (4) the negligence caused [is] within the scope of a legal obligation of the perpetrator (not of the fraud but of the negligent act) to the victim;
- (5) the victim was not negligent (no contributory negligence).¹²⁶⁷

Fuady argues that in practice, the doctrine of *res ipsa loquitur* is widely used in relation to a defendant who is an expert or a professional group member or group who is required to carry out their activities with a high degree of care or prudence. In this regard, a bank is definitely an instance of a professional financial institution that required to be very careful and skilful in its operations and obliged to exercise a high degree prudence in those operations, among other things to ensure the safety of its consumer transactions.¹²⁶⁸ Other than that, it is also argued that most successful identity theft and fraud in ATM/debit card operations are typically facilitated by a bank’s preceding and dominant negligence that might cause the occurrence of the subsequent negligent conduct of the consumer. For instance, in the card-trapping fraud method, consumer negligence in revealing his/her PIN to the con-artist may never happened if the bank had not previously been negligent in securing its consumer activated terminal.

Further, Fuady believes that the implementation of the *res ipsa loquitur* doctrine will benefit society, as:

- (1) It is more just and equitable for the parties;
- (2) There is a presumption of negligence;

¹²⁶⁷ Fuady, ‘*Perbuatan Melawan Hukum*’, above n 914, 103. See also Makarim, above n 857, 167.

¹²⁶⁸ See regulations describe in Chapter Five of this thesis, especially section 5.2.2 ‘Regulatory Framework for ATM/Debit Card Transactions: Bank Indonesia Regulations Concerning Prudential Principle, Risk Management, and Security Improvement.

- (3) 'Circumstantial' evidence is accepted;
- (4) Defendants are forced to explain the nature of the disputed occasion/incident;
- (5) There can be a solution in cases where more than one perpetrator is involved.¹²⁶⁹

In the rules of evidence law in Indonesia, the *res ipsa loquitur* doctrine can be implemented by the judge based on presumed evidence. This is derived from both Indonesia's Civil Proceedings Law (Procedural Law) and the Civil Code, as governed by Articles 1915, 1916, 1921, and 1922 of Indonesia's Civil Code.¹²⁷⁰ Zulham states that the use of the *res ipsa loquitur* doctrine is nothing but a means to preserve consumers' interests.¹²⁷¹ Subekti contends that presumption that is based on statute or fact is indeed recognised in the procedural law in Indonesia. However, Subekti argues that presumption is only 'tentative evidence', and thus it should be followed up with other evidence.¹²⁷² Sutantio and Oeripkartawinata concur with Subekti that several complementary presumptions are needed to shed light on and prove the fact that is being disputed. Presumption is needed when in the court examination process, it is very difficult to present a witness that is directly involved or knows about the facts.¹²⁷³ Judges decide on the value of the various presumptions and the facts upon which they may be based, that is, whether they have probative force or value as evidence. In other words, the judge has full authority to attribute the level of strength to the presumption, whether as perfect evidence, preliminary evidence, or lacking any probative force at

¹²⁶⁹ Fuady, 'Perbuatan Melawan Hukum', above n 914, 104–8. Fuady contends that basically the *res ipsa loquitur* doctrine is derived from the thought that it is unfair for the victim of an unlawful act (in this case the consumer) who knew nothing about the incident should bear the loss arising due to the negligent act of the perpetrator (of the negligent act, that is the bank), especially if the perpetrator of the negligent act / defendant (in this case a bank) is a party that actually understands more about the actual incident that is the basis of the dispute. In such circumstances, it is impossible for the victim to prove the perpetrator's negligence before the court. With the *res ipsa loquitur doctrine*, the burden of proof shifts from the victim to the perpetrator, and the victim does not have to prove perpetrator's negligence but the mere existence of circumstances that would indicate that such a result usually will occur if there is negligence on the part of the perpetrator would suffice.

¹²⁷⁰ Ibid 103. See art 1915 of Indonesia's Civil Code: Presupposition is a conclusion which the law or the judge draws from a known or unknown actual event that has taken place. There are two types of presuppositions: (i) presupposition based on the statute and (ii) presupposition which is not based on statute. Article 1922 of the Indonesian Civil Code states: 'Presuppositions which are not based upon the statute shall be considered by and shall be at the discretion of the judge, who shall only pay attention to those which are significant, accurate, specific, and consistent with one another. Such presupposition shall only be noted in circumstances in which the law admits evidence by witnesses, and also due to bad faith or an act or deed of deceit.' See also R Subekti, *Hukum Pembuktian* [The Law of Evidence] (PT Pradnya Paramita, 2005) 45–9.

¹²⁷¹ Zulham, Hi and Hum, above n 969, 91.

¹²⁷² Mertokusumo, 'Hukum Acara Perdata Indonesia', above n 152, 177; Simanjuntak, above n 945, 380.

¹²⁷³ Retnowulan Sutantio and Iskandar Oeripkartawinata, *Hukum Acara Perdata Dalam Teori dan Praktek* [Civil Law Proceeding in Theory and Practice] (CV Mandar Maju, 2009) 77.

all.¹²⁷⁴ However, whether or not there will be a presumption or what quality of presumption will be attributed by the judge, will rely heavily on the judge's individual knowledge. The role of 'expert witness' is very important to improving a judge's knowledge about particular facts.¹²⁷⁵

7.4.1.2.2. Test for Comparative Negligence: Between Bank and/or Consumer Negligence

Court verdicts in cases of unauthorised ATM/debit card transaction disputes (mentioned earlier) were all adjudicated and examined by the relevant Indonesian courts on the basis of tortious liability claims based on tort law.¹²⁷⁶ In order to establish tort law as a claim basis, the Indonesian Civil Code and jurisprudence requires that the perpetrator's act contain the element of fault, that is, intention or negligence, and no defence.¹²⁷⁷ Nevertheless, many flaws occurred in the CDSB and court verdicts. It is argued that most of these flaws were caused by the lack knowledge on relevant facts, legal, economic and technological, and subjective interpretation between the between consumer, bank and adjudicator of fault or negligence in the ATM/debit card operation.¹²⁷⁸

Below is the author re-visits and conducts a comparative analysis of the CDSB/court verdicts concerning unauthorised ATM/debit card transaction disputes between banks and consumers using multi-disciplinary approaches and the comparative negligence principle, and argues that many of the CDSB/court cases considerations as described earlier at Chapter Six / section 6.4.3.2.2 and 6.4.3.3.3 actually were not accurate, as follows:

- ***Evi Yulisna br Harahap v Bank Mandiri (Card Trapping Case)***

Fact of the Case:

- The plaintiff withdrew some money from the defendant's ATM at the Tanjungsari Gas Station (Medan, West Sumatra, Indonesia). The withdrawal

¹²⁷⁴ Ibid 78.

¹²⁷⁵ Teguh Samudera, *Hukum Pembuktian Dalam Acara Perdata [Evidence Law in the Law on Civil Procedure]* (Alumni, 1992) 76, 82. See also Clarke and Maurushat, above n 1246, 48–9.

¹²⁷⁶ See Chapter Six / sections 6.4.3.2.2 and 6.4.3.3.3 of this thesis.

¹²⁷⁷ See Hermansyah, above n 683, 264. 'Fault' in Article 1365 of the Indonesian Civil Code has every gradation from 'intentional fault' to 'negligence'. See also Kelsen, above n 947, 95–8.

¹²⁷⁸ See CDSB/court verdicts at Chapter Six / section 6.4.3.2.2 and 6.4.3.3.3.

failed but the card was ‘swallowed’ by the ATM. The plaintiff then called the call-centre number that appeared on the ATM to make sure that everything was under control. The plaintiff has asserted that she never revealed her PIN during the conversation. Later, the plaintiff eventually found that she had lost funds totalling IDR78 million from her account. Following the plaintiff’s report, the defendant officers admitted that someone had compromised their ATMs, but they refused to be liable for the plaintiff’s loss. The CCTV footage at the site was not up-to-date and could not be used to confirm the transactions.

- The plaintiff then filed a lawsuit with the CDSB which then concluded a verdict in favour of plaintiff and instructed the defendant to make redress for the plaintiff’s damages within 14 days of the decision. However, the defendant refused to make redress and submitted an appeal to the District Court of Medan. The case is still in trial (as at 30 August 2015).

Analysis of the Case:

- From the facts of the case (that also seems similar to Mr. Panggabean case described in the subsection 6.4.1), apparently a third party fraudster managed to install a malicious card-trapping device and stuck a fake call centre number on the defendant’s ATM. The defendant’s officer confirmed this. If this is true, it is argued that the defendant to some extent has been negligent as it failed to secure its ATM/ATM booth (occupiers’ liability), thus liable for the consumer’s damages. Further, the plaintiff admitted that she indeed called the ‘fake defendant call centre number sticker’ that was attached to the ATM to report the incident, but insisted that she did not reveal her PIN number (most consumers typically think that the sticker is genuine since it is stuck to the bank’s ATM and has a ‘perfect bank logo’).
- The CDSB judges ordered the defendant pay the plaintiff damages. According to the author, the CDSB decision was reached based on the fact that the defendant has been negligent by failing to keep its electronic agent secure — which has given the fraudster opportunity and that person/s has managed to install malicious devices (card-trapping device and fake call centre number). At this point, we can assume that the defendant was punished based on the tortious liability principle (negligence) coupled with vicarious and occupier liabilities (negligence to secure and monitor the defendant's ATM). However, apart from

the CDSB decision, the judges failed to notice that the plaintiff assertion that she did not reveal her PIN when contacting what she believed was the ‘defendant’s call centre’ actually did not make any sense (it is to be assumed that by putting a fake bank consumer call centre number on the ATM or its booth that a fraudster is attempting to use a common social engineering method to gain the consumer’s PIN, deceiving the consumer into unwittingly revealing their PIN). Most probably, a fraudster ‘apprentice’ acting as a fake bank call centre officer at the other end of the phone was successful in tricking the plaintiff to reveal her PIN). If this is the real case, then to some extent the plaintiff probably also contributed to her loss, a situation where the defendant’s liability should be reduced (comparative negligence). Nevertheless, how much the decrease in the defendant’s liability (still liable in part as it had failed to secure its ATM infrastructure) will of course still rely on many tests in relation to the degree of negligence committed by the defendant, and whether or not the defendant had previously provided education to the plaintiff about the inherent risks in the ATM/debit card operation (such as card-trapping identity theft/fraud method and fake call centre PIN theft methods).

- The CDSB decision ordered the defendant make full redress to its consumer showed that the arbitrators involved in the case basically did not understand completely about the technicality of ATM operation, the facts about the adequacy of defendant’s consumer education material, and plausible comparative negligence doctrine instead of contributory negligence doctrine that has already abandoned by most countries. The CDSB verdicts that favour consumers — even though in line with consumer protection spirit — might be deemed unfair for a bank since such a consumer had to some extent contributed to their loss.

- ***Mr Bahari v PT Bank Negara Indonesia (Persero) Tbk (Card Trapping Case)***

Facts and Analysis of the Case:

- The plaintiff is the defendant’s consumer. His ATM/debit card was trapped/swallowed by the ATM while he conducted a transaction. A stranger then stepped into the defendant’s ATM booth and encouraged the plaintiff to press the cancel button on the keypad. Nevertheless, even though the plaintiff followed this

stranger's advice, the ATM card was still trapped inside the ATM slot. After that, the plaintiff straight away visited the defendant's branch at Tebing Tinggi to report the incident. At the branch, the plaintiff met the defendant's security officer who told him that if the card was swallowed by the ATM, it meant that the card was safe. Later, it was revealed that several unauthorised withdrawals and transfers had been made from the plaintiff's account and drained his funds, with a total loss of IDR60 million.

- In accordance with these facts, it is obvious that the plaintiff's loss of funds was due to fraudulent activities by an unknown third party fraudster who had successfully installed a card-trapping device in the defendant's ATM. If this is true, it is argued that the defendant to some extent was negligent in failing to secure its ATM/ATM booth (occupiers' liability). This then contributed to a con artist being able to act as a fake 'Good Samaritan' and apparently stealing the plaintiff's PIN (using, it is assumed, the shoulder surfing method). According to *LIET*, the ATM is a bank's electronic agent. Hence, the bank, as principal of its electronic agent and the owner of the ATM/ATM booth, must be liable for its electronic agent (vicarious liability and occupier liability).
- The plaintiff then filed a lawsuit with the CDSB based on the *LCP*. In its verdict the CDSB punished the defendant by ordering it to redress the plaintiff's loss. CDSB decisions are, among other things, based on the fact that the defendant is guilty of negligence if it failed to abide by Bank Indonesia's regulations that state that the bank is to secure its ATMs (negligence per se / tortious liability), that is, by not installing CCTV and/or a security guard, which in turn enabled the fraudster to proceed with his crime and caused a loss for the plaintiff.
- The defendant then appeals to the District Court — which then, *conversely*, reaches a verdict in favour of the defendant. The District Court's decisions apparently were based on the fact that the plaintiff has a 'pure contributory negligence' that enables the loss by unintentionally letting a stranger capture his PIN (it is argued that this decision was unjust because it did not consider the negligence on the part of the defendant to secure its ATM/ATM booth which then had become the main enabler of the process of identity theft).
- Following this decision, the plaintiff appealed to the Supreme Court on the basis that the defendant failed to comply with Bank Indonesia's security regulation that

obliged all banks to have ‘chip technology’ and six digit PINs for ATM/debit cards (negligence per se) and exhibited negligence by failing to provide security guards to improve ATM security (tortious liability). Interestingly, the Supreme Court concurred with plaintiff’s argument and overturned the district court decision. It ordered the defendant to fully redress the plaintiff’s damages based on several argumentations as follows (which, according to author analysis, are not entirely accurate):

- (1). The judges believed that the plaintiff never revealed his PIN (the plaintiff argued that he only pressed the cancel button). This argumentation from a technical ATM operation point of view, is hard to believe. According to the author’s knowledge of the technical operation of ATM/debit card systems — and also based on several interviews with card-trapping victims such as Mr. Panggabean — as a victim is often in a state of panic, with their ATM/debit card trapped inside an ATM slot, victims generally follow the deceitful instruction from a stranger acting as a ‘Good Samaritan’ to key their PIN into the ATM PIN pad in order to make the ATM machine spit the card out. Thus, the plaintiff in this case was probably not aware that he was being observed by the con artist when keying in the PIN (identity theft using the ‘shoulder surfing’ method). From the author’s knowledge of the technical operations of ATMs, just pressing the ‘cancel button’ will never reveal the plaintiff’s PIN, but only will reverse the transaction to the previous stage. Judges’ argumentation in this matter has shown that in general they do not understand how ATMs work, which tends to make their decisions misleading, lacking in substance, and not credible.
- (2). The plaintiff reported the incident to the security officer in the bank branch within 15 minutes of the incident. According to the author’s opinion, this fact well supported the final judges’ decisions, since the defendant’s security officer failed to treat the plaintiff’s report appropriately and immediately, which would otherwise have prompted the adoption of a mitigation process to avoid consumer’s subsequent loss (vicarious and negligence liability principle).
- (3). The judges concluded that the defendant had failed to comply with Bank Indonesia’s security regulation and so permitted the fraudster to install the

malicious card-trapping device. It had also failed to provide a security guard at the ATM booth (negligence per se and tortious liability. These are, it is argued, very sensible considerations by the judges).

(4). The judges decided that the defendant had not complied with Bank Indonesia's regulation concerning the minimum digit for PINs. (The judges believed it was supposed to be six digits instead of just four digits. Actually, this consideration was a fatal mistake made by the judges in the Court of cassation, since the obligation to change the consumer PIN to six digits still is yet apply, coming into effect on 1 January 2016. More interestingly, this obvious mistake made by Court of cassation judges was later brought by the defendant into the final stage — the 'case review' stage in the Supreme Court. Surprisingly, this incorrect Supreme Court judges verdict was backed up by the Supreme Court civil case review judges on the basis that the Court of cassation judges had applied the right law (which actually is wrong).

- This Supreme Court's final verdict became the sole verdict that so far favours a consumer. Unfortunately the decision was never plausible since it contains a few incorrect and fatal considerations (points (1) and (4) of the Judges' reasoning).

- ***Muhajidin Tahir, SE v PT Bank Mandiri (Persero) Tbk and PT Advantage CSM (Card Trapping Case)***

Facts and Analysis of the Case:

- The plaintiff is a consumer who authorised his wife to make a transaction using his ATM card and PIN. It was very unfortunate that while his wife was making a transaction in the defendant's ATM, the ATM card was trapped in a card-trapping device installed by the third party fraudster in the ATM slot. Further, the ATM PIN was also obtained by fraudster, as the plaintiff's wife was ensnared by the con artist who acted as a 'Good Samaritan' who was 'helping' the plaintiff's wife to unwittingly contact a fake call centre. As result, the plaintiff's savings in the defendant institution were drained. A prolonged dispute occurred since the plaintiff's claim for redress was rejected by the defendant on the ground that the plaintiff had breached the confidentiality of the PIN by having revealed it to his

wife. Thus, according to the defendant, the loss that had occurred was triggered by the plaintiff's own fault (plaintiff's contributory negligence).

- The dispute then was brought to the CDSB under the *LCP*. The CDSB found in favour of the plaintiff and ordered the defendant to pay the damages in full, apparently on the basis that defendant had 'vicarious and occupier liability' for the ATM /ATM booth. Hence, according to the CDSB, all identity theft that occurs after a consumer's ATM card has migrated from his/her possession to the bank's infrastructures (such as when a payment card has inserted into the ATM slot) will then be the bank's responsibility and liability will attach to the bank. Meanwhile, the plaintiff's conduct in revealing the ATM PIN to his wife was — according to CDSB — not a breach of a contract since it is recognised under customary law (*adat*). However, it is unfortunate that the CDSB did not dig further into the question of the existence of 'negligence' on the part of plaintiff's wife by unwittingly revealing the PIN to others.
- The defendant then appealed to the District Court on the basis that the defendant had educated the consumer quite well including by issuing its official contact centre number, hence the plaintiff's loss was basically derived from the plaintiff's own fault by giving his confidential PIN to his wife who then called the fraudster's phone number instead of defendant's official phone number (which had been given to the plaintiff). The District Court issued a verdict in favour of the plaintiff and rejected the defendant's appeal. Importantly, the verdict also confirmed that the liability dumping provision in defendant's standard contract was in violation of the *LCP*, and hence should be deemed null and void.
- The defendant then made a cassation to the Supreme Court on the ground that the defendant had abided by Bank Indonesia regulations concerning payment card operation, consumer protection and so on, and had educated the plaintiff about the importance of PIN secrecy. In regard to liability dumping provision, the defendant argued that this provision was a customary provision in the payment system industry. Concerning the loss, the defendant asserted that it happened due to the plaintiff's own fault, not because the defendant's infrastructure had weaknesses. In contrast to the CDSB and District Court decisions, the Supreme Court decision was in favour of the defendant, on a basis similar to the defendant's argumentation above.

- Apparently in this verdict, the Supreme Court decision was based on pure contributory negligence, that is, the plaintiff was negligent in revealing the ATM PIN to his wife who later revealed it to the fraudster. Interestingly, the fact that the defendant failed to safeguard the safety of their consumers — that is, was negligent in terms of failing to prevent their ATM booth from having malicious devices installed by a third party (occupiers' liability) that became the main enabler of the identity theft — was not discussed whatsoever by the judges. It is argued that if a bank could prevent a fraudster from setting up their card-trapping device at an ATM, the question of consumer fault would never have arisen. The matter of consumer 'fault', where a consumer revealed his PIN and authorised his wife to conduct a transaction would not have become a problem as her action would never have been able to be used to create an unauthorised ATM/debit card transaction. Therefore, this court's verdict seems unfair for consumer and did not create incentives for bank to improve the security of its ATMs/ATM booths.

- ***Nasruddin v PT Bank Mandiri Tbk (Card Trapping Case)***

Facts and Analysis of the Case:

- The plaintiff is a defendant's consumer who holds a ATM/debit card issued by the defendant. According to plaintiff's explanation, he was about to withdraw money from an ATM of the defendant when his ATM was trapped in the ATM slot when he attempted to cancel an incorrect transaction. He then called the defendant's call centre number that appeared on the defendant's sticker that was stuck on the body of the ATM. He answered several questions from the 'defendant's call centre officer' named Iskandar. These questions included his ATM card number, mother's maiden name and so on. Subsequently, the plaintiff found that his savings in the defendant institution had been drained.
- Later, the plaintiff obtained information from the defendant's officer that accepted the plaintiff's loss of funds report and from a school guard near the compromised ATM premises; both of them concurred that card-trapping frauds frequently occurred in association with the particular ATM. As a result, the plaintiff alleges that the defendant was negligent in failing to secure the ATM from card-trapping fraud even though many crimes had frequently occurred at the scene (if this is the case, then this is indeed a foreseeable risk). The plaintiff argued that the defendant

should put a security officer at the ATM site and conduct closer security monitoring. The absence of such security precautions by defendant were believed to have caused damage to a number of its consumers;

- However, apart from the fact that the plaintiff's ATM/debit card was really entrapped in the defendant's ATM slot, it seems that the rest of the story was not true. From the point of view of ATM operations, if the plaintiff just pressed the 'cancel button', it will not cause the ATM/debit card to be trapped inside the ATM. Most probably, based on the card-trapping method typology, a fraudster/s had managed to install the card-trapping device in the ATM slot and stuck a fake bank call centre number on the body of the ATM. Thus, when the plaintiff inserted his ATM/debit card into the ATM slot, the card-trapping device entrapped the ATM/debit card inside the slot, but did not activate the ATM system. Therefore, the plaintiff's story about entering the incorrect amount and then pressing the cancelation button that caused his ATM/debit card to be trapped in the ATM slot was deemed to be false information because in the card-trapping fraud method typically the ATM system is still not in an active mode.
- The plaintiff then filed a lawsuit against the defendant to the District Court based on tortious liabilities governed by articles 1365 and 1366 of Indonesia's Civil Code, where the defendant allegedly had:
 - 1) violated the law (that is, the obligation of the defendant under Bank Indonesia regulations to safeguard and improve payment card security, and obligations under the *LCP* to provide comfort, security and safety for those utilising the defendant's services — occupiers' liability);
 - 2) violated the subjective right of the plaintiff to protection of his deposit in the defendant institution;
 - 3) breached duty of care requirements to safeguard and improve the security of its payment cards;
 - 4) undertaken unlawful conduct that caused the plaintiff damage.
- Following the allegation, the defendant raised several defences as follow:
 - 1) The fraudster (referred to as Mr Iskandar) was the one who should be liable for the plaintiff's loss (*novus actus interveniens* — intervening causation). Therefore, the defendant argued that the civil lawsuit only could be

adjudicated after the fraudster's criminal offence had been tried in a criminal court.

- 2) The litigation only could proceed if the fraudster also could be a party to and present before the court.
 - 3) The plaintiff's loss was due to the plaintiff's own negligence in revealing his PIN to someone other than the defendant's official staff.
 - 4) The defendant had fulfilled its obligation to improve its ATM security, and had also conducted various consumer education initiatives including disseminating their official call centre number to consumers.
- After examining the case, the District Court issued a verdict as follows:
- 1) That the civil lawsuit can be examined by the court without the need to have the fraudster tried for (and convicted of) a criminal offence preceding any civil action. Hence, *novus actus interveniens* is not a defence in the defendant's tortious liability cases.
 - 2) The defendant was not liable for the plaintiff's loss on the grounds that:
 - a) The defendant had provided enough security for their ATM;
 - b) The plaintiff was unsuccessful in their attempt to prove that many other consumers had also become the victim of card-trapping fraud method at the defendant's ATM;
 - c) The plaintiff should have been more vigilant when seeing a spurious call centre number for the defendant and the existence of such a number on the defendant's ATM does not automatically mean that the defendant has conducted an unlawful act;
 - d) The defendant had done enough to publish its official call centre number;
 - e) The plaintiff should be responsible for their PIN secrecy and deemed responsible if it is used by an unauthorised person.
- Again, the court's verdict ignored the fact that bank's failure to prevent the fraudster's card-trapping devices being set up at the bank's ATM was the main contributing factor that enabled the identity theft/fraud to occur. The court also ignored the fact that bank's consumer education about the bank's genuine call centre number is not the same as the fraud risk education required by regulations.

- These unfortunate circumstances are also exacerbated by the use of the old and unjust contributory negligence doctrine in the litigation.¹²⁷⁹ It is argued that the court's use of the pure contributory negligence principle to favour the defendant in the court's decision — when that defendant actually exhibited greater contributory negligence in regard to the occurrence of card-trapping fraud than the plaintiff — was neither fair nor sensible. Therefore, it is argued that law reform in regard to unauthorised ATM/debit card transactions should also include reform of ADR/court litigation proceedings processes.

Fuady contends that according to Articles 1365 and 1366 of the Indonesian Civil Code, for an unlawful act to be viewed as a tort or to have created tortious liability, it should contain the following elements:¹²⁸⁰

- (1) An act. It is generally accepted that tort or unlawful act not only consists of an action (an act of commission), but also failing to do something (an act of omission).¹²⁸¹
- (2) Such act being unlawful. After the case of *Lindenbaum v Cohen* in 1919, the element of unlawfulness must be interpreted in the broadest sense, which includes: (a) acts that violate applicable laws; (b) acts that violate the rights of others that are guaranteed by law; (c) acts contrary to the legal obligations of the perpetrator; (d) acts contrary to morality or decency; and/or (e) acts contrary to good manners in society (failure to consider the interests of others).
- (3) Culpa or fault. In order to use Article 1365 of the Indonesian Civil Code in a tort claim, the law and jurisprudence require that there is a fault element in the perpetrator's act. An act would be considered to contain the fault element if it has met the following criteria: intention or negligence, and no defence.¹²⁸² In this regard, an unlawful act intentionally committed has a higher degree of fault compared to an unlawful act that occurred due to negligent conduct. An act will be depicted as having 'intention' if it possesses the following elements: (a) an awareness (state of mind) to perform the act; (b) the act leads to a particular

¹²⁷⁹ See general discussion about CDSB and court litigation flaws in Chapter Seven / sections 7.2.2.2 and 7.2.2.4 of this thesis.

¹²⁸⁰ Fuady, '*Perbuatan Melawan Hukum*', above n 914, 99–103.

¹²⁸¹ Soeroso, above n 844, 294; Hermansyah, above n 683, 260. See also Sidabalok, above n 792, 107–11.

¹²⁸² See Hermansyah, above n 683, 264. 'Fault' in Article 1365 of the Indonesian Civil Code has every gradation from 'intentional fault' to 'negligence'. See also Kelsen, above n 947, 95–8.

consequence; and (c) the ‘awareness of commission or omission of an act is not just that it will inflict certain consequences, but includes the belief that the existence of the act ‘certainly’ can produce the intended consequences. In this regard, even where the perpetrator of a particular action (or an omission) does not intend to harm others, however, the perpetrator can still be considered to have an intention to commit an unlawful act, when the offender knows or is reasonably suspected of knowing that his actions/omission would cause a loss to another person.¹²⁸³

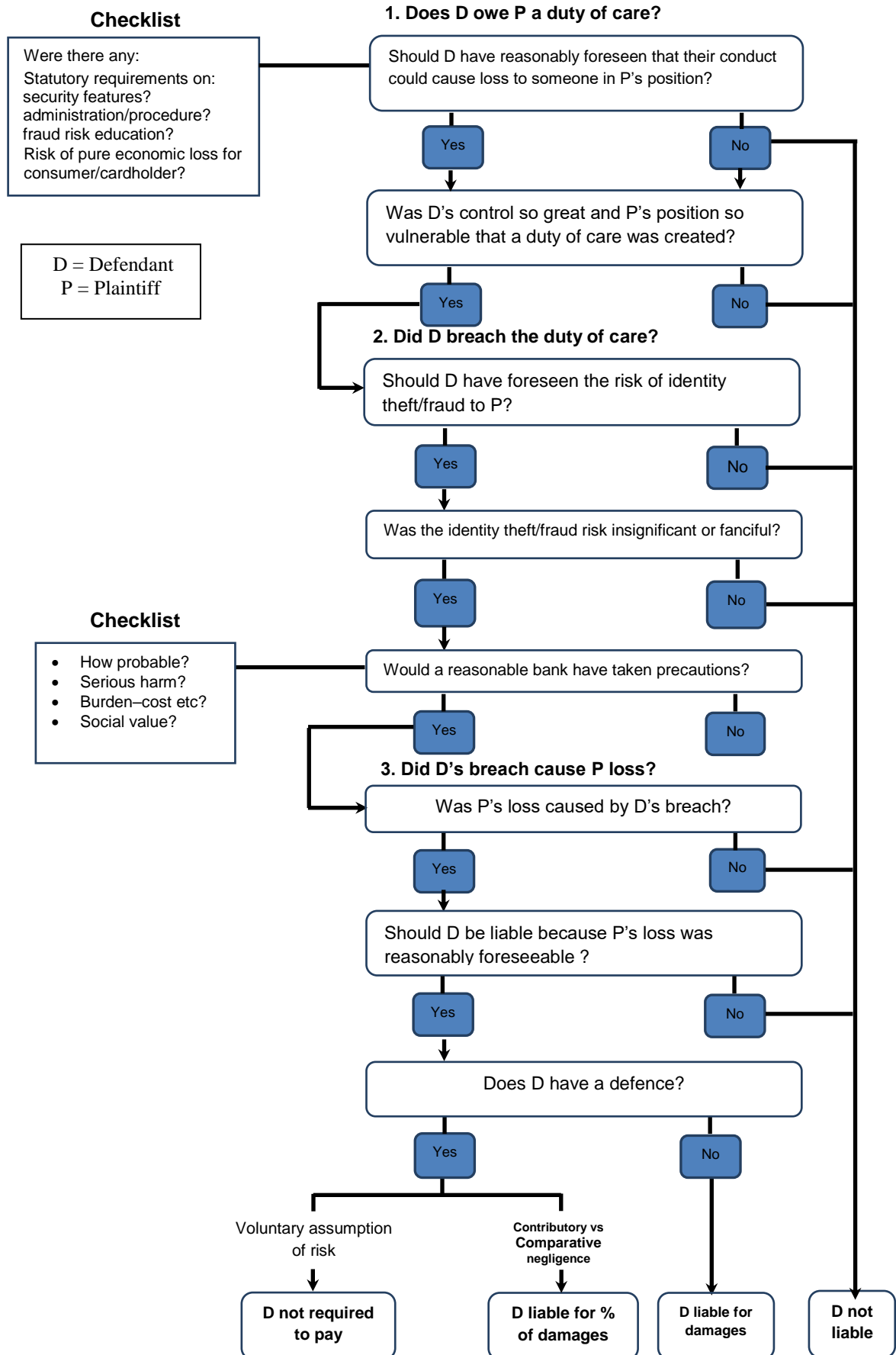
- (4) An occurrence of damages suffered by the victim. Damages here include not only actual damages but also immaterial damages, which can be valued monetarily.
- (5) Causality between an unlawful act and the associated damages.¹²⁸⁴

As a guidance for the test of comparative negligence in the tortuous liability cases, it is argued that a flow chart for negligence test below (Figure 20) — that used to be utilised in court proceedings in common law countries — if examined carefully using a multi disciplinary approach (involving economic, technological and legal perspectives) will supply great assistance to payment card stakeholders, especially for payment system authority and adjudicators. It could thus be used to fairly gauge the comparative negligence of acts undertaken by banks and/or consumers that contributed to the occurrence of unauthorised ATM/debit card transactions in Indonesia. It is believed that fair allocation of losses between banks and/or consumers based on comparative negligence could create proportional incentives for banks and/or consumers to improve precautions taken against identity theft and/or fraud in ATM/debit card operations.

¹²⁸³ Marzuki, ‘*Pengantar Ilmu Hukum*’, above n 155, 258–9; Kelsen, above n 947, 95–8.

¹²⁸⁴ Fuady, ‘*Perbuatan Melawan Hukum*’, above n 914, 5–9. See also Sidabalok, above n 792, 108; Gibson and Fraser, above n 917, 10–14, 45–50, 83–4; Shofie, *Kapita Selekta Hukum Perlindungan Konsumen di Indonesia*, above n 683, 297; Kristiyanti, above n 928, 78–9; Muhammad, above n 954, 260; Hermansyah, above n 683, 264–5; Simanjuntak, above n 945, 353–4; Setiawan, ‘*Aneka Masalah Hukum dan Hukum Acara Perdata*’, above n 939, 281–8.

Figure 20: Flow Chart of Tests for Negligence



1. Do the Defendants Owe the Plaintiffs a Duty of Care?

a. Should the Defendants Have Reasonably Foreseen that their Conduct Could Cause Loss to Someone in the Plaintiff's Position?

As can be seen from various regulations on ATM/debit card transactions, consumer protection, and liability rules on unauthorised ATM/debit card transactions in Indonesia as described in the Chapter Five (ATM/debit card security, consumer protection, and liability regulations) and information contained in the Table 5, a bank as a financial institution and owner of e-banking infrastructure is obliged by regulations to be aware of, prevent and mitigate various inherent fraud risks in e-bank operations, such as in ATM/debit card operations.¹²⁸⁵

From the empirical evidence it is known that bank ATM/debit card systems are considered a relatively easy and prominent target for fraudsters.¹²⁸⁶ A bank's inability to establish good security technology on their ATM/debit card infrastructure — including good procedures for identification, authentication, and authorisation of ATM/debit cards; and/or the delivery of quality fraud risk education material to consumers — could result in the occurrence of unauthorised ATM/debit card transactions that can drain consumer deposits at the bank.

From the many reports by consumers, in the mass media or by the central bank of unauthorised ATM/debit card fraud incidents,¹²⁸⁷ most consumer ATM/debit card identity theft and fraud incidents in Indonesia (such as skimming, card trapping, malware, social engineering, PIN theft using PIN-hole camera, PIN-pad overlay, malware, counterfeit card, and other methods) should be considered foreseeable risks, because they have occurred frequently either in Indonesia and/or in various overseas countries for a long time. In this regard, a bank as a professional entity and one that has a special fraud unit arguably know the nature of these identity theft and fraud risks, including the factors that enable such events to happen. For instance, the risk of unauthorised ATM/debit card transactions using skimming, card trapping, malware and counterfeit card is still high as long as the bank still employs magnetic stripe card

¹²⁸⁵ See BID-RMUITCB. In this regulation various inherent identity theft/fraud risks in e-banking operations have been enumerated, such as the risk of skimming, network interception, 'man-in-the middle' attack, virus, '*phishing*', key logging, 'spoofing', social engineering, and so on.

¹²⁸⁶ See discussion in Chapter Three.

¹²⁸⁷ For instances of ATM/debit card fraud reports, see the skimming deluge case in 2010 and 2013, the Body Shop case, and the bank ATM/debit card fraud data in Table 1.

technology and is unable to fully monitor and secure their consumer activated terminals from the possibility of fraudster attack that uses various kind of malicious devices. It is submitted that banks actually can foresee the risk of identity theft and fraud to their consumers in ATM/debit card operations in Indonesia (owe profesionall liability to its consumer).

b. Was the Defendant's Control so Great and Plaintiff's Position so Vulnerable that a Duty of Care was Created?

A bank as a fiduciary, prudential and professional institution is obliged by the ATM/debit card security, consumer protection, and liability regulations to safeguard its consumer transactions by regularly enhanced and implemented state-of-the art fraud risk management of the people, processes, and technology involved in electronic banking operations. This obligation is derived from the fact that consumer as a layperson in the bank's ATM/debit card operation is very vulnerable to fraudulent activities.

In theory, consumers can reduce losses by improving ordinary prudence, knowledge of various fraud method, and exercising due care in making payments.¹²⁸⁸ However, most consumers are not familiar with technology and how it works. The absence of fraud risk education by banks, and the fact that banks only give positive education about the 'infallibility' of their ATM/debit card operations, has made consumers more vulnerable due to a false sense of security and an incapacity to detect identity theft methods due to the absence of adequate fraud risk education. A false sense of security is bad because it does not encourage consumers implement precautions in regards to fraud risk.¹²⁸⁹

Banks can reduce payment losses by taking precautions against fraud according to the specific circumstances and fraud typology. Choices about the quality and level of security either of the infrastructure and procedures under the control of bank (such as the installation of state-the-art ATM/EFT-POS machines, antivirus software, encryption software, CCTVs, and employment of security guard personnel, their number and hours) and in regard to infrastructure that is transferred so as to be under the control of consumers (such as the security and quality of chip and/or magnetic ATM/debit card, number of PIN digits, and fraud risk material) — all are determined exclusively by

¹²⁸⁸ Cooter and Rubin, above n 105, 73.

¹²⁸⁹ See CPSS, 'Core Principles for Systemically Important Payment Systems', above n 3176.

bank. In this regard, consumers do not have options at all and can merely accept and use what their bank has provided.

Several instances of specific statutory duty imposed by regulations on a bank in its ATM/debit card operations include (among other things) the obligation to:

- provide physical security for important information processing facilities, such as by the regular maintenance and inspection of the bank's ATM/ATM booth/EFTPOS-terminals — so the bank can prevent or remove any malicious device (such as a card-trapping device, a skimming device, a PIN-hole camera/PIN-pad overlay device, malware, and so on) to guarantee the safety of consumer transactions;
- provide CCTV to the ATM/ATM booth — so the bank can have complete information regarding who initiates an ATM/debit card transaction and/or whether or not an attacker has set-up a malicious device at the ATM /ATM booth;
- provide antivirus software to the operating system, application system, database and network — so the bank and/or its counterpart agent institutions can detect and remove any malicious software (malware) that might be placed in or on the ATM/EFT-POS machine/computer and/or bank/counterpart host computer (such as viruses, Trojan horses, worms, spyware, Denial-of-Service (DOS), war driving, 'spoofing', and 'logic bombs');
- provide an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), and encryption for data communicated through communication lines — so the bank can detect any eavesdropping attack and/or assure data confidentiality and integrity;
- provide and deliver adequate and comprehensive fraud risk education materials by letter to the consumers — so consumers can have an awareness of the risk and take adequate precautions against the possibility of the occurrence identity theft and fraud in ATM/debit card operations.¹²⁹⁰

The statutory duties that mainly address banks instead of consumers indeed make sense considering that banks are the owners of the e-banking system. As Cooter and Rubin

¹²⁹⁰ It is worth noting that consumer education that lacks fraud risk material and/or is not delivered individually to the consumer (such as consumer education material that is only placed on a website, pamphlet, or mass-media) is deemed inadequate.

argue, the bank is the party that has an ‘innovation element’, that is, it has the possibility to innovate and improve its electronic payment transaction systems. Unlike the precautions element, which initially can be addressed by financial institutions and consumers, in the innovation element, the pendulum of liability will always swing to the financial institutions as the only party that own, develop, and have an obligation to comply with *LIET* in general and Bank Indonesia’s specific regulations concerning enhancement of payment card security features. Hence, ‘if technological innovation is the cheapest way to eliminate a particular type of loss, liability should be assigned to the financial institution’.¹²⁹¹ From the perspective of innovation, loss allocation rules that assign liability to the financial institution can benefit banks, consumers and the payment system industry as there is an incentive for the bank to continually improve anti-fraud technology through innovation.¹²⁹²

In conclusion, banks in Indonesia definitely should have foreseen the fraud risk to consumers in the ATM/debit card operation. The various regulations imposed by the authorities on banks is in the context of safeguarding consumers as the most vulnerable party in the ATM/debit card system and is part of a bank’s duty of care obligation to its consumers. Therefore, according to the scope of tort based on the Indonesian Civil Code and the landmark case of *Lindenbaum v Cohen*, a defendant’s action or omission that fail to prevent and mitigate identity theft and fraud in the ATM/debit card operation can be deemed as a tortious action because it is in conflict with:

- the plaintiff’s right to have secure ATM/debit card infrastructure and fraud risk education;
- the defendant’s own legal obligation/statutory duty to provide various risk management and security enhancement in ATM/debit card operations;
- morality (banks need to admit their systems are not infallible and that there exists inherent risk in ATM/debit card operations); and/or
- a bank’s professional standing and its adherence to the prudential principle.

¹²⁹¹ Cooter and Rubin, above n 105, 84.

¹²⁹² Ibid 77.

2. Did the Defendants Breach their Duty of Care?

a. Should the Defendants have Foreseen the Risk of Identity Theft/Fraud to the Plaintiff?

Improved technology in retail e-banking transactions such as in ATM/debit card transactions offers many opportunities for Indonesia banks and consumers such as the increased efficiency, quicker transactions, increased consumer loyalty, and more, but many aspects of fraud development can also be related to technology. The very important question is whether the various identity theft and fraud risks, such as skimming, card trapping, malware, counterfeiting card, and so on are new risks or actually foreseeable risks?

In the case of Indonesia, it is argued that most identity theft and fraud in ATM/debit card operations are foreseeable risks for banks.¹²⁹³ Lost and stolen cards, skimming, card trapping (Lebanese loop), malware and other kinds of criminal methods have been around in Indonesia for quite some time. Almost all of these identity theft and fraud methods have occurred earlier in other countries ATM/debit card operations. Generally, various international journals, bank and technology related newspapers and/or websites (whether official website or simply just technology bloggers), specific security risk magazines, or the like have openly discussed those identity theft and fraud methods quite exhaustively.

Within a bank's management, typically a bank's risk management unit staff members have shared and discussed such information with their counterparts in the various international or domestic banking forums. Many banks have also been reporting instances to the authorities for quite some time now. For instance, Bank International Indonesia reported a skimming attack incident at one of its ATM booths to Bank Indonesia in 1996. The Jakarta District Court convicted Eng Kim Hook, a Malaysian citizen, of skimming fraud in 2003.¹²⁹⁴ This instance occurred long before the 'skimming deluge' that occurred in 2010 and 2013 in many cities in Indonesia (not to mention the individual skimming incidents that randomly occur intermittently and can be seen from consumers' complaints shared in mass-media).

¹²⁹³ See discussion in the Chapter Three / section 3.3.5 and Chapter Four.

¹²⁹⁴ See Jakarta Court Verdict No 532/PID.B/2003/PH.JKT.PST dated 4 June 2003.

Therefore, from the time such identity thefts and fraud methods occurred and/or were reported publicly onwards, banks had a duty to take reasonable care of consumers exposed to such risks. Conversely, given the lack of fraud risk education of consumers by the banks, it is also submitted that most identity theft and fraud methods discussed above are not foreseeable risks for consumers, unless their bank can prove that they had already given adequate fraud risk education to consumers.

b. Was the Identity Theft/Fraud Risk not Insignificant or Fanciful?

Identity theft and fraud risks are real and not insignificant nor far-fetched or fanciful. Its existence and relatively significant exposure in term of volume and value can be seen from various individual consumer reports in the mass-media, Bank Indonesia official reports,¹²⁹⁵ or from several unauthorised ATM/debit card transaction disputes adjudicated in ADR and/or court.¹²⁹⁶ Even though the fraud figures are deemed significant, many believe that because of the ‘dark figure’ phenomenon, the actual fraud figures are far higher than those presented in the official fraud reports. Moreover, the losses of consumers due to identity theft and fraud actually are not only related to the pecuniary loss such as fraud damages and/or litigation costs, but also to several other non-pecuniary losses, such as mental distress, hassles, and so on. In conclusion, the ATM/Debit card identity theft and fraud risks are indeed significant.

c. Would a Reasonable Bank Have Taken Precautions?

A bank is a professional institution. Banks, which carry on activities requiring special skill or knowledge, are required to assure a reasonable standard or care expected of competent practitioners in the banking industry.¹²⁹⁷ Based on ATM/debit card security, consumer protection, and liability regulations, a bank is required to understand the inherent risk in their operations. A bank as a professional institution is obliged to secure its infrastructure and possess lots of information about various trends in identity theft and fraud methods. A bank also has an obligation to educate its consumers about any inherent risk its products and/or services. In general, a bank is obliged to guarantee the safety of its consumers when using its products and/or services. In this regard, Geva has

¹²⁹⁵ See Table 1.

¹²⁹⁶ See consumer redress claims in several adjudication cases discussed in Chapter Six / sections 6.6.4.2.2 and 6.6.4.3.

¹²⁹⁷ See Stewart and Stuhmcke, above n 912, 158–68.

stated that a bank can be charged with a duty of care failure if it fails to ensure the safety and security of its public-access terminals.¹²⁹⁸

Empirical evidence in Indonesia has shown that several reasonable banks indeed have taken precautions to contain identity theft and fraud in fulfilment of the security enhancement regulations. Some examples of bank security enhancement are: replacing old ATM/EFT-POS machines with new ones that are considered more sophisticated and secure,¹²⁹⁹ and installing jitters, anti-skimming devices, CCTV and so on to combat skimming fraud. A small number of banks — even though not yet obliged by Bank Indonesia's regulations — have also taken precautions to mitigate unauthorised ATM/debit card transactions by implementing 'neural network applications' on their ATM/debit card systems to enable 'real time' transaction notification for consumers. Therefore, it is argued that banks as professional and fiduciary institutions should always have to safeguard their consumers and taken precautions against identity theft and fraud risks.

3. Did the Defendant's Breach Cause Loss to Plaintiff?

a. Was the Plaintiff's Loss Caused by the Defendant's Breach?

Identity theft in an ATM/debit card operation that subsequently becomes an unauthorised ATM/debit card transaction (identity fraud) is regrettably becoming more frequent, an unfortunate aspect of current electronic payment operations around the world, including in Indonesia. Unauthorised ATM/debit card transactions typically cause financial losses for the affected consumer, either from unauthorised money withdrawals at ATMs or unauthorised electronic fund transfers.

In the case of ATM/debit card operations in Indonesia, a bank is obliged by ATM/debit card security, consumer protection, and liability regulations to implement a secure system for all ATM/debit card operations. This includes a safe and robust distribution of ATM/debit card instruments (access devices), identification, authentication and authorisation of electronic payment instructions procedures, and effective fraud risk education for consumers. Banks are also obliged to mitigate the fraud risk, as there is the risk that some incidents will nevertheless still happen — such as by providing

¹²⁹⁸ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 231.

¹²⁹⁹ Such as having a sensor to spot any malicious device set up inside an ATM slot, a camera in front that automatically snaps the cardholder, and so on.

reports and effective systems of blocking unauthorised ATM/debit card transactions upon being advised of the loss or theft of the consumer's access device.

In respect of the Cooter and Rubin economic approach and the loss reduction principle, the bank is a cheaper cost avoider for identity theft and fraud perpetrated by third party fraudsters who attack bank infrastructure. In this regard, banks can invest in state-of-the-art ATM/debit card infrastructure to prevent and/or reduce losses that might occur because of technical vulnerabilities and/or insecurity of bank infrastructure. The occurrence of identity theft incidents to consumer ATM/debit card data and PIN using identity theft methods such as malware, card trapping, skimming, and so on are evidence of a bank's inability to secure their ATM/debit card infrastructure.

The pervasive incidents of card swapping, card trapping, PIN theft using fake bank call centre stickers and/or a con artist (social engineering) on bank ATM/debit card operations can arguably also be blamed on the banks for their reluctance to give fraud risk education to consumers.

Many scholars concur that good fraud risk education can create precautionary attitudes among consumer.¹³⁰⁰ By knowing the nature and typology of identity theft and fraud methods, consumers can most probably avoid several types of identity theft methods, especially the tangible methods of identity theft such as card trapping, the use of fake call centre number, card swapping, and con artist (social engineering method). However, it is submitted that passive identity theft attacks — such as skimming, malware, eavesdropping, hacking, PIN-hole camera, and PIN-pad overlays — are types of intangible identity theft methods that can only be prevented and removed by banks as the owner of the system. Therefore, in such cases, the plaintiff's loss indeed finds its causality in the defendant's breach of the security and consumer protection regulations.

However, there is also the possibility that a plaintiff's loss is due to a consumer's own criminal intention to defraud bank (first party fraud), or due to the actions of someone acquainted with the consumer (second party fraud). In first party fraud, the person is criminally liable and a bank's compliance or not to the regulations is not relevant because the fraudster legitimately possesses all authentication factors (card and PIN). In

¹³⁰⁰ See Kitten, *3Reason Skimmers are Winning*, above n 1134. See also BCBS, *Risk Management for Electronic Banking and Electronic Money Activities*, above n 3, 6–7.

second party fraud, it is argued that the occurrence of identity theft and fraud perpetrated by an acquaintance of the consumer (relative or friend, workmate and so on) is due to the consumer's own negligence in failing to safeguard their ATM/debit card and associated PIN, an act that is beyond bank control. Other than this, there are also many examples where consumer negligence indeed becomes the main enabler in the success of fraudulent activities, such as where a consumer loses their ATM/debit card and the PIN was written on the ATM/debit card or the PIN uses the consumer's birthday date. In these examples, the consumer is the cheaper cost avoider. However, the latter statement can only be granted if the bank has previously informed the consumer with fraud risk education as obliged by regulation.

b. Should a Defendant be Liable Because a Plaintiff's Loss was Reasonably Foreseeable?

As has been discussed previously in section 7.3.2.2, ATM/debit card identity theft/fraud typology (card present transaction) can be divided according to the perpetrators and/or point of compromise into two broad categories, namely: 1) the first/second party identity theft/fraud typology; and 2) the third party identity theft/fraud typology. The third party identity theft/fraud typology can be further subdivided into three different circumstances of ATM/debit card identity theft/fraud, as follows: a) the lost and/or stolen ATM/debit card which targets the consumer as the point of compromise; b) the lost and/or stolen ATM/debit card which target consumer and bank infrastructure as a joint point of compromise; and c) the counterfeit ATM/debit card.

Even though this thesis argues that most ATM/debit card identity theft/fraud risks are foreseeable, it is submitted that in tortious liability adjudication/litigation, the fraud damages only can be awarded in full to the plaintiff if the defendant — from economic and technological perspectives — is the least cost identity theft/fraud avoider. Meanwhile, in unauthorised ATM/debit card dispute cases where both defendant and plaintiff have through their fault/negligence contributed to the occurrence of identity theft/fraud, it is argued that the damages should be split between the defendant and plaintiff according to the degree of fault/negligence of their conduct (comparative negligence).

i. ***Proposed General Rules for Loss Allocation Liability Based on Multi-Disciplinary Perspectives.***

Basically, according to the *LCP* and *LIET*, a defendant is liable for consumer losses (presumed liability). A defendant's liability will be concluded in law if it is proved that the defendant has breached the duty of care owed to the consumer, and consumer is guilty of no fault/negligence that facilitated the loss. In Indonesia, the defendant's duty of care can arise from (among other things) statutory duty, ethics, and morality.¹³⁰¹ In terms of the bank's statutory duty, it is argued that the defendant's duty can be divided into two broad taxonomies, which are: 1) the duty to secure the bank's ATM/debit card infrastructure (physically and logically) from a fraudster's malicious device/software; and 2) the duty to give identity theft/fraud risk education to consumers.¹³⁰² These duties are established by the regulator because the bank is the owner of the ATM/debit card system, and has the capability to determine and sole control over determining the adoption of state-of-the-art bank infrastructure, its level of security, and provision of consumer protection (including education specific to that bank). From a law of tort perspective, the defendant owes a duty of care to protect their ATM/debit card infrastructure to ensure consumer safety from identity theft/fraud risks; to do otherwise involves a risk of negligence, occupier and vicarious liability.¹³⁰³

Nevertheless, bank liability also can be seen from another legal perspective. A bank is a professional entity, which has great resources in terms of highly skilled staff, sophisticated infrastructure, and a great amount of funds. As has been discussed in the Chapter 6.2.2, the law of tort itself consists of intentional, unintentional and miscellaneous tort. An unlawful intentional act has a higher degree of fault compared to an unlawful act that occurred due to negligent conduct. According to Marzuki and Kelsen, an act or omission that does not intend to harm others can still be considered to have an intention to commit an unlawful act, when the perpetrators knows or is reasonably suspected of knowing that their action/omission would cause a loss to another person.¹³⁰⁴ In this regard, Douglass has argued that putting liability on the

¹³⁰¹ See explanation about tort at Chapter Six / section 6.2.2 on tortious liability.

¹³⁰² The consumer's fraud risk education should consist of comprehensive information about identity theft/fraud methods and ways to avoid them. This fraud risk material also should delivered individually to a consumer's address (either printed out or through electronic media). See various Bank Indonesia Regulations pertaining to risk management and the card-based payment system.

¹³⁰³ See explanation about tortious, occupier's and vicarious liability in Chapter Six of this thesis.

¹³⁰⁴ Marzuki, '*Pengantar Ilmu Hukum*', above n 155, 258–9; Kelsen, above n 947, 95–8.

defendant (bank) may have a greater benefit in terms of electronic payment system development. According to him:

Designing a card-based payment system that increases consumer liability for fraudulent transactions would likely undermine confidence in the system overall and result in reduced transaction volume — the opposite of the desired effect. Given these counterincentives among those who promulgate the applicable public laws and private rules, increased cardholder liability is likely not a viable option for improving the overall efficiency of fraud liability allocation rules.¹³⁰⁵

Therefore, it is submitted that in the unauthorised ATM/debit card transaction cases where the bank is the fraud least cost avoider, has great control of the improvement ATM/debit card infrastructure security, deep knowledge of the inherent risks of ATM/debit card operation — and given the fact that consumers have a false sense of security and severe asymmetry of information about inherent risks in the ATM/debit card operation — the bank is deemed to have performed an intentional act instead of just a negligent act that enabled the identity theft/fraud to occur.¹³⁰⁶

Thus one can say in the event of identity theft/fraud happening where the risks are obvious or foreseeable, the defendant's liability should be complete or greater than that of the consumer (in the case joint liability) because the defendant is a professional entity and the action or omission which resulted in the occurrence of identity theft/fraud can be deemed to be intentional. The allocation of losses to the bank will increase effective loss distribution, and will promote bank investment in more secure or sophisticated infrastructure.

ii. *Loss Allocation Rules Based on Multi-Disciplinary Perspectives (Economic, Technological, and Legal) of First Party Fraud Typology*

In the first party fraud typology (assuming the defendant can prove it), it is argued that this type of fraud is beyond defendant's liability. In first party fraud typology, a defendant has relatively no control *ex-ante* to prevent the loss because the unauthorised ATM/debit card transactions are derived from the plaintiff's own criminal conduct. Is

¹³⁰⁵ Douglass, above n 122, 46.

¹³⁰⁶ It is argued that a bank actually is fully aware that: a bank's ATM/debit card that still utilises a magnetic stripe card is highly vulnerable to skimming attack; the absence of anti malware or malware removal in the ATM/debit card's infrastructure's computers (either in the ATM/EFT-POS terminal and bank/counterparty party's computer) exposes the consumer's data to logical identity theft; failure to provide CCTV and a security guard to secure a bank's ATM/ATM booth can have consequence of a fraudster installing a malicious device such as a skimmer, card-trapping device, PIN-hole camera, PIN-pad overlay, fake bank's call centre number, malware, and so on.

impossible for banks to know a consumer's *mens rea* in instances where the fraudulent transaction is executed using the right and legitimate authentication method. The consumer is deemed liable if he/she acted fraudulently¹³⁰⁷ and/or has benefitted from it.¹³⁰⁸ Therefore, a consumer has no legal basis to claim redress in instances of proven first party fraud.

iii. ***Loss Allocation Liability Based on Multi-Disciplinary Perspectives (Economic, Technological, and Legal) of Second Party Fraud Typology***

Meanwhile, in the second party fraud typology, the defendant also does not have liability to redress the plaintiff's damages, because the plaintiff has a statutory duty to safeguard their ATM/debit card instrument and PIN security/secrecy from other parties, including his/her own family and/or acquaintances.¹³⁰⁹ From an identity theft/fraud avoidance perspective, the plaintiff is the only party that has the ability to prevent fraud losses at the lowest cost in the event of second party fraud. Hence, the plaintiff will be liable for his/her own loss that is caused by his/her own negligence. In this regard, Gillette argues that imposing negligence liability on consumers could be expected to induce optimal care by consumers.¹³¹⁰ Geva also asserts that 'allocating to the consumer losses caused by his or her fault will enhance diligence and minimise losses'.¹³¹¹ However, if the defendant is unable to prove that the unauthorised ATM/debit card has occurred because of a first party or second party fraud, then the defendant should bear liability.

iv. ***Loss Allocation Liability Based on Multi-Disciplinary Perspectives (Economic, Technological, and Legal) of Third Party Fraud Typology***

In the third party identity theft/fraud typology, the defendant's liability is more difficult to define. The defendant's liability will depend on whether or not the defendant has breached its duty of care and so enabled the occurrence of an unauthorised ATM/debit card transaction and whether the plaintiff has demonstrated his/her own fault/negligence, so the defendant can pass liability — either either full or in part — to the plaintiff. However, it is argued that a plaintiff can be blamed for their negligence

¹³⁰⁷ Steennot, above n 47, 555. See also Levitin, above n 114.

¹³⁰⁸ It is argued that Indonesia should have definition of 'unauthorised transaction' such as is the case in other countries. In the US an EFT will be deemed authorised if a consumer has benefitted from the transfer: (15 USC § 16931(11); 12 CFR § 205.2(m).

¹³⁰⁹ See Chapter Four / section 4.2.1.1.4.

¹³¹⁰ Gillette, above n 130, 184.

¹³¹¹ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 231.

that contributed to the identity theft/fraud, only if the defendant has given the plaintiff comprehensive fraud risk education including on ways to avoid it — thus in such circumstances the plaintiff is entitled to become the least cost avoider.¹³¹²

Therefore, in the third party identity theft/fraud scenario of lost and/or stolen ATM/debit card which target the consumer as the point of compromise alone outside a bank's perimeter, then a defendant might be not liable for the plaintiff's loss if the identity theft method was foreseeable for plaintiff and did not require specific fraud risk education, such as the risk of use of a lost/stolen ATM/debit card taken by a pickpocket or simply misplaced and the plaintiff's PIN is birthday date or easy to guess numbers or recorded on or near the card. In such instances, the plaintiff is the least cost avoider and should be liable, because the loss occurred because of the plaintiff's own fault or negligence as regulated by the *LCP* and *LIET*. It is argued that US approaches where any unauthorised transaction initiated with the access device that was obtained in an illegal manner (robbery or fraudulent inducement), regardless of the situation,¹³¹³ should be deemed unfair to the defendant who might not be the least cost avoider in such circumstances.

Nevertheless, where a plaintiff has reported an identity theft/fraud to a defendant, the defendant bears all the economic losses caused by the use of lost/stolen or misappropriated payment instrument after that notification.¹³¹⁴

However, when an identity theft method is foreseeable for the defendant but not the plaintiff, and the method is considered very tricky, exploits weaknesses in one or more defendant infrastructure, and the risk is unforeseeable for plaintiffs without a specific fraud risk education from the defendant, it is argued that to some extent the defendant should be liable for the plaintiff's loss (for instance, the plaintiff may bear a predetermined cap/limited loss liability,¹³¹⁵ and the defendant bear the remaining

¹³¹² Most consumers are laypersons and identity theft and fraud methods are specific, varied, perfectly disguised or hidden, and laypersons need special knowledge to understand them. Thus, without specific information from a bank in the form of fraud risk education as has been obliged under the regulations, the consumer will suffer a severe asymmetry of information concerning the inherent risk of identity theft and fraud in the ATM/debit card operation. In these circumstances, expecting a consumer to prevent identity theft/fraud from occurring in the ATM/debit card operation and/or liable for the consequences is absurd and unfair.

¹³¹³ See (12 CFR § 205.2(m)(3), Official Staff Commentary).

¹³¹⁴ Steennot, above n 47, 555. See also Clarke and Maurushat, above n 1246, 47.

¹³¹⁵ For instance, see Chapter Seven / section 7.5.2.3 for cardholder limited liability regulation in Australia.

loss).¹³¹⁶ An example of this circumstance is when a fraudster successfully steals the consumer's identity (and later defrauds) an ATM/debit card consumer outside bank's perimeter using the card swapping method. As has been discussed previously, in the card swapping method, a fraudster typically exploits the defendant's ATM/debit card anonymity which means that a consumer could not immediately be aware of the swap.

In the third party identity theft/fraud scenario of card trapping or card swapping which targets consumer and bank's infrastructure as a joint point of compromise, the court should observe whether a causal link exists between the plaintiff's negligent conduct and the reasonably foreseeable damage suffered by the plaintiff.¹³¹⁷ One of the principles that might be beneficial to use is the principle of 'imminent danger' (also known as the 'agony of the moment' rule', the 'sudden emergency' rule or the 'doctrine of 'alternative danger'). As Stewart and Stuhmcke observe, '[c]ourts will often not hold a plaintiff negligent where the negligence of the defendant has placed the plaintiff in a position of imminent personal danger'.¹³¹⁸

Therefore, the defendant bank might have full liability if it failed to secure its public consumer activated terminals and also failed to provide fraud education to the consumer about the foreseeable risk of the ATM/debit card operation. In this regard, the defendant is the sole least cost avoider. As Clarke and Maurushat argue, it is impracticable to make consumers responsible for the impacts of actions by banks' electronic agent/public access terminals that they did not initiate and/or authorise.¹³¹⁹ So, the defendant might be liable for all the plaintiff's loss — since the loss typically originated where the fraudster's malicious device had been successfully planted in the defendant's infrastructure to steal the ATM/debit card (a theft otherwise attributed to plaintiff 'negligence' in failing to keep their PIN secret due to a social engineering or shoulder surfing attack). As Geva asserts,

in the case of the electronic authentication, the institution is bound to implement a safe system [for] the distribution of access devices, a safe security procedure for the authentication of payment instructions, as well as an effective system of blocking access upon being advised of loss or theft of the access device. The financial institution may

¹³¹⁶ Both US and Australian loss allocation rules have a pre-determined cap on loss liability.

¹³¹⁷ Stewart and Stuhmcke, above n 912, 259–61.

¹³¹⁸ Ibid 258–9.

¹³¹⁹ Clarke and Maurushat, above n 1246, 56.

also be charged with a duty to ensure the safety and security of public-access terminal.¹³²⁰

However, the defendant's liability can be reduced and re-allocated in part to the plaintiff, if a defendant has provided the necessary fraud risk education to the consumer about the specific identity theft method utilised by the fraudsters. In this case the identity theft risk is a foreseeable risk for the plaintiff, at least the identity theft method which attacks a consumer's PIN. For instance, in the various unauthorised ATM/debit card cases that were adjudicated the ADR/court as discussed in the Chapter Six, all were related to unauthorised ATM/debit card transactions that were derived from the card-trapping identity theft method which utilises the consumer's genuine card, and they typically involved to a fake bank's call centre sticker and associated fraudulent personnel to whom the consumer unwittingly reveals their PIN, or a con artist (fake 'Good Samaritan') who steals the consumer's PIN by 'shoulder-surfing' or other means. In all these identity theft methods, the defendant is arguably the least cost avoider. For instance, to avoid the installation of card-trapping device in the bank's ATM, the defendant can replace its old ATMs with the more advance ones which can incorporate a sensor to detect a foreign object or malicious device set up in the ATM slot. The defendant bank also can place security guards to safeguard their ATMs, making sure no one can install malicious devices. Meanwhile, to avoid PIN-theft through the use of social engineering methods (such as those mentioned above), a bank could educate its consumers with regular and up to date fraud risk education which could contain information regarding various popular and prominent identity theft/fraud methods, including social engineering methods and ways how to avoid them.

In the last scenario, that of third party identity theft, which involves the use of counterfeit ATM/debit cards and typically employs sophisticated and intangible malicious device/software planted in the defendant's infrastructure and that impossible for a consumer to detect — the defendant is definitely the sole least cost avoider, and therefore should bear all the consumer's loss. For example, a bank should be liable for consumer losses that are derived from identity theft/fraud involving a consumer's ATM/debit card data and using skimming, card swallowed theft, malware, and eavesdropping.¹³²¹ A defendant bank also should liable for consumer PIN theft using a

¹³²⁰ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 231.

¹³²¹ In these identity theft methods, all the fraudster's attacks are directed to bank infrastructure such as ATM/EFTPOS machines/computers and the bank's network.

PIN-hole camera, PIN-pad overlay, malware, and/or the shoulder surfing method. As Geva asserts, 'facilitating payments without providing adequate security is a risk to be assumed by the financial institution. In effect, this means that where the customer denies responsibility, the risk ought to be allocated primarily to the financial institution that chose to facilitate a transfer not reliably authenticated'.¹³²² Further he states that 'the imposition of loss on financial institutions will enhance the development of improved technologies for precluding unauthorized transfers as well as for identifying the wrongdoer and his or her apprehension'.¹³²³

Referring to the fact that many identity theft and fraud methods and/or fraudsters malicious devices are undetected by both defendant and plaintiff, and the fact that not all banks have equipped their infrastructure with appropriate monitoring/surveillance devices, many unauthorised ATM/debit card transactions are considered as 'phantom withdrawals', that is, unauthorised ATM/debit card transactions where there is no clear evidence in regard to who the perpetrator actually was. In these circumstances, the perpetrator can be anyone, and the fraud itself might fall into the category of first party fraud, second party fraud or third party fraud typology. However, regardless of who the perpetrator was, it is argued that in this kind of circumstances, the defendant should be liable based on several argumentations, as follows:

- Based on the *LCP* and *LIET*, a defendant always is presumed liable for consumer losses. Liability will stay with the defendant when it cannot prove under the balance of probability that the plaintiff is at fault or has demonstrated negligence that enabled the loss to occur. These rules will create strong incentives for defendants as the least cost avoider to enhance their ATM/debit card system security to prevent the occurrence of identity theft/fraud, and/or to establish more advanced mitigation/surveillance methods to prevent excessive losses if a preventive measure can be penetrated, and/or to detect the perpetrators for better evidential and apprehension purposes.
- From a technological perspective, most identity theft and frauds are intertwined with technological aspects of ATM/debit card operation. Hence, it does make sense that defendant as the sole party that can secure their own infrastructure and/or third-

¹³²² Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 230.

¹³²³ Benjamin Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers' (2003) 38 *Canadian Business Law Journal* 207, 237.

party counterpart/agents and safeguard a plaintiff's transaction should be liable because the defendant typically has a statutory duty, and occupier and vicarious liability¹³²⁴ to do so.

- Defendants typically enjoy huge profits from their operations. The defendant bank's revenue is arguably much higher than the cost for security enhancement in ATM/debit card operation. Defendants also are able to absorb consumer losses from fraud by spreading the loss to others. This is done in the form of transaction fee, credit interest, and so on. Most plaintiffs, however, have no capacity to spread the loss. Hence, allocating the liability to the consumer without strong evidence and compelling reason is not only deemed unjust but also can reduce consumer confidence in electronic banking operations — something that the defendant also does not want to have happen.

c. Does the Defendant Have a Defence?

i. Voluntary Assumption of Risk

In the absence of fraud risk education undertaken by the bank, and the presence of intensive promotion of the infallibility of a bank's electronic payment system in Indonesia, it is submitted that a plaintiff does not have a precise knowledge of the inherent fraud risk and various identity theft/fraud methods that might be encountered in a ATM/debit card transaction. Instead, consumers have a false sense of security that causes them not to take any precautions when conducting ATM/debit card transactions. It is also argued that a common defence by banks in court litigation that the consumer had already been given education is utopian rather than factual. Some banks have already given security tips for consumers to improve security (such as by urging consumers to keep their PIN secret and not to reveal it to anyone, and warn consumers about fake Good Samaritans at ATM booths. However, these bank security tips normally are only placed on small sticker and stuck to the ATM body/booth.

This kind of education it is argued cannot be claimed as 'a fraud risk education' because it does not contain any information whatsoever about other identity theft/fraud methods such as other popular and the most recent the identity theft/fraud methods, fraud trend

¹³²⁴ See art 1367 Indonesia's Civil Code. See also art 21(2)b LIET; art 10 *Peraturan Bank Indonesia Nomor 16/1/PBI/2014 Tentang Perlindungan Konsumen Jasa Sistem Pembayaran* [Bank Indonesia Regulation Number 16/1/PBI/2014 Concerning Consumer Protection on Payment System Services].

data, information on how to spot a fraudster's malicious device, how to avoid it, and so on.¹³²⁵ A bank's security tip notice is relatively small and stuck onto the ATM body/booth, and has generally failed to raise consumer's fraud awareness or encouraged them to take suitable precautions because it is simply too small and also because most consumers typically already have a false sense of security and so only focus on finishing the ATM transaction as quickly as they can. Under the regulations, a bank is not only obliged to supply fraud risk education, but should also deliver it to the consumer's address individually using a written message¹³²⁶ — which has never happened in Indonesia. Hence, it can be concluded that most consumers in Indonesia have no fraud risk awareness when conducting ATM/debit card transactions.

Besides that, often in the unauthorised ATM/debit card transaction dispute proceedings, banks offer as a defence based on the assertion that their systems are infallible — thus, if there were any unauthorised ATM/debit card transaction, it must be derived from first/second party fraud, or from third party fraud that is facilitated by a consumer's own negligence. Indeed, as has been discussed previously, the consumer's fault/negligence may have contributed to an unauthorised ATM/debit card transaction. This assumption then is normally 'wrapped-up' in the bank–consumer contract's standard provisions, which contain a one sided fraud allocation loss to the consumer. In essence, the contract's provisions oblige consumers to keep their ATM/debit card safe and their PIN secret. Any misuse of these instruments by third party fraudsters will be the consumer's own responsibility and all transactions executed using correct consumer's ATM/debit card data will be deemed valid and become a consumer's own responsibility, with consequent liability if that duty is breached.

From the identity theft and fraud typology described in the section 7.3.2.2 above, the perpetrator of an unauthorised ATM/debit card transaction actually can be first party, second party or third party fraudsters. Clarke and Maurushat contend that 'who caused the unauthorised banking transaction is virtually unascertainable. Digital evidence and forensics issues exacerbate the problem'.¹³²⁷ Thus, the point of compromise can be

¹³²⁵ For a comparison with genuine fraud risk education in other countries, see fraud risk education by the Australian Payment Clearing Association (APCA) in Australia <<http://www.apca.com.au>>; Financial Fraud Action (FFA) in the United Kingdom <<http://www.financialfraudaction.org.uk>>; and Bank Negara Malaysia in Malaysia <<http://www.bnm.gov.my>>.

¹³²⁶ See *BIR-CBPI*.

¹³²⁷ Clarke and Maurushat, above n 1246, 45–6.

directed to the consumer itself, bank and/or its counterpart infrastructures alone, and one or more of them. As Budniz contends, ‘transactions involving electronic transfers are becoming ever more complex and less transparent’.¹³²⁸ In this regard, Clarke and Maurushat have warned that the facts about technical vulnerabilities in any system should always be considered from the legal and evidential perspectives. According to these authors, ‘the technical vulnerability may be derived from a physical feature in the device, at the point of connection to the device, from the use of particular software, or, all too commonly, from combinations of several such factors’.¹³²⁹

From empirical evidence, the consumer’s ATM/debit card data and PIN can be stolen with or without consumer’s negligence or fault. In many instances, especially if the fraudster employed identity theft passive attack method such as skimming with PIN-hole camera or PIN-pad overlay, and malware — the consumer even might not have noticed that their ATM/debit card data and PIN had been compromised. According to Anderson, consumers ‘cannot reasonably be expected to establish whether the problem lies in the card, in the reader, in the network, in the settlement system, or in the bank branch’.¹³³⁰

This situation is exacerbated by a bank’s moderate security choices, lack of state-the-art fraud prevention infrastructure, lack of comprehensive fraud risk education, and the absence of bank fraud mitigation aspects, such as of neural network applications, real time on-line transaction notification, and/or regular publication of reports of statistics on unauthorised ATM/debit card transactions. All of these ‘poor’ choices by banks are mostly driven by business or economic considerations to reduce expenses and maximize profit, not from a policy of fraud containment. As result, consumers are highly vulnerable to fraudulent activities in their ATM/debit card transactions. Specific to the absence of real time notification of ATM/debit card transactions from the bank, typically the fraud damage becomes excessive, since the consumer has no information whatsoever to detect a fraudulent transaction in real time.

On the occasion of most frauds, banks typically are unwilling to admit that they actually contributed to the occurrence of identity theft/fraud: they are reluctant to admit their

¹³²⁸ Mark E Budnitz, ‘Commentary: Technology as the Driver of Payment System Rules: Will Consumers Be Provided Seatbelts and Air Bags?’ (2009) 83(2) *The Chicago-Kent Law Review* 932–4.

¹³²⁹ Clarke and Maurushat, above n 1246, 11.

¹³³⁰ Anderson, above n 1159.

technical security weaknesses, lack active supervision of their infrastructure (including counterpart infrastructure), and/or reluctance to supply fraud risk consumer education. Instead, banks are tempted to accuse the consumer of negligence whenever an unauthorised ATM/debit card transaction happens. That is, unless the ‘phantom ATM/debit card transactions’ is later acknowledged as fraudulent and overtly becomes part of public consumption via the media and comes to the central bank’s attention, banks have a tendency to assert that all ATM/debit card disputed transactions must have been carried out with the consumer’s genuine card and PIN and/or must have been due to fraudulent collusion or negligence. Hence, the consumer’s loss claim often is rejected based on an assumption of the existence of pure contributory negligence on the part of the consumer.¹³³¹

Nevertheless, in regard to unauthorised ATM/debit card transactions which use the correct consumer’s PIN, the defendant should have strong evidence that the PIN being used in the fraudulent transaction was indeed used by the real consumer. Unlike a manual signature or a strong electronic signature (such as digital signature or biometric that is individual and unique to the signer) ATM/debit card data and PIN do not have non-repudiation value and technically can key into a bank’s consumer activated terminal by the legitimate consumer/cardholder or any fraudster who possesses the consumer’s ATM/debit card data and PIN. In fact, since the authentication of a consumer’s ATM/debit card transaction is verified remotely only by technical means using a method without non-repudiation value, and hence relying only on the appropriateness of the data, a bank is unable to distinguish whether the data is actually coming from a genuine ATM/debit card or a counterfeit card or whether the use of the data is authorised or not.

A bank’s reluctance to invest in state-of-the-art security and fraud risk education features is typically related to the relatively high investment cost which it is afraid will reduce bank revenue. Anecdotal evidence (from bank officers unwilling to be named for obvious reasons) has revealed that bank reluctance to give adequate fraud risk education to consumers is also being driven by economic motives, that is, there is a widespread

¹³³¹ See Mr Panggabean case at n 1040. In this case, the consumer’s claim was still rejected even though it was proved that a third party fraudster was the perpetrator and bank’s ATM was the point of compromise.

perception that such education will reduce the number of consumer transactions.¹³³² However, it is here argued that bank's economic reason for breaching their statutory duty has no economic and legal basis, since bank profits¹³³³ are extremely huge and that would outweigh the cost to establish more sophisticated banking security features and the supply of fraud risk education material in the context identity theft/fraud containment (prevention and mitigation). These measures would ultimately increase rather than decrease consumer confidence and, importantly for bank revenues, reduce consumer and therefore bank vulnerability to the types of fraud outlined in this thesis.

As a consequence of what they perceive as prioritising profit by avoiding panicking consumers (through such education programs) and thus reducing transaction numbers and value while also avoiding (or significantly delaying) additional expenditure required for infrastructure upgrades and education, banks have generally failed to secure their infrastructure from foreseeable risks, such as identity theft using skimming and card trapping/Lebanese loop method (occupiers' liability and tortious liability) and fake bank's call centre. Often, banks also have difficulties in proving who actually performed the unauthorised ATM/debit card transaction (phantom transaction), since the banks have not equipped consumers with a non-repudiation authentication method, employed state-of-the-art logical and physical anti fraud infrastructure, nor installed CCTV with good and durable footage to catch the perpetrator.

Banks also have failed to establish consumer fraud awareness and equip consumers with adequate knowledge about identity theft/fraud risk to avoid become identity theft/fraud victims. When officers from several banks were interviewed, their explanations were that the banks tend to educate consumers only about the benefit of bank products and services (positive education) — and avoid education about the threat of fraud to those

¹³³² See BI-Fraud Survey, above n 1133. In the BI-Fraud Survey 2015, the vast majority of respondents assert that bank's fraud risk education will not decrease consumer's confident and/or number of ATM/debit card transactions. Instead, consumers will be more confident because they would take precaution against fraud and have enough knowledge to avoid become the identity theft/fraud victim.

¹³³³ See Karnoto Muhamad, 'Focus: Rating 118 Bank Versi Infobank 2015 [2015 Infobank Version Rating 118 Banks]', *Infobank* July 2015, 22–66. In this article, it was shown that Indonesia banks' profit in the years 2000 to 2014 consistently increase quite significantly year on year, including the profits of prominent banks that have been the main target of fraudster activities. For instance, looking at profits for the year 2014 compared to 2013 some prominent banks earned significant profits as follows (assume AUD 1 is equal to Rp 10,000,000): Bank Rakyat Indonesia: AUD2,425,000,000 – up 13.58%; Bank Central Asia: AUD1,651,000,000 – up 15.82%; Bank Mandiri: AUD2,065,000,000 – up 9.69%; and Bank Negara Indonesia: AUD1,083,000,000 –up 19.56%. It is argued that such profits ifar outweigh any anticipated cost of bank investment to enhance security features in ATM/debit card system and/or provide fraud risk education to consumers.

products or services (negative education). This practice is taken to avoid loss of consumer confidence which could reduce banks' transactions volume (which then reduce banks' fee based income). Not surprisingly, this lack of consumer education about the identity theft and fraud methods has created a big asymmetry of information gap between banks' consumers and the fraudsters — which make bank consumers in general easy targets for fraudsters.¹³³⁴

In this regard, it is submitted that bank should be liable for their 'intentional' incapacity to safeguard consumer's safety from identity theft/fraud when conducting ATM/debit card transaction in bank infrastructure. As Geva asserts,

It may be argued that facilitating payments without providing adequate security is a risk to be assumed by the financial institution. In effect, this means that where the customer denies responsibility, the risk ought to be allocated primarily to the financial institution that chose to facilitate a transfer not reliably authenticated.¹³³⁵

Therefore, it is submitted that voluntary assumption of risk cannot be used by a defendant in the defence for waiver of the liability, unless the defendant can prove that they already gave comprehensive and adequate fraud risk education that was effectively delivered to the consumer.

Hence, the use of pure contributory negligence as a defence for defendants that is used in existing court's litigation, tends to be unjust for consumers since bank negligence in most unauthorised ATM/debit card transactions was actually the dominant contributing cause or was more than 50 per cent responsible for the losses compared to the consumer's negligence (if any).¹³³⁶ Other than that, if pure contributory negligence is preserved, it will not create incentives for banks to improve ATM/debit card security and give comprehensive and adequate fraud risk education to consumers. As an alternative for contributory negligence, it is proposed that the comparative negligence principle that is fairer and recognised in Indonesia tort law should be used to gauge disputant parties' liability in the unauthorised ATM/debit card transaction dispute between bank and consumer.¹³³⁷

¹³³⁴ See, eg, interviews with BO-1; BO-2; BO-3; and BO-4.

¹³³⁵ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 230.

¹³³⁶ See Fuady, '*Perbuatan Melawan Hukum*', above n 914, 80. See also Gibson and Fraser, above n 917, 79–80; ePayments Code cl 11.3.

¹³³⁷ See Rusch, above n 106, 599–600.

ii. Comparative Negligence Principle

In comparative negligence, the onus of proof rests with the defendant who pleads this defence in order to defend him/herself against a tortious/negligence liability claim from the plaintiff for damages. If the defendant is successful in proving their defence, there will be a reduction of damages to be paid to the plaintiff, based on the comparison of the plaintiff's degree of lack of standard of care that a reasonable person would observe in the plaintiff's position, 'and the matter will be decided on the basis of what the person knew or ought to have known at the time.'¹³³⁸ The standard of care test that the defendant must pass to evade claims of contributory negligence/comparative negligence is similar to the standard of care that is owed by the defendant to the plaintiff. In relation to the amount of the reduction, Gibson and Fraser state that, 'the reduction is calculated on the basis of the damages that would have been awarded to the plaintiff if there had been no fault/negligence on their part, and then reduced by the percentage of their negligence.'¹³³⁹

In Indonesia, Article 1365 of Indonesia's Civil Code obliges the tortfeasor/defendant to redress the damage to the victim/plaintiff in full; however, if the loss incurred is attributed to the tortfeasor and to the victim's own fault/negligence (joint fault/negligence), then the tortfeasor need only to pay partial compensation. In other words, the victim in such circumstances should also bear part of the damages suffered. This situation has actually existed in the Netherlands since 1916 and is acknowledged in Dutch case law.¹³⁴⁰ In general, the plaintiff's fault or negligence will reduce the liability of the defendant. Both plaintiff and defendant should bear the damages based on their degree of fault/negligence.¹³⁴¹ The division of liabilities between plaintiff and defendant is known in the civil law, and also in tort under customary law (as can be seen from Indonesia's Supreme Court Verdict on 10 January 1957 No 206 K/Sip/1955).¹³⁴²

In regard to unauthorised ATM/debit card transaction, it is argued that the adjudicator in ADR/court should seek and compare the degree of fault/negligence of the defendant and plaintiff that enabled the identity theft/fraud to occur. Several relevant facts that should

¹³³⁸ Gibson and Fraser, above n 917, 112.

¹³³⁹ Ibid 111–12.

¹³⁴⁰ See *Arrest Hoge Raad* dated 4 February 1976 in Setiawan, 'Tinjauan Elementer Perbuatan Melawan Hukum', above n 939, 17.

¹³⁴¹ Ibid 37–9.

¹³⁴² Ibid 38–9.

be considered carefully using multi-disciplinary approaches (economic, technological and legal), among other things are:

- Whether the defendant is a professional and highly positioned entity who had occupier liability for the ATM/debit card infrastructure, capacity to spread the loss, and a due care to provide secure ATM/debit card infrastructures and provide fraud risk education for the plaintiff.
- Most consumers are laypersons who do not have much knowledge about ATM/debit card technology and its inherent identity theft/fraud risks. Most consumers also have a false sense of security about bank ATM/debit card operations. Therefore, it is submitted that a plaintiff's negligence that contributes to the occurrence of unauthorised ATM/debit card transaction that occurs because of a defendant's reluctance to provide fraud risk education (which made plaintiff suffer from a severe asymmetry of information about ATM/debit card operations and fraud risk information) should be disregarded. However, a plaintiff's gross negligence in failing to abide with a defendant's security tips on ATM/debit card transactions (such as the obligation to avoid selecting an easy to guess PIN, or the defendant's prohibition on a consumer using their date of birth for a PIN) should be regarded as a negligence.
- Fraudster's malicious device/identity theft methods may be either tangible (such as card trapping, skimming, PIN-hole camera, PIN-pad overlay) or intangible (such as malware, eavesdropping, hacking) and are difficult for consumers to spot simply because they are intangible, cannot be seen, and/or are perfectly disguised. Therefore any expectation that a consumer notice the fraudster's malicious device is considered unfair because it is deemed an impossible task.
- A bank as a professional, fiduciary, and prudential institution has a duty of care to ensure consumer security. This is derived from various regulations, ethics, and morality.
- All ATM/debit card infrastructure, identification/authentication/authorisation procedures, identity theft/fraud prevention and mitigation policies, consumer education, and so on are mostly determined solely by banks. Therefore, when the occurrence of unauthorised ATM/debit card transactions are mostly due to a bank's employment of vulnerable technology (such as magnetic stripe card) and weak electronic signature methods (such as a PIN) which have no non-repudiation

authentication aspect both from technological and legal aspects, or when a bank fails to safeguard consumer security by failing to provide adequate CCTV devices and guardian/security personnel at bank ATMss/ATM booths, or fails to perform active monitoring at consumer activated terminal (occupier liability), it is submitted that the bank should be liable for the consumer's loss.

However, in some instances of unauthorised ATM/debit card transactions where the point of compromise is bank infrastructure and the identity theft methods utilised are impossible for consumers to spot because the malicious device is hidden, perfectly disguised, or simply intangible (such as is the case with malware, skimming, and eavesdropping identity theft methods), it is argued that the use of the negligence per se doctrine with its strict liability principle might be justified. Strict liability can also be used in situations where a consumer has reported the unauthorised ATM/debit card incident and/or possible breach on his/her ATM/debit card and/or PIN, but the bank has failed to respond appropriately. Therefore, from the time that a consumer reported it to the bank, the bank bears full liability for the consumer's loss.

It is submitted in this thesis that with the use of comparative negligence principle to gauge a degree of bank and/or consumer negligence and hence liability in the resolution of an unauthorised ATM/debit card transaction dispute between a bank and its consumer, both disputant parties will have incentives to improve precautionary measures. More specifically, a bank will have great incentive to improve its ATM/debit card security and provide fraud risk education to the consumer — that is, in order to reduce liability. Banks also can have more incentives to settle unauthorised transaction disputes in its internal dispute resolution unit instead of at an ADR venue or court to avoid prolonged disputes, high litigation costs, consumer disloyalty, and reputation risk.

The proposed comparative negligence assessment example for unauthorised ATM/debit card transactions is set out in Table 5 below.

Table 5: ATM/Debit Card Point of Compromise, Identity Theft Methods and Comparative Negligence Loss Allocation Percentage

Point of Compromise	Fraudster Goal	Identity Theft Methods	Comparative Negligence Loss Allocation Percentage		Note
			B	C	
Consumer (C)	ATM/debit Genuine Card	Lost/stolen, card swapping outside bank's premise	0%	100%	<ul style="list-style-type: none"> - Consumer is the least cost avoider, so should bear 100% of the loss. - Will create incentives for consumer to improve precaution and prudential behaviour.
	PIN	Shoulder surfing, PIN guessing			
Bank's ATM Machine (B)	(1) ATM/debit Genuine Card	<ul style="list-style-type: none"> - Card trapping - Card swapping 	75%	0%	<ul style="list-style-type: none"> - Bank owes a duty of care (occupier liability) - Bank is the least cost avoider. - Bank's fault is the dominant contributing factor for fraud. - Will create incentives for the bank to improve security/monitoring.
	(2) PIN	<ul style="list-style-type: none"> - fake call centre sticker - Con-artist 	25%	0%	<ul style="list-style-type: none"> - In the event of no bank fraud risk education, the bank is the least cost avoider, & liable for 100% of the loss. - Will create incentives for bank to give fraud risk education.
			or		
			0%	25%	<ul style="list-style-type: none"> - Where bank fraud risk education exists, the consumer is the least cost avoider. Therefore, the bank will liable for 75% of the loss and consumer for 25% of the loss.
<ul style="list-style-type: none"> - Bank ATM Machine - Merchant EDC - Cashier/ Waitress - Bank's network - Bank/ Counter-part computer 	ATM/debit card magstripe data	<ul style="list-style-type: none"> - skimming - malware - eavesdropping - double swiping (transform into counterfeiting card) 	100%	0%	<ul style="list-style-type: none"> - Bank owes a duty of care (occupier liability) - Bank is responsible for its agent/counterpart's breach (vicarious liability) - Bank is the least cost avoider, so should bear 100% of the loss. - Bank's fraud risk education is irrelevant because fraudster's malicious device/software is unseen or impossible to spot by consumer. - Will create incentives for the bank to improve security.
	PIN	<ul style="list-style-type: none"> - PIN-hole camera - PIN-pad overlay - Shoulder surfing - malware - eavesdropping 			
First Party Fraud			0%	100%	Consumer's criminal liability.
Phantom withdrawal (unauthorised ATM/debit card claim by a consumer where the point of compromise, identity theft/fraud methods, and/or the perpetrator of identity theft/fraud cannot be determined/revealed by the bank, for instance because a bank does not have CCTV and/or CCTV footage on the ATM, data stolen using malware, and so on).			100%	0%	<ul style="list-style-type: none"> - ATM/debit card data within the magstripe card is so vulnerable and PIN is weak authentication method and does not have non-repudiation aspect. Hence, that bank cannot have a defence only based on proof that the fraud has been conducted using the consumer's correct data and PIN. - Bank is liable for 100% of the loss because it was unable to prove consumer negligence. - create incentives for better security.

7.4.2. Law Reform on Fraud Liability Rules by Creating Clear, Fair, Detailed, and Decisive Unauthorised ATM/Debit Card Loss Allocation Regulations in Indonesia

7.4.2.1. Between US and Australia Approaches to Fraud Liability Rules

The quest for an answer to the very important question of who should bear liability for the damages incurred by an unauthorised ATM/debit card transaction requires clear, fair, detailed, and decisive rules to supply a good answer. The absence of specific unauthorised ATM/debit card transaction loss allocation rules in Indonesia has made the unauthorised ATM/debit card dispute resolution decisions between a bank and its consumer — either in an internal bank dispute resolution unit or in the various adjudication forums — fail to achieve sensible decisions which reflect fairness, and predictability/certainty; nor in the absence of such rules has there been any ability to create incentives to increase the adoption of identity theft/fraud precautions on the part of the least cost avoider party. The importance of the existence of robust payment system rules which clearly define the rights and obligations of the parties involved in the system has been highlighted by Bank for International Settlement as follows:

the rules and procedures of a system should be specified clearly, enforceable and their consequences predictable. A system which is not legally robust or in which the legal issues are poorly understood could endanger its participants. Poor understanding can give participants a false sense of security leading them for example, to underestimate their credit or liquidity exposures. Participants, the system operator, and other involved parties – in some cases including customers – should understand clearly the financial risks in the system and where they are borne. An important determinant of where the risks are borne will be the rules and procedures of the system. These should define clearly the rights and obligations of all the parties involved and all such parties should be provided with up-to-date explanatory material. In particular, the relationship between the system rules and the other components of the legal environment should be clearly understood and explained. In addition, key rules relating to financial risks should be made publicly available.¹³⁴³

In the need to create of clear, fair, detailed, and decisive fraud liability rules for ATM/debit card transactions, it is argued that other countries' unauthorised ATM/debit card rules (fraud liability rules) — that are derived from various legal and other disciplines' principles such as economic and/or probably technological principles — can be studied, compared and, if necessary, adopted. However, they should be examined carefully, especially to ensure their compatibility with and appropriateness to the

¹³⁴³ CPSS, 'Core Principles for Systemically Important Payment Systems', above n 317, 6.

specific circumstances of ATM/debit card operations as part of the retail payment system and rule of law in Indonesia.

The *ex-ante* precise rules on unauthorised ATM/debit card transactions in Indonesia, can be used as a tool to limit judicial discretion which has often proved far from sensible but rather has served to create judicial error. Gillette asserts that precise fraud risk allocation rules have many benefits, such as that they can create clear liability rules which can reduce costs of enforcement processes, make legal doctrine more accessible to those untrained in legal matters, and facilitate coordination by ensuring that all parties involved in the payment system follow similar patterns of behaviour (uniformity).¹³⁴⁴ Therefore, a precise set of principles and rules, if they could be implemented, would enhance fairness to consumers.¹³⁴⁵

From various regulation options for ATM/debit card transactions, such as using legislation and central bank regulation with the strict liability principle as in the United States (*EFTA 1978* and *Regulation E*) or adopting a payment system industry code of practice with fault/negligence based liability as in Australia (ePayments Code), this thesis argues that the latter option probably is more appropriate to remedy and create sensible and fair resolution of any unauthorised ATM/debit card transaction dispute between a bank and its consumer in Indonesia. This choice is derived from several considerations as follows:

- 1) The fraud liability rules should not only give better consumer protection in the ATM/debit card transaction, but also create fairness and incentives between bank and consumer to increase precautions to avoid the occurrence of unauthorised ATM/debit card transactions. In fact, both US and Australian fraud liability rules are good and contain many provisions that are in line with the spirit of modern consumer protection, which places a greater burden on business actors to ensure consumers' safety and/or comfort when they consume business actors' products or services (*caveat venditor* principle). This comforting approach or less stringent rules for consumers is created to maintain a high level of consumer protection and promote confidence in the safe and sound practice of the electronic payment instrument. However, it is here argued that US unauthorised ATM/debit card transaction regulation that employs the strict liability principle which always makes

¹³⁴⁴ Gillette, above n 130, 186.

¹³⁴⁵ Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 210.

the financial institution/bank fully liable for the unauthorised ATM/debit card transaction losses (regardless whether or not there was consumer's negligence)¹³⁴⁶ tends to be unjust to the bank and discourages consumers from improving the precautions taken when conducting ATM/debit card transactions.¹³⁴⁷ Whereas, in Australia's e-Payment code, loss allocation rules for unauthorised ATM/debit card transactions are determined according to the degree of fault/negligence (fault-based liability) between the bank and consumer, depending on the circumstances of the case. Therefore, it tends to be fairer and provide greater incentives for banks to improve their security and consumer education, and for consumers to improve their precautions in order to avoid the occurrence of unauthorised ATM/debit card transactions.¹³⁴⁸

- 2) Even though Australia's comparative liability fraud model is probably more difficult to adjudicate and administer compared to US strict liability model,¹³⁴⁹ this deficiency can be mitigated by the establishment of fraud loss allocation rules, which are clear, fair, detailed, and decisive to make the adjudication/litigation proceeding simple and easy. Therefore, the rules not only should include provisions that explain what constitutes bank/consumer fault/negligence in the ATM/debit card operation, but also decisive loss allocation rules, burden of proof, and guidelines to weigh the evidence.¹³⁵⁰ It is argued that when rights and obligations and also liability rules for each party involved in the ATM/debit card operation can be specified clearly, are enforceable and their consequences predictable by every electronic payment system stakeholder, it will encourage disputant parties to settle most disputes between themselves. This will significantly reduce or avoid the need to escalate the dispute to the adjudicator/litigator forums which used to happen and often created additional pecuniary and non-pecuniary loss or burden for disputant parties in terms of time, money, effort, hassle, stress, and so on.

¹³⁴⁶ Actually the consumer might have liability. However, the portion of consumer liability will be very limited and depend on how rapid the consumer reports the loss of their access device and promptly informs the financial institution of any unauthorised funds transfers. See 12 CFR *Regulation E* § 205.6.

¹³⁴⁷ See Geva, 'Consumer Liability in Unauthorized Electronic Funds Transfers', above n 107, 231. According to Geva, 'the consumer's fault/negligence may have contributed to an unauthorised funds transfer. That is, due to the customer's fault, a person may unlawfully assume control of the card and code, or bypass their use altogether, and initiate an unauthorized transfer. Obviously, allocating to the customer losses caused by his or her fault will enhance diligence and minimize losses'.

¹³⁴⁸ See ePayments Code cl 4. See also Weerasooria, above n 887, 97.

¹³⁴⁹ See White, above n 111, 4, 187.

¹³⁵⁰ In the ePayments Code, burden of proof and proof of fault is clearly set out and should be borne by the financial institution/bank.

- 3) With the Australian e-Payment model, flaws in the unauthorised ATM/debit card dispute resolutions which emanate from consumer or adjudicator lack knowledge on the economic, technological, and legal aspects (that are closely entwined with unauthorised ATM/debit card transactions) can be reduced or eliminated. This can happen because there will be clear rules that link liability to enumerated, prescribed and precise acts or omissions constituting fault/negligence concerning unauthorised ATM/debit card transactions, and the burden of proof will always lie on the bank's shoulders.
- 4) Compared to US approaches, the Australian e-Payment Code provisions are more aligned with existing Indonesian regulations and legal principles concerning unauthorised ATM/debit card transaction and consumer protection, which still rely on tortious/negligence liability, not strict liability.¹³⁵¹ For instance, the e-Payment Code, which employs comparative negligence doctrine, is in conformity with Indonesia's *LCP*, *LIET*, and other regulations that place presumed liability on the shoulders of the relevant business actor/bank in instances of unauthorised ATM/debit card transactions. However, an innocent bank can avoid compensating consumer losses, if the bank can prove on the balance of probability that the consumer's loss was caused by the consumer's own negligence.¹³⁵² Therefore, both bank and consumer will have the incentive to increase awareness and precautions to avoid identity theft/fraud in their ATM/debit card operations.

7.4.2.2. The ePayments Code Model and Its Prospects of Settling Unauthorised ATM/Debit Card Transaction Disputes between Banks and Consumers in Indonesia

The ePayments Code has been created to provide (among other things) 'a quality consumer protection regime for payment facilities, a framework to promote consumer confidence in electronic banking and payment systems, clear and fair rules for allocating liability for unauthorised transactions, and effective procedures for resolving complaints'.¹³⁵³

¹³⁵¹ In Indonesia, strict liability is only employed in the Indonesia environmental law.

¹³⁵² This will not happen in United States. In other words, there the diligent consumers subsidise the negligent consumers.

¹³⁵³ ePayments Code cl 4. See also Weerasooria, above n 887, 97.

It is submitted in this thesis that if ePayments Code provisions concerning unauthorised ATM/debit card transactions are adopted in Indonesia, the questions existing in regard to who should be liable for consumer losses that have been caused by various identity theft/unauthorised ATM/debit card fraud methods that occur in Indonesia will arguably have more clear, fair, predictable, and decisive answers, as will be outlined below.

7.4.2.2.1. When the Bank is Liable for the Loss

In the Code, the account institution or issuer bank is liable for replacing consumer losses arising from unauthorised ATM/debit card transactions, which occur among other reasons because of or on occasions such as:

1. fraud or negligence by a bank employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent;¹³⁵⁴
2. a device, ATM/debit card or PIN which is forged, faulty, expired or cancelled;¹³⁵⁵
3. a transaction requiring the use of a ATM/debit card and/or PIN that occurred before the consumer received their ATM/debit card and/or PIN (including a reissued ATM/debit card and/or PIN);¹³⁵⁶
4. a transaction being incorrectly debited more than once to the same facility;
5. an unauthorised transaction performed after the bank has been informed that an ATM/debit card has been misused, lost or stolen, or the security of a PIN has been breached;¹³⁵⁷

¹³⁵⁴ ePayments Code cl 10.1(a). The issuer bank will be liable for their consumer's loss if it was caused by fraud or negligence of a bank employee or the bank's third party agent/counterpart employee (such as switching company electronic agent or employee, acquiring bank's electronic agent or employee, merchant's electronic agent or employee, and so on). Therefore, the issuer bank in Indonesia should still be liable for the consumer's loss even if the identity theft/fraud point of compromise were not in its infrastructure but at its agent or third party counterparts infrastructures (such by the use of skimmer, card trapping, or malware devices found in acquiring bank's ATM/EFTPOS machines). Another example is when identity theft/fraud occurs because of a data breach at the merchant's computer that is derived from the use of prohibited double swipe practices (such as in Body Shop cases). The good thing with this kind of provision is that the issuer bank in Indonesia will no longer be able to avoid liability and pass it to the agent/counterpart party with which the consumer has no contractual or direct relationship. Actually, the general rule of this provision is already contained in the LCP, LIET, Indonesian Civil Code and Bank Indonesia regulations (BID-RMUTCB, *BIR-CBPI*, BIR-CPPSS, BIR-Outsource to Other Party). However, detailed and clear regulation is deemed to be better.

¹³⁵⁵ Issuer bank is liable for unauthorised ATM/debit card transactions using counterfeiting card method, which is normally derived from the use of an identity theft method, such as skimming, malware, eavesdropping, and double swiping.

¹³⁵⁶ ePayments Code cl 10.1(b). The issuer bank is liable for 'card not received' fraud that occurs in credit card operations.

¹³⁵⁷ ePayments Code cl 10.1(e). The issuer bank is liable for consumer loss after a consumer notifies a bank about a lost or stolen, misused, or possibly breached consumer ATM/debit card and/or PIN.

6. an unauthorised transaction that can be made using an ATM/debit card without PIN;¹³⁵⁸ or
7. where it is clear that a consumer has not contributed to the loss.¹³⁵⁹

7.4.2.2.2. When the Consumer/Cardholder is Liable for the Loss

The consumer/cardholder is liable to bear a loss arising from fraud (unauthorised ATM/debit card transactions) if: a). the bank did not have any liability to the consumer;¹³⁶⁰ and b). the bank can prove on the balance of probability that:

1. The consumer contributed to the loss through fraud, or breaching the PIN security requirements,¹³⁶¹ such as:
 - a. voluntarily disclosing the PIN to anyone, including a family member or friend;
 - b. where an ATM/debit card is also needed to perform a transaction, writing or recording the PIN on an ATM/debit card, or keeping a record of the PIN on anything
 - carried with an ATM/debit card, or
 - liable to loss or theft simultaneously with an ATM/debit card, unless the consumer makes a reasonable attempt to protect the security of the PIN;¹³⁶²
 - or
 - c. where an ATM/debit card is not needed to perform a transaction, keeping a written record of all the PIN (required to perform transactions) on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the PIN;¹³⁶³

¹³⁵⁸ ePayments Code cl 10.2. The cardholder can be liable only if the user unreasonably delays reporting the loss or theft of the device.

¹³⁵⁹ ePayments Code cl 10.3. This provision can be used in unauthorised ATM/debit card transactions that derive from a fraudster's passive attack (such as skimming, malware, eavesdropping, PIN-pad overlay, PIN-hole camera, and the like). This provision will give strong incentives to issuer banks to develop good and reliable administrative procedures in order to make sure that only the genuine consumer receives the ATM/debit card and its PIN by verified written acknowledgement from consumer.

¹³⁶⁰ This condition, therefore, negates the responsibility of bank, as regulated in Chapter C: Liability, Clause 10 of the ePayments Code.

¹³⁶¹ ePayments Code cl 11.2.

¹³⁶² ePayments Code cl 12.2.(a) & (b).

¹³⁶³ See ePayments Code cl 12.2.(c). See also cl 12.3. For the purpose of clauses 12.2(b)–12.2(c), a reasonable attempt to protect the security of a pass code record includes (i) making any reasonable attempt to disguise the pass code within the record, or preventing unauthorised access to the pass code record, among other things by: (a) hiding or disguising the pass code record among other records; (b) hiding or disguising the pass code record in a place where a pass code record would not be expected to be found; (c) keeping a record of the pass code record in a securely locked container; or (d) preventing unauthorised access to an electronically stored record of the pass code record.

- d. selecting a numeric PIN that represents their birth date, or an alphabetical PIN that is a recognisable part of their name — even though the bank has specifically instructed the consumer not to do so and warned the consumer of the consequences of doing so at the time of selecting the PIN;¹³⁶⁴
2. When an ATM/debit card is lost, stolen or misused until it is reported to the bank.¹³⁶⁵
3. The consumer contributed to losses by leaving their ATM/debit card in the ATM, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM.¹³⁶⁶
4. The consumer contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of an ATM/debit card, or that the security of a PIN has been breached. The consumer is liable for the actual losses that occur between: a) when the consumer become aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen ATM/debit card, and b). when the security compromise was reported to the bank.¹³⁶⁷

7.4.2.2.3. Consumer/Cardholder Limited Liability

Limited liability is governed by clause 11.7 of the ePayments Code, and only will apply if a PIN is required to perform an unauthorised transaction, and there are no circumstances that could make a consumer liable for the loss. Tyree contends that this clause about limited liability in the Code is the most important aspect for unauthorised transactions. According to him, this clause establishes a basic ‘no fault liability or liability without fault’ for consumers, which may only be turned into a ‘fault based liability’ if the financial institution can prove a consumer’s fault, such as when the consumer was involved in the fraud or utilised the access method contrary to the rules set out in the Code.¹³⁶⁸

¹³⁶⁴ ePayments Code cl 12.5 and 12.6..

¹³⁶⁵ ePayments Code cl 11.2(a). However, the consumer is not liable for the portion of losses which were: a). incurred on any one day and were in excess of any applicable daily transaction limit; b). incurred in any period that exceeds any applicable periodic transaction limit; and so on. See ePayments Code cl 12.2(b).

¹³⁶⁶ ePayments Code cl 11.4. Note: Reasonable safety standards that mitigate the risk of a card being left in an ATM include ATMs that capture cards that are not removed after a reasonable time and ATMs that require a user to swipe and then remove a card in order to commence a transaction.

¹³⁶⁷ ePayments Code cl 11.5(a).

¹³⁶⁸ Tyree, ‘Banking Law in Australia’, above n 886, 351.

If the bank fails to prove that the consumer contributed to a loss through fraud, fault (such as breaching the PIN security requirements) or negligence (such as leaving a card in an ATM, unreasonably delaying reporting the misuse, loss or theft of an ATM/debit card, or that the security of a PIN has been breached), then in accordance with cl 11.7 of the ePayments Code, the consumer is liable for the least of:

- (a) \$150, or a lower figure determined by the [bank],
- (b) the balance of the facility or facilities which the [bank] and the holder have agreed can be accessed using the [ATM/debit card] and/or [PIN], including any prearranged credit, or
- (c) the actual loss at the time that the misuse, loss or theft of [an ATM/debit card] or breach of [PIN] security is reported to the [bank], excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.¹³⁶⁹

Pertaining to limited liability, Geva argues that allocating the loss to the consumer only up to a low threshold, irrespective of fault ‘could still enhance diligence without causing the consumer undue hardship’. That is, minimum liability will serve as an incentive for consumers to guard their card and PIN.¹³⁷⁰

7.4.2.2.4. Proof that a User Contributed to Losses

In proving the balance of probability, that is, whether or not a consumer has contributed to the losses in an unauthorised ATM/debit card transaction, the bank is obliged to explore all reasonable evidence and explanations regarding the alleged unauthorised transaction.¹³⁷¹ However, although Indonesian banks tend to judge that any and all electronic transactions that use the correct data and PIN as a cardholder valid transaction (not actually a sensible claim),¹³⁷² the Australian ePayments Code (cl 11.8(b)) (by way of contrast) has prohibited the claim by a financial institution to have merely found that ‘a correct device data and pass code’ was used in an unauthorised

¹³⁶⁹ ePayments Code cl 11.7.

¹³⁷⁰ Geva, ‘Consumer Liability in Unauthorized Electronic Funds Transfers’, above n 107, 231, 293–341.

¹³⁷¹ ePayments Code cl 11.8(a). See also Article 59(1) of Council Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market [2007] OJ L 319/1 (‘European Payment Services Directive’). In this Article, when a consumer denies having authorised an executed payment transaction, the payment system provider has an obligation to prove that the payment transaction was authenticated.

¹³⁷² See ASIC, ‘Discussion Paper on an Expanded EFT Code’, above n 890, 27–8. In the paper, ASIC contends that financial institutions tend to shift the fraud risk onto consumers by showing the record which depicts that the correct authentication mechanism was used in the disputed transaction, even though it does not show who the purported consumer really is. Further, ASIC also asserts that the one sided liability rules from financial institutions generally derive from the standard contract that made cardholders liable for any transaction authenticated by use of the card and PIN, regardless of loss or theft of the card or surreptitious observation of the PIN.

transaction as a proof of a consumer's involvement in a fraud or a breach of the PIN security requirements, recognising:

the fact that a facility has been accessed with the correct device and/or pass code, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in clause 12.¹³⁷³

This important clause is derived from the consideration that often it is impossible to distinguish an unauthorised PIN instruction from an authorised one, because — from a technological viewpoint — the PIN is exactly the same whether keyed in by a fraudster or an authorised consumer.¹³⁷⁴ It is also a fact that PIN security is very weak and transactions often involve inherently insecure PIN authentication procedures that make them vulnerable to detection, such as from PIN theft methods using 'shoulder surfing', PIN hole cameras, key loggers, eavesdropping, malware and so on.¹³⁷⁵ Besides its presence in the ePayments Code, this provision is also highlighted in other prominent regulations, such as those for Europe where it features in the European Payment Services Directive. According to Article 59(2) of the Directive, 'where [the consumer] denies having authorised an executed payment transaction, the use of a payment instrument recorded by the [bank] shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently...'.¹³⁷⁶

It is argued that if this specific clause were to be also employed in the unauthorised ATM/debit card transaction loss allocation rules in Indonesia (through regulation reform), banks would no longer be able to reject consumer's losses by utilising as a defence their unfair and illegitimate liability dumping provision which gives a one sided

¹³⁷³ See ePayments Code cl 11.8(b): 'the fact that a facility has been accessed with the correct device and/or pass code, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in clause 12'. For pass code security requirements, see clause 12 of the Code that forbid a consumer to:

- (a) voluntarily disclose one or more pass codes to anyone, including a family member or friend,
- (b) where a device is also needed to perform a transaction, write or record pass code(s) on a device, or keep a record of the pass code(s) on anything:
 - (i) carried with a device, or
 - (ii) liable to loss or theft simultaneously with a device,
- (c) where a device is not needed to perform a transaction, keep a written record of all pass codes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the pass code(s).

¹³⁷⁴ See 'Discussion Paper on an Expanded EFT Code', above n 890, 27.

¹³⁷⁵ Ibid 28. See also various PIN theft methods in Chapter Four of this thesis.

¹³⁷⁶ Council Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market [2007] OJ L 319/1 ('European Payment Services Directive').

allocation of losses to the consumer, that is, where the unauthorised ATM/debit card transaction conducted using the correct consumer's ATM/debit card data and PIN.

As a consequence, banks will have great incentives to equip themselves with state-of-the-art identity theft/fraud prevention and mitigation infrastructure to ensure that consumer ATM/debit card data and PIN are secure from identity theft/fraud. Banks will also probably have greater incentive to equip all the ATMs and their booths with good quality CCTV and/or security guard in anticipation of, or for the detection of, possible unauthorised ATM/debit card transactions that occur because of first party or second party fraud or third party fraud facilitated by consumer negligence.

7.5. Conclusion

Loss allocation rules on unauthorised ATM/debit card transaction disputes depend on the specific circumstances of the identity theft/fraud (such as the location of the point of compromise, typology of identity theft/fraud methods employed, the authentication process, the reliability/vulnerability of the ATM/debit card infrastructure, the possible perpetrators, relevant regulations, and whether or not bank has educated consumer about inherent risks in the ATM/debit card infrastructures/system.

The need of law reform on unauthorised ATM/debit card transactions in Indonesia is triggered by the failure of Alternative Dispute Resolution forums (the bank's internal dispute unit, Bank Indonesia Banking Mediation Agency, and CDSB) and of courts as the final forum to produce sensible decision on resolution of unauthorised ATM/debit card transaction disputes between banks and consumers.

Most court decisions favoured of the bank on the grounds of pure contributory negligence, that is, that the consumers enabled identity theft/fraud to occur. These decisions are deemed unjust to consumers, given that bank negligence to secure its infrastructure and failure to provide adequate fraud risk education or safeguard consumer' transactions are actually the dominant contributory factors that cause consumer negligence and facilitate the success of fraudster identity theft and fraud. The flaws in the courts decisions were mostly caused by the consumer's inability to support his/her claim and the successful defence by the bank (based on anecdotal defence about bank ATM/debit card system's infallibility and the existence of consumer's negligence that has contributed to the occurrence of the third party fraud.

In fact, bank ATM/debit card infrastructure is not infallible/tamper resistant and impenetrable due to the various adaptive and innovative identity theft methods adopted by fraudsters (such as skimming, card trapping, card swapping, eavesdropping, malware, and various PIN theft methods). Often, the consumer becomes the weakest link and vulnerable to social engineering attack due to a false sense security fostered by a bank's reluctance to give fraud risk education to consumers. Hence, reliance on consumer vigilance is absurd.

The banks' magnetic stripe card and PIN technology are weak, have no non-repudiation aspect, and are very susceptible to fraud. Unauthorised ATM/debit card transactions (identity theft) using either a stolen consumer's genuine card or use of counterfeit cards and methods that are indistinguishable from the authorised transactions. Therefore, the bank raising a defence on the basis that unauthorised ATM/debit card transactions were enabled by correct consumer ATM/debit card data and PIN was weak as this did not automatically prove that a consumer must have been negligent or careless in keeping their card data and PIN secret. In other jurisdictions, such as in Australia and the EU, this kind of defence is not allowed unless accompanied with other empirical evidence.

Therefore, this thesis argues that the comparative negligence doctrine — that is actually acknowledged in Indonesia's legal system and deemed fairer and could create incentives for both disputant parties for fraud containment — should replace the pure contributory negligence doctrine in the effort to fairly determine the bearer of fraud losses in the adjudication/litigation process. The application of the comparative negligence doctrine using multi-disciplinary approaches to the various typologies of identity theft/fraud on ATM/debit card transactions typically will direct liability to the least cost avoider in the specific identity theft/fraud circumstances. However, it is argued that consumers will only be liable for the loss if they had fraud risk education from their bank. Thus, in first party, second party, and third party fraud (where the consumer becomes the point of compromise outside the bank's perimeter), the consumer will be the least cost avoider and hence liable for the loss. Meanwhile, in third party fraud where bank or its electronic agent/third party counterpart infrastructure and consumer become the joint of point of compromise, liability will be divided between the bank and consumer according to the degree of fault/negligence involved. Last but not least, in the counterfeiting fraud typology where bank infrastructure is the sole point of

compromise and the consumer demonstrates no fault/negligence, the bank is fully liable for the consumer's losses.

In the quest for clear, fair, detailed, and decisive loss allocation rules on the unauthorised ATM/debit card transaction as part of law reform objective, US strict liability and Australia's fault based liability regulation model have been compared and critically evaluated. Arguably, Australia's loss allocation rules for unauthorised ATM/debit card transactions are deemed more appropriate and a better fit with Indonesia's current legal system and the nature of its retail payment system which has pervasive consumer activated terminal highly involvement by consumers in the initiation of such transactions. It is also believed that fault/negligence based liability could also create more incentives for parties involved in the ATM/debit card system to improve precautions and identity theft/fraud containment.

CHAPTER 8 – THE FINAL DENOUEMENT

The development of electronic banking in Indonesia and elsewhere has been facilitated by the rapid and advanced development of information, computer and telecommunication technology. Globalisation, electronic commerce, and the need to conclude economic transactions in the most effective and efficient way have made electronic payments or electronic fund transfers the main method chosen by the modern society in preference to other payment instruments. From a wide selection of electronic payment systems, the ATM/debit card is the electronic payment instrument most widely used by people in Indonesia and it has become a mainstay in the country's electronic payment system. This development is characterised by (among other things) the proliferation of ATM/debit card consumer activated terminals, namely ATMs and EFT-POS terminals in a variety of places — ranging from major centres in large cities to various crossroads and villages.

However, as the old proverb of Indonesia '*ada gula ada semut*' or 'if there is sugar there is ants', so too it is with bank ATM/debit card operations. Banks have long been the place where people deposit money, and the bricks-and-mortar branches and their customers subject to robbery using physical attack, with menaces or arms. New transaction methods have been accompanied by new methods of robbery. The same factors that have supported the development of e-banking, — the advanced development of information, computer and telecommunication technology — have also supported the rise of identity theft and fraud in the banking sector. Many fraudsters consider that attacking ATM/debit card operations well worth attempting since it is relatively easy (with technological tools readily available and social engineering skills easy to master and the entire operation involving little or no risk of physical violence) with a 'sky is the limit' potential return and very minimal risk of being caught. The result has been rising crime associated electronic transactions of every type, including ATM/debit card operations.

This thesis originated from concerns associated with rampant identity theft and fraud that afflicts ATM/debit card consumers in Indonesia. When unauthorised ATM/debit card transactions occur and a consumer's funds in their bank are drained — this is just the start for most consumers. The real ordeal occurs when consumer's claims to obtain

compensation for the unauthorised transactions are rebuffed by their banks. The rejection is generally justified on the grounds of liability dumping provisions in the standard bank–consumer standard contract, in which it is stated that all unauthorised ATM/debit card transactions conducted using the correct consumer data and PIN will be considered valid or authorised. That is, it is alleged that the consumer must have somehow neglected to maintain the security and confidentiality of their ATM/debit card data.¹³⁷⁷ The research sought to explore this, together with the absence of specific loss allocation rules/fraud liability rules in Indonesia, and answer a very important question that become the main topic of the thesis — that is, whether the bank or the consumer should bear the liability for the loss incurred from the disputed transaction.¹³⁷⁸ This thesis argues that in order to give a comprehensive and sensible answer to the question and its legal ramifications, multi-disciplinary approaches, namely economic, technological and legal should be employed. Law reform in the area of loss allocation regulation in regard to unauthorised ATM/debit card transactions is arguably necessary to ensure any dispute between bank and consumer pertaining to unauthorised transactions can be settled on a most efficient and fair basis.

Since the payment system itself is still not well understood by many people in Indonesia, Chapter 2 thus sought to explain the reason behind banks' eagerness to embrace and promote payment cards as the preferred instrument for consumer payment. The technical nature of bank infrastructure and the basic security procedures involved in the ATM/debit card operations are also explained.

In Chapter 3 inherent and natural risks in the operation of ATM/debit card as part of retail payment system are described. The economic and technological reasons behind the proliferation of ATM/debit card identity theft/fraud — such as banks employing relatively old and vulnerable ATM/debit card instruments and moderate security features (and the reasons for this) — are also explored to prepare the ground for the discussion of liability rules in later chapters. Incentives for payment card fraud and the wide range of fraudsters and their capabilities to perform innovative and adaptive attack are also discussed in this chapter, so a more complete picture of unauthorised ATM/debit card transactions are depicted.

¹³⁷⁷ See n 66 for example of bank's liability dumping provision.

¹³⁷⁸ See Chapter 1 / section 1.5 of this thesis.

Having acknowledged the inherent risks in ATM/debit card operations in Chapter 3, Chapter 4 outlined quite exhaustively the identity theft and fraud methods that are utilised by fraudsters to compromise consumer card data and PIN. In regard to the thesis objective of determining the party or parties that have liability for the damage that is caused by such fraud, this thesis has classified the identity theft methods according to the point of compromise. These attempts, it is argued, are very important because by knowing where the point of compromise is, the position of the pendulum of liability can be more easily defined. Hypothetically, the party or parties that by their nature are the least cost avoider for the occurrence of identity theft/fraud at the point of compromise apparently also become the liable party for the loss. For this purpose, the identity theft methods have been classified into five branches of point of compromise, namely cardholder as point of compromise, consumer-activated terminal and cardholder as (joint) point of compromise, consumer-activated terminal and/or communication network as a point of compromise, ATM/EFTPOS communication link as point of compromise, and bank and/or its counterpart data centre as point of compromise. Chapter 4 generally depicted the occurrence of identity theft/fraud from a technological perspective — vulnerabilities in the ATM/debit card systems that occur across the whole cycle of operations, and include the aspects of people, processes and technology. Several prominent conventional and advanced identity theft methods and tools utilised in the crime are enumerated, such as lost and stolen card fraud, card swapping, card skimming, malware, eavesdropping, and social engineering. For PIN theft, several major methods also have been canvassed such as PIN guessing, shoulder surfing, PIN-pad overlay, PIN-hole camera and PIN interception/cracking. The perpetrators of identity theft/fraud ranging from the consumers themselves (first party fraud), consumer's acquaintances and family (second party fraud) or in third party fraud the 'lone wolf' perpetrator, organised crime bodies (or organised crime working in concert with an individual), or simply a disgruntled or dishonest worker / bank owner, merchant, or third party agent/counterpart.

An unpublished ATM/debit card fraud report in Indonesia has shown that the threat of identity theft/fraud is real and has grown from year to year.¹³⁷⁹ Empirical evidence also proved that fraudsters are almost always able to circumvent bank security features,

¹³⁷⁹ See Table 1: Type of ATM/Debit Card Fraud and Data.

regardless of bank's security improvement efforts. However, the report itself has its own problem, since it was not constructed using a reliable, current, and complete identity theft/fraud taxonomy. As result, the existing fraud report fails to give a clear reflection of the seriousness and trends of ATM/debit card fraud in Indonesia. Instead, it gives a false sense of security and provides misleading information for identity theft/fraud containment to the stakeholders of electronic payment system.¹³⁸⁰ Hence, it is argued that this unreliable report also contributes to the rise of identity theft/fraud incidents in Indonesia.

In Chapter 5, this thesis has endeavoured to provide a complete picture of the legal and regulatory framework of ATM/debit card transactions, consumer protection, and liability rules on unauthorised ATM/debit card transactions in Indonesia. From the regulations, it can be concluded that a bank as a financial institution is a fiduciary, professional and prudential entity that owes a duty of care to its consumers.¹³⁸¹ In regard to a bank's ATM/debit card operation/system, various acts of legislation and Bank Indonesia regulations / decrees have regulated it quite profoundly (providing statutory duties that banks must fulfil). In general, a bank as the ATM/debit card system provider has many obligations: to provide risk management policy, secure its infrastructure from logical and physical attack, and safeguard consumer safety while consuming its products or services. Hence, a bank is obliged (among other things) to provide consumers with fraud risk education to ensure their safety and their taking of adequate precautions, to be responsible and liable for its agent and/or third party counterpart conduct, and to provide good and responsive consumer complaint procedures. Therefore, from a theoretical legal point a view, consumer protection in ATM/debit card transactions has been guaranteed.

However, when it comes to the fraud liability rules concerning the unauthorised ATM/debit card transaction, all of those regulations especially *LCP* and *LIET*, only provide very general liability rules. Basically, according to the rules, the bank as a provider of the ATM/debit card system is liable for consumer losses (presumed liability). However, a bank can pass this liability to the consumer if it can prove that the losses have occurred because of the consumer's own fault/negligence (tortious

¹³⁸⁰ See results of most recent BI-fraud Survey at n 1136.

¹³⁸¹ See Chapter 5 /section 5.2.1.1.

liability).¹³⁸² What constitutes fault or negligence in regard to the consumer's ATM/debit card transaction is blurred and unclear — which hypothetically has caused prolonged disputes between banks and consumers as to who should be liable for consumer losses due to the fraud. Comparisons have been drawn with the situation regarding unauthorised ATM/debit card regulation in the United States and Australia.¹³⁸³ This is considered very important in gauging whether or not Indonesia's regulation concerning unauthorised ATM/debit card transactions is adequate. In fact, Indonesia's regulations contain many deficiencies compared to the US and Australian fraud liability rules regulation. In the United States, loss allocation regulation adopts *strict liability* rules. Hence, a bank will always be liable for an unauthorised ATM/debit card transaction (that is, transaction that is not authorised by the consumer and where the consumer has no benefit from the transaction). In Australia, loss allocation regulation adopts *comparative negligence* rules, where provisions regarding when and in what circumstances a bank or consumer will be liable for unauthorised ATM/debit card transaction have been enumerated quite clearly and in detail. Hence, it is argued that the risk of contentious disputes concerning what constitutes fault or negligence in ATM/debit card operations in Australia can be eliminated or at least substantially reduced.

In Chapter 6, empirical evidence on the adjudication process in ADR/court forums to resolve unauthorised ATM/debit card disputes between banks and consumers are brought forward and analysed. The basic theories of liability and tortious negligence are described, so critical analysis can be drawn to see whether there are gaps between loss allocation liability theory and its practice in the real world. From case analysis, it is revealed that even though regulation concerning consumer protection and a bank's obligation to secure a consumer's transactions is quite strong and complete, in practice consumer protection for unauthorised ATM/debit card transactions is still absurd and far from objective. In almost all of the adjudication cases in the formal court system court (several of which cases were initially aired in ADR adjudication forums), the court verdicts always favoured the bank. It is argued that the verdicts had many flaws, were misleading, and not sensible. These wrong decisions arguably occur because the courts implement outmoded and unjust pure contributory negligence principle in the

¹³⁸² See *LIET* arts 21(2)c and 21(5); *LCP*.art s19(1) and 19(5)

¹³⁸³ See Chapter 5 / section 5.5 of this thesis.

examination of cases. Therefore, regardless of how dominant the bank's negligence is in regard to securing its ATM/debit card infrastructure and its deficiency in giving fraud risk education to consumer, the pendulum of the liability will always reside with the consumers. Typical reasons for the verdicts were that the consumer had demonstrated contributory negligence and/or because the unauthorised transaction had been conducted with the correct consumer's card data and PIN.¹³⁸⁴

In Chapter 7, all relevant theories and facts in relation to the operation of bank ATM/debit cards and unauthorised ATM/debit card transactions are analysed, discussed and synthesized to reach general conclusions and make recommendations. This chapter highlights flaws in unauthorised ATM/debit card dispute resolution practices between bank and consumers in a variety of ADR/court forums and presents the compelling reasons why legal reform on the loss allocation rules regulation and the ADR/court adjudication practices in Indonesia is necessary. It is argued in this chapter that such legal reform is required due to (among other things) continuation of market failure in ATM/debit card operations and the flaws in and/or misleading decisions from the ADR/courts concerning disputes between banks and consumers on unauthorised ATM/debit card transactions in Indonesia.

The flaws and unfair practices in the bank's internal dispute resolution unit generally emerges in association with the use of liability dumping provisions in a bank's standard contract. This is cited by the bank to settle the unauthorised ATM/debit card transaction dispute. Therefore, almost always a bank will reject a consumer's claim for redress on the ground that either the unauthorised transaction was conducted with the correct consumer card data and PIN and/or the consumer must have been negligent and that facilitated the occurrence of identity theft/fraud. This decision is generally reached by a bank regardless of who was the perpetrator (first party, second, and third party fraud) and/or how slight the consumer's negligence was. In joint liability cases where a bank actually had a dominant contribution in terms of negligence that (in turn) caused or facilitated the subsequent negligence by the consumer, such as in card trapping cases (where a bank fails to safeguard a consumer's genuine card by failing to keep their ATM free from a fraudster's malicious devices) and where a consumer fails to

¹³⁸⁴ See *Evi Yulisna v Harahap v Bank Mandiri case*, *Mr Bahari v PT Bank Negara Indonesia (Persero) Tbk*, *Muhajidin Tahir, SE v PT Bank Mandiri (Persero) Tbk* and *PT Advantage CSM, Nasruddin v PT. Bank Mandiri Tbk* in Chapter 6 of this thesis.

safeguard the secrecy of his/her own PIN data from a fraudster's social engineering trap (where the bank again may not have kept the ATM free of fake call centre number stickers or provided adequate consumer education) — and whether or not that third party fraud was obvious — a bank typically will also reject a consumer's claim on the ground that the loss was due to the consumer's own negligence.¹³⁸⁵

Meanwhile, the Banking Mediation Agency / Banking Facilitated Agency run by Bank Indonesia was also deemed to have failed to protect consumer interest. This is due to mediation being the only dispute resolution method acknowledged in the agency in many instances. Bank Indonesia as the mediator cannot make any binding decision but can only attempt to persuade the disputants to conclude a win-win agreement. However, mediation proceedings typically only replicate the original argumentation and the rejection of the claim by a bank's internal dispute resolution unit. The few banking mediation agency decisions which granted consumer claims, whether in part or in full, were typically derived from feelings of compassion or in order to have credit with the central bank, not from compelling fraud liability rules.¹³⁸⁶

In contrast to a bank's internal dispute resolution unit and the Banking Mediation Agency, dispute resolutions results from Consumer Dispute Settlement Board decisions always favour consumers. In the CDSB, the adjudicators tend to blame banks for a consumer's losses on the ground that the bank has failed to safeguard a consumer's transaction on the bank's premises. Several instances of consumers' negligent conduct (such as by letting their family and acquaintances have access to their ATM/debit card and PIN) were justified with argumentation that the practice is acknowledged in customary law (*adat*). Nevertheless, consumers never benefit from such a victory since the banks always appeal to the court and challenge the CDSB's verdict. There is also tendency for banks to avoid the CDSB as an adjudication forum to settle a dispute with a consumer, since CDSB verdicts favour consumers. Banks may refuse to have a dispute to be handled by the CDSB simply by filing an objection with the adjudicator and indicate that they prefer the court as a forum to resolve the dispute.¹³⁸⁷ As CDSB mediation is a voluntary process that needs the cooperation of both parties, this prevents any adjudication in that forum when a bank objects.

¹³⁸⁵ See Chapter 7 / section 7.2.2.1 in this thesis.

¹³⁸⁶ See Chapter 7 / section 7.2.2.2 in this thesis.

¹³⁸⁷ See Chapter 7 / section 7.2.2.3 in this thesis.

The court, as the final forum for settling any dispute on unauthorised ATM/debit card transactions, has apparently also failed to make sensible, fair and predictable decisions. Most court decisions favour banks, based on the use of the pure contributory negligence principle. That is, unless a plaintiff has can show no fault/negligence at all (clean hands policy), the plaintiff will always liable for his/her losses on unauthorised ATM/debit card transactions regardless how big and even dominant the defendant's fault/negligence was. In the absence of expert witnesses, it is apparent that a judge's verdicts were not based on actual facts and a genuine understanding of the situation (especially in regards to technological matters) nor on the basis of comprehensive regulations relevant to ATM/debit card operations. Bank failure to fully abide by the regulations where they do exist (such as the obligation to secure their ATM/debit card infrastructure (both logical and physical security), and including a failure to conduct active surveillance of its consumer activated terminals, and/or to provide adequate fraud risk education to the consumer — all of which became dominant contributing factors to the occurrence of identity theft/fraud — were not considered. This unfortunate situation is also exacerbated by the dearth of publicly available and officially unauthorised ATM/debit card figures that make a plaintiff's attempts to prove the proliferation of fraudulent activities more difficult.¹³⁸⁸

Concerning the existence of flaws in dispute resolution in ADR/court forums, it is argued that poor ADR/court verdicts on unauthorised ATM/debit card disputes are actually caused by: 1). the adjudicators' lack knowledge of the economic and technological factors involved, and the precise relevant law and legal principle concerning the circumstances of unauthorised ATM/debit card transaction disputes; and 2). the lack of clear, fair, detailed, and decisive loss allocation rules on unauthorised ATM/debit card transactions in Indonesia. It is also feared that misleading verdicts of ADR/courts could reduce consumer confidence, increase legal and reputational risks of the banking industry, and hinder e-banking and e-commerce development in Indonesia.

In order to remedy this situation of market failure,¹³⁸⁹ it is submitted that legal reform in Indonesia is necessary and immediately relevant. Pertinent economic, technological and legal facts and prominent principles are employed in the analysis so as to ensure that the

¹³⁸⁸ See Chapter 7 / Section 7.2.2.4 in this thesis.

¹³⁸⁹ See Chapter 7 / section 7.2.1 in this thesis.

recommendations for legal reform on loss allocation rules for unauthorised ATM/debit card transactions in Indonesia can be established according to world best practice and current trends in development on loss allocation regulation which give more protection to the consumer.

From an economic perspective, it is arguably very important that the Cooter and Rubin theory on loss spreading, loss reduction and loss imposition principles are established and are considered in regard to unauthorised ATM/debit card disputes.¹³⁹⁰ The loss-spreading principle is deemed acceptable in this respect as it always places liability on the financial institution/banks instead of consumers. Banks in Indonesia generally earn huge profits each year from their operations. Much of Bank Indonesia's regulation has also encouraged banks to build good risk management into the ATM/debit card system and prepare a buffer fund to absorb losses from the fraudulent activities. Therefore, it is argued that the adoption of the loss-spreading principle is in accordance with *LCP* and *LIET* and Bank Indonesia's regulation that embraces the presumed liability principle.¹³⁹¹ That is, the liability for damages will first be placed on the shoulders of the bank as the professional and fiduciary institution unless the bank can prove that the losses incurred are actually due to the consumer's own fault/negligence.

In regard to the loss-reduction principle, it is argued that it is very important to establish this principle in disputes between banks and consumer on unauthorised ATM/debit card transactions. This principle becomes the key to determining which party should be liable for the losses, whether the bank or the consumer is solely liable, or the bank and consumer together are jointly liable. According to this principle, liability should reside with the party who can avoid identity theft/fraud at the lowest cost. However, it is submitted that this principle should be associated with technological and legal aspects in order to perform optimally. Since fraudsters' identity theft and methods are varied and can be directed at either bank infrastructure or consumers, or both the bank infrastructure and consumer as a joint target, the loss-reduction principle should assess the situation on a case by case basis according to the specific identity theft/fraud circumstances coupled with relevant technological and legal facts and principles.

¹³⁹⁰ See Cooter and Rubin, above n 105.

¹³⁹¹ See Makarim, above n 857; Samsul, 'Perlindungan Konsumen', above n 863.

In this regard, the technological aspects that should be considered closely pertaining to the loss-reduction principle are (among other things) the quality and comprehensiveness of a bank's ATM/debit card infrastructure and the technology employed by the fraudsters to perform the fraudulent activities. As has been described in Chapter 2, a bank's ATM/debit card system as part of an electronic fund transfer system is heavily supported by information technology infrastructure. This technology is involved in almost all aspects of a bank's ATM/debit card operations, both in logical or physical aspects, such as the ATM/debit plastic card with magnetic stripe and/or chip technology, ATM/EFT-POS machines, the bank's host computer server, networks, software used for data communication, encryption, and so on. From the discussion in the chapters 2 and 3, it is also revealed that there is trade-off between the security technology aspect of securing ATM/debit card operations with business and the economic aspect of optimising revenue. In practice, banks generally equip their ATM/debit card infrastructure only with moderate security features regardless of the fact that most ATM/debit card fraud risks are foreseeable and identity theft and/or fraud has happened repeatedly.

Concerning incidents of identity theft/fraud in the ATM/debit card operations, the fact should be highlighted by parties to any dispute that many of the fraudsters' malicious devices are difficult or even impossible for consumers to detect because they are in the form of intangible material (such as malicious software, eavesdropping devices and so on) or if of a solid material, the malicious devices are hidden or disguised perfectly by fraudsters in the consumer activated terminal or its surroundings (such as in the case of card trapping and skimming methods). This is especially the case for the adjudicator in the adjudication proceedings who has to determine who is the least cost avoider.¹³⁹² Hence, it is argued that any expectation that the consumer spot the fraudsters' malicious devices in many identity theft/fraud incidents is unfair and unrealistic, especially when banks have not given any specific and comprehensive fraud or risk education to the consumer.¹³⁹³ In contrast, most of identity theft and fraud methods in ATM/debit card transactions are considered as foreseeability risks for banks. Other than this, many unauthorised ATM/debit card transactions occur because of phantom transactions, that

¹³⁹² See Chapter 4 / sections 4.2.1, 4.2.2., and 4.2.3 of this thesis.

¹³⁹³ For instance, see statement from Diebold Incorporated, 'White Paper: ATM Fraud and Security', above n 348, 4–7.

is, the transaction happens using the correct consumer card data and PIN but the consumer denies having initiated the transaction. In this instance, several relevant technological facts should be considered:

- the bank's magnetic stripe card data and consumer's PIN are considered a very old and weak — hence very vulnerable to compromise by fraudsters with or without a consumer's fault/negligence, such as what happened in the card skimming with PIN-hole camera/PIN-pad overlay method, malware, and eaves dropping methods;
- a bank or bank's agent/third party counterpart including merchants data based computer and/or network are also not infallible from various identity theft attacks, such as malware, hacking/cracking activity, eavesdropping, or simply that the data may be abused by an insider (where consumers are absolutely not involved whatsoever in the flow of ATM/debit card data); and/or
- PIN has no non-repudiation aspect.

These should always be considered by the disputant parties and adjudicator when determining liability. Of course, the possibility of first party fraud and second party fraud instead of third party fraud also should always be considered.

From a legal perspective, many regulations have obliged banks to secure their ATM/debit card system. These obligations include the obligation to conduct fraud risk education in order to safeguard consumer safety in ATM/debit card transactions. Many of the regulations are quite detailed and are to be complied with as a security standard that banks should meet in their ATM/debit card operations. This includes the obligation to encrypt ATM/debit card data, provide anti malware and firewalls, perform logical and physical surveillance of the consumer activated terminals, and so on. Therefore, banks absolutely have occupiers' liability for their consumers in ATM/debit card operations, because the entire ATM/debit card system and infrastructure are provided by the banks and banks intentionally invite their consumer to perform the ATM/debit card transaction in banks' consumer activated terminals such as ATMs and EFTPOS terminals. In this regard, the regulations also clearly define that banks have vicarious liability for their agent or third party counterpart. It is also clearly stated in the regulation and court verdicts that banks should still be responsible and liable for a consumer's loss even though the damages were caused by third party attack. Hence, a

new intervening act or *novus actus interveniens* is not acceptable as a defence submitted by banks. All in all, it is argued that banks indeed have statutory duty and owe a duty of care to consumers.

From the analysis of courts verdicts on unauthorised ATM/debit card disputes between banks and consumers, it is revealed that judges in Indonesia still utilised the old, unjust and largely abandoned pure contributory negligence principle when determining the party liable for the damages. The judges also appear unable to understand the complete picture of the facts involved in unauthorised ATM/debit card transactions. Apparently, this occurred due to judges' lack of knowledge of the economic aspects, as well as the state-of-the-art technology employed, and legal aspects that are relevant to ATM/debit card operations. Consequently, the judges — almost without fail — direct that the consumer bear all their losses, often just based on anecdotal evidence that the consumer must be fault or negligent and contributed to the unauthorised ATM/debit card transaction. In this regard, the fact that a consumer probably only has slightly negligent conduct compared to the dominant negligence by banks was not a factor in their consideration of the cases before them. In most other countries, the pure contributory negligence principle has been replaced by the comparative negligence principle, which is deemed fairer, and could trigger incentives for banks and consumers to improve their precautions to avoid identity theft/fraud.

Therefore, there is no doubt that legal reform should be implemented in the adjudication proceedings to resolve disputes between banks and consumers concerning which party should be liable for consumer losses from unauthorised ATM/debit card transactions. In this regard, it is argued that several legal reforms should be implemented in the ADR/court proceedings concerning unauthorised ATM/debit card transaction disputes in order to achieve the most sensible result. These reforms include:

- in general, adjudicators should consider all economic, technological, and legal aspects that involved in the specific unauthorised ATM/debit card transaction in order to have a comprehensive picture of the circumstances of the specific identity theft and/or fraud;
- the comparative negligence principle should replace the pure contributory negligence principle;

- the least cost avoider should be determined on the basis of the location of the point of compromise in the specific identity theft and/or fraud circumstances;
- since a bank is the owner of the ATM/debit card system and possesses all ATM/debit card transactions data, the onus of proof should lie with the bank instead of on the consumer's shoulders. In this regard, negligence per se and *res ipsa loquitur* doctrine should be acknowledged by adjudicators; and
- a bank cannot have as a defence only that the fraudulent transaction conducted with the correct consumer's card data and PIN.

It is believed that law reform on the ADR/court adjudication proceedings using economic, technological, and legal approaches will create more accurate, fair, and sensible decisions. Pertaining to this, several recommendations on law reform in civil liability adjudication/litigation proceedings have been drawn in Chapter 7. These include recommendations:

- to use negligence per se as a basis for civil liability adjudication. To give clear inputs to stakeholders in a dispute on an unauthorised ATM/debit card transaction, Table 5 'ATM/debit Card Point of Compromise, Identity Theft Methods and Bank's Statutory Duties' depicts many bank obligations to improve security features to combat fraud based on regulations;
- to ensure that in tortious liability/negligence liability civil lawsuits that the burden of proof in the adjudication proceedings lies with the defendant, based on provisions in *LCP* and *LIET*; or based on the *res ipsa loquitur doctrine* (as is argued in the thesis); and
- a flow chart of test for the use of the comparative negligence doctrine (Figure 20) to establish whether a defendant owes a duty of care to a plaintiff or has breached of duty of care, and also to establish the causality between the defendant's breach and plaintiff's losses. In order to fairly allocate the loss to the least cost avoider, multi-disciplinary approaches that contain economic, technological, and legal approaches were utilised. From the flow chart test using the comparative negligence approach, it is apparent that a defendant cannot avoid liability for plaintiff losses caused by unauthorised ATM/debit card transaction for a number of reasons. First, the defendant as a professional and fiduciary entity has a statutory duty to safeguard a consumer's safety; secondly,

most of the fraud risks are foreseeable; and thirdly, in many instances, a defendant was negligent in fulfilling its obligation to secure its ATM/debit card infrastructure and provide adequate fraud risk education to consumers.

However, to mitigate the risk of prolonged disputes and misleading adjudication verdicts that might occur because of different interpretations by banks, consumers, and adjudicators concerning what constitutes fault or negligence on unauthorised ATM/debit card transactions (considering that every adjudicator might have a different level of knowledge regarding relevant and recent economic, technological and legal factors), it is also argued that in the quest for the liable party in any such dispute, it is important that a set of clear, fair, detailed, and decisive loss allocation rules on unauthorised ATM/debit card be established and used as a common binding guide. Therefore, having compared and analysed the advantages and disadvantages of US and Australian loss allocation rules regulation, it is submitted that the ePayment Code of Australia is more appropriate for Indonesia's current legal and regulatory framework for unauthorised ATM/debit card transactions. It is believed that the establishment of detailed and clear bank and consumer liability on unauthorised ATM/debit card transactions, based on specific circumstances, will create far more uniform and predictable results. It is expected that this kind of regulation could encourage disputant parties to resolve the dispute between themselves, and hence avoid the hassle and the waste of excessive resources in terms of both time and money for dispute adjudication in ADR/court forums.

It is also believed that the Australian model is fairer because it puts the consumer and the bank in a relatively equal position. In the ePayment Code, a bank is also not allowed to use the defence with the sole evidence that the unauthorised ATM/debit card transaction had been conducted using the correct consumer ATM/debit card data and PIN. Therefore, it is believed that the adoption of the Code could also give greater incentives for bank and consumer in Indonesia to avoid losses from identity theft/fraud. On the one hand, it is expected that banks will have more incentives to improve their ATM/debit card infrastructure security features, including the use of surveillance and security guard personnel, and pay more attention to their agent or third party infrastructure and procedures, and give comprehensive fraud risk education to consumers. To be able avoid liability, it is believed that banks will put more

surveillance devices such as CCTV on their ATM infrastructure and ensure their regular maintenance. Hence, in first party fraud and second party fraud, the bank will have more opportunity to create a legitimate defence, by submitting that there more than just the fact that the correct card and PIN were used in the transaction. On the other hand, consumers also will have greater incentive to be more vigilant after having had fraud risk education from banks so as to avoid become the victim of fraud and/or be liable for losses. This ePayment Code can be adopted in Indonesia in either the banking industry code of conduct (or also known as ‘by-laws’) or in the form of Bank Indonesia’s Regulation (loss imposition).

Conversely, the US fraud liability model (*EFTA* and Regulation E) which employs strict liability rules which put more liability on banks, though it probably has justification from loss-spreading, loss-reduction, and loss-imposition principle (by being easy to administer). However, it is feared that this kind of fraud liability model is not appropriate for retail payment system such as ATM/debit card transactions where consumer involvement in the initial transaction is necessary, especially as a holder of a payment card. Empirical evidence has also shown that consumers — as probably the weakest in the link in the ATM/debit card operation — have become a prominent target for identity theft, especially from social engineering attacks. Therefore, it is believed that the US fraud liability model will create disincentives, especially for consumers, to improve precautions. This result would be unfair for banks and it is feared that such an approach could nurture the proliferation of fraudulent activities.

It is submitted, that even though this thesis specifically only discusses loss allocation rules for unauthorised ATM/debit card transactions, the economic, technological, and legal principles embedded in the discussion could arguably also be implemented in other types of unauthorised electronic banking transactions such as card not present, internet banking, and SMS banking fraud — of course with appropriate modification according to the specific point of compromise and e-banking circumstances.

BIBLIOGRAPHY

Articles, Books, Reports

Adepoju, Adelowo Solomon and Mohammed Enagi Alhassan, 'Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria - A Case Study of Selected Banks in Minna Metropolis' (2010) 15(2) *Journal of Internet Banking and Commerce*

Akindemowo, Olujoke, 'Electronic Payment Systems and Cyberbanking' in Jay Forder and Patrick Quirk (eds), *Electronic Commerce and the Law* (John Wiley & Sons 2001)

Albrecht, W Steve et al, *Fraud Examination* (South-Western, 2012)

Anderson, Ross et al, 'Security Economics and the Internal Market' (European Network and Information Security Agency, 2008)

Anderson, Ross J, 'Liability and computer security: Nine principles' in *Computer Security—ESORICS 94* (Springer, 1994) 231

Arora, Anu, *Electronic Banking and the Law* (IBC Financial Books, 1988)

Atmasasmita, Romli, *Pengantar Hukum Kejahatan Business [Introduction to the Law on Bisnis Fraud]* (Prenada Media, 2003)

Australian Securities & Investments Commission, 'Discussion Paper on an Expanded EFT Code of Conduct' (Australian Securities & Investment Commission's, July 1999)

Australian Securities & Investments Commission (ASIC), 'Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC Proposals' (2008)

Australian Securities & Investments Commission (ASIC), 'Reviewing the EFT Code' (Consultation Paper 78, Australian Securities & Investments Commission, 2007)

Badan Pembinaan Hukum Nasional, '*Laporan Akhir Penelitian Perlindungan Konsumen Atas Kelalaian Produsen* [Research Final Report on Consumer Protection over Producer Negligence]' (Departemen Kehakiman, 1992)

Bank Indonesia, '*Laporan Bulanan Sistem Pembayaran Periode Maret* (Payment System Monthly Report: March 2013)' (2013)

Barwise, Mike and Daniel Bachfeld, *Attack of the Card Cloners* (2007) The H Security <<http://www.h-online.com/security/features/Manipulated-ATMs-746193.html>>

Basel Committee on Banking Supervision (BCBS), *Risk Management for Electronic Banking and Electronic Money Activities* (Bank for International Settlements, 1998)

Basel Committee on Banking Supervision (BCBS), 'Risk Management Principles for Electronic Banking' (Bank for International Settlement, 2003)

- Bell, Judith, *Doing Your Research Project: A Guide for First-Time Researchers in Education and Social Science* (McGraw-Hill, 1999)
- Benson, Carol Coye and Scott Loftesness, *Payments Systems in the US* (Glenbrook Partners, 2010)
- Berkman, Omer and Odelia Moshe Ostrovsky, 'The Unbearable Lightness of PIN Cracking' (2007) 4886 *Lecturer Notes in Computer Science* 224
- Bevan, Alexander H, *Alternative Dispute Resolution* (Sweet and Maxwell, 1992)
- Blomquist, Robert F, 'The Trouble with Negligence Per Se' (2009) 61(2) *South Carolina Law Review* 221
- Blommestein, Hans J and Bruce J Summers, 'Banking and the Payment System' in Bruce J Summers (ed), *The Payment System: Design, Management and Supervision* (International Monetary Fund, 1994)
- Board of Governors of the Federal Reserve System, 'Report to the Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Product' (1997)
- Bohm, Nicholas, Ian Brown and Brian Gladman, 'Electronic Commerce: Who Carries the Risk of Fraud?' (2003) (3) *Journal of Information & Technology*
- Bond, Mike and Piotr Zielinski, 'Decimalisation Table Attacks for PIN Cracking' (University of Cambridge computer Laboratory Technical Report TR-560, 2003) <<http://www.cl.cam.ac.uk/~mkb23/research/PIN-Cracking.pdf>>
- Bolton, Richard J and David J Hand, 'Statistical Fraud Detection: A Review' (2002) 17(3) *Statistical Science*
- Bradbury, Danny, 'A Hole in the Security Wall: ATM Hacking' (2010) 2010(6) *Network Security*
- Braun, Michele et al, 'Understanding Risk Management in Emerging Retail Payments' (2008) 14(2) *Economic Policy Review - Federal Reserve Bank of New York* 137
- Budnitz, Mark E, 'Commentary: Technology As The Driver of Payment System Rules: Will Consumers Be Provided Seatbelts and Air Bags?' (2009) 83(2) *The Chicago-Kent Law Review*
- Bottomley, Stephen and Simon Bronitt, *Law in Context* (Federation Press, 3rd ed, 2006)
- Calabresi, Guido, 'Some Thoughts on Risk Distribution and the Law of Torts' (1961) 70(4) *The Yale Law Journal* 499

Carbo-Valverde, Santiago and Fransisco Rodriquez Fernandez, 'Competing Technologies for Payments: ATMs, POS Terminals and the Demand for Currency' (Federal Reserve Bank of Chicago, 2009)

Cartwright, Peter, 'Consumer Protection in Financial Services: Putting the Law in Context' in Peter Cartwright (ed), *Consumer Protection in Financial Services* (Wolters Kluwer, 1999)

Casey, Eoghan, *Digital Evidence and Computer Crime* (Academic Press, 2000)

Chandler, Jennifer A, 'Negligence Liability for Breaches of Data Security' (2008) 23(2) *Banking and Finance Law Review*, 223

Choo, Kim-Kwang Raymond, 'The Cyber Threat Landscape: Challenges and Future Research Directions' (2011) 30(8) *Computer & Security* 719

Claessens, Joris et al, 'On the Security of Today's Online Electronic Banking Systems' (2002) 21(3) *Computers & Security* 253

Clarke, Roger and Alana Maurushat, 'Passing the Buck: Who Will Bear the Financial Transaction Losses from Consumer Device Insecurity' (2007) 18 *JL Inf. & Sci.* 8

Colombatto, Enrico, 'A Free-Market View on Accidents and Torts' (2014) 77(2) *Law and Contemporary Problems* 117

Committee on Payment and Settlement Systems (CPSS), 'Core Principles for Systemically Important Payment Systems' (Bank for International Settlements, 2001)

Committee on Payment and Settlement Systems (CPSS), *A Glossary of Terms Used in Payment and Settlement Systems* (Bank for International Settlements, revised ed, 2003)

Committee on Payment and Settlement Systems (CPSS), Bank for International Settlements, 'Core Principles for Effective Banking Supervision (Basel Core Principles)' (Bank for International Settlements, 1997)

Committee on Payment and Settlement Systems (CPSS), 'Clearing and Settlement Arrangements for Retail Payments in Selected Countries' (Bank for International Settlement, 2000)

Committee on Payment and Settlement Systems (CPSS), 'Policy Issues for Central Banks in Retail Payments' (Bank for International Settlements, 2003)

Committee on Payment and Settlement Systems (CPSS), 'Retail Payments in Selected Countries: A Comparative Study' (Bank for International Settlements, 1999)

Cooter, Robert D and Edward L Rubin, 'A Theory of Loss Allocation for Consumer Payments' (1987) 66 *Texas Law Review* 63

Council Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market [2007] OJ L 319/1 ('European Payment Services Directive').

Davidson, Alan, *The Law of Electronic Commerce* (Cambridge University Press, 2009)

Davies, Martin and Ian Malkin, *Torts* (LexisNexis Butterworths, 5th ed, 2008)

Department of Economic and Social Affairs, 'United Nations Guidelines for Consumer Protection (as expanded in 1999)' (United Nations, 2003)

Devos, Jan and Igor Pipan, 'The Role of IT/IS in Combating Fraud in the Payment Card Industry' (2009) 14(3) *Journal of Internet Banking and Commerce*

Diebold Incorporated, 'White Paper: ATM Fraud and Security' (2002)

Directorate of Banking Research and Regulation, Financial System Stability Bureau, 'Financial Stability Review No. 14, March 2010' (Bank Indonesia, 2010) <<http://www.bi.go.id/NR/rdonlyres/9379845A-3B22-488D-A5BA-6D08321BAD03/20251/FSR14March2010.pdf>>

Division of Supervision, Federal Deposit Insurance Corporation (FDIC), 'Electronic Banking: Safety and Soundness Examination Procedures' (Federal Deposit Insurance Corporation, 1998)

Djumhana, Muhamad, *Asas-Asas Hukum Perbankan Indonesia [Principles of the Indonesian Banking Law]* (PT Citra Aditya Bakti, 2008)

Dorminey, Jack et al, 'The Evolution of Fraud Theory' (2012) 27 *Issues in Accounting Education* 555

Douglass, Duncan B, 'An Examination of the Fraud Liability Shift in Consumer Card-Based Payment Systems ' (2009) 33 *Economic Perspectives* 43

Drimer, Saar, Steven J Murdoch and Ross Anderson, 'Failures of Tamper-Proofing in PIN Entry Devices' (2009) 7 *IEEE Security & Privacy Magazine* 39

Heckel, Fred E and Fowler V Harper, 'Effect of the Doctrine of Res Ipsa Loquitur' (1928) 22 *Illinois Law Review* 724

Edwards, Robin, 'Working Out Loss Liability in the Light of Efficiency Principles' in Wickrema Weerasooria (ed), *Financial Regulation and Payment Systems* (Prospect Media, 2001)

Electronic Banking Group, 'Electronic Banking Group Initiatives and White Papers' (Basel Committee on Banking Supervision, 2000)

Epstein, Richard A and Thomas P Brown, 'Cybersecurity in the Payment Card Industry' (2008) 75 *University of Chicago Law Review* 203

European Central Bank, 'Report on Card Fraud' (2012)

Facciolo, Francis J, 'Unauthorized Payment Transactions and Who Should Bear the Losses' (2009) 83(2) *Chicago-Kent Law Review* 605

Federal Financial Institutions Examination Council (FFIEC), 'E-Banking' (2003)

Federal Financial Institutions Examination Council (FFIEC), 'Retail Payment Systems' (Federal Financial Institutions Examination Council, 2004)

Federal Financial Institutions Examination Council (FFIEC), *Information Security* (Federal Financial Institution Examination Council, 2006)

Franz, Charles R and Sharon A Asbill, 'Liability Implications in Electronic Fund Transfers' (1982) 5 *Information & Management* 87

Directorate of Banking Research and Regulation, Financial System Stability Bureau, 'Financial Stability Review I - 2006' (Bank Indonesia, 2006)

Flaming, Mark, Klaus Prochaska and Stefan Staschen, 'Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia' (CGAP, 2009) <<http://www.cgap.org/gm/document-1.9.34817/Branchless%20Banking%20Diagnostic%20in%20Indonesia.pdf>>

Fry, Maxwell J et al, *Payment Systems in Global Perspective* (Routledge, 2009)

Fuady, Munir, *Perbuatan Melawan Hukum [Tort]* (PT Citra Aditya Bakti, 2010)

Garner, Bryan A (ed), *Black's Law Dictionary* (West Group, 9th ed, 2009)

Gates, Tiffany and Katy Jacob, 'Payments Fraud: Perception versus Reality - A Conference Summary' (2009) XXXIII(1) *Economic Perspectives*

Gautama, Sudargo, *Indonesian Business Law* (PT Citra Aditya Bakti, 2006)

Geva, Benjamin, 'Consumer Liability in Unauthorized Electronic Funds Transfers' (2003) 38 *Canadian Business Law Journal* 207

Gercke, Marco, 'Legal Approaches to Criminalize Identity Theft' in United Nations Office on Drugs and Crime (ed), *Handbook on Identity-related Crime* (United Nations, 2011)

Geva, Benjamin, *The Law of Electronic Funds Transfer* (LexisNexis, Release No 9 ed, 2001)

Gibson, Andi and Douglas Fraser, *Business Law* (Pearson Prentice Hall, 2nd ed, 2006)

Gifford, Nick, *Information Security: Managing the Legal Risk* (CCH Australia Limited, 2009)

- Gillette, Clayton P, 'Rules, Standards, and Precautions in Payment Systems' (1996) 82 *Virginia Law Review* 181
- Glaessner, Thomas C, Tom Kellermann and Valerie McNevin, 'Electronic Safety and Soundness: Securing Finance in a New Age' (The World Bank, 2004)
- Gleason, Kristeen and Dan Heimann, *Electronic Banking, Doing Business Electronically* (Springer-Verlag, 1998)
- Grabosky, Peter, Russell G Smith and Gillian Dempsey, *Electronic Theft: Unlawful Acquisition in Cyberspace* (Cambridge University Press, 2001)
- Goddard, Claire and Michael Deakin, 'Managing Treasury Security' in Brian Welch (ed), *Electronic Banking and Treasury Security* (Woodhead Publishing, 1999)
- Greene, Mark N, 'Divided We Fall: Fighting Payments Fraud Together' (2009) 33(1) *Economic Perspectives* 37
- Gup, Benton E and James W Kolari, *Commercial Banking: The Management of Risk* (John Willey & Sons, Inc, 3rd ed, 2005)
- Hancock, Diana and David B Humphrey, 'Payment Transactions, Instruments, and Systems: A Survey' (1998) 21 *Journal of Banking & Finance* 1573
- Hayashi, Fumiko and Zhu Wang, 'Product Innovation and Network Survival in the US ATM and Debit Card Industry' (2009 (Revised 2011)) *SSRN Working Paper Series*
- Hayashi, Fumiko, Richard Sullivan and Stuart E Weiner, 'A Guide to the ATM and Debit Card Industry' (Federal Reserve Bank of Kansas City, 2003)
- Hendry, Mike, *Smart Card Security and Applications* (Artech House, 2nd ed, 2001)
- Hermansyah, *Hukum Perbankan Nasional Indonesia [Indonesia National Banking Law]* (Kencana, 2005)
- Hillebrand, Gail, 'Before the Grand Rethinking: Five Things To Do Today with Payments Law and Ten Principles To Guide New Payments Products and New Payment Law' (2009) 83(2) *Chicago-Kent Law Review*
- Hunt, Robert M, 'An Introduction to the Economics of Payment Card Networks' (Federal Reserve Bank of Philadelphia, 2003)
- Hutchinson, Terry, *Researching and Writing in Law* (Thomson Lawbook, 2nd ed, 2006)
- Iannacci, Jerry and Ron Morris, *Access Device Fraud and Related Financial Crimes* (CRC Press LLC, 2000)
- Idroes, Ferry N and Sugiarto, *Manajemen Risiko Perbankan: Dalam Konteks Kesepakatan Basel dan Peraturan Bank Indonesia [Risk Management in Banking: Within Basel and Bank Indonesia Regulatory Context]* (Graha Ilmu, 2006)

Imaniyati, Neni Sri, *Pengantar Hukum Perbankan Indonesia [Introduction to Indonesia Banking Law]* (Refika Aditama, 2010)

Irawan, Candra, *Aspek Hukum dan Mekanisme Penyelesaian Sengketa di Luar Pengadilan (Alternative Dispute Resolution) di Indonesia [Legal Aspect and Alternative Dispute Resolution Mechanism in Indonesia]* (CV Mandar Maju, 2010)

Irianto, Sulistyowati, 'Hukum dan Hakim [Law and Judge]', *Kompas* 16 October 2013, 7

Jamie B Stewart (Jr), 'Changing Technology and the Payment System' (2000) 6 (11) *Current Issues in Economics and Finance* 1

Javelin Strategy & Research, '2010 LexisNexis True Cost of Fraud Study' (LexisNexis, 2010)

Kelsen, Hans, *Teori Umum Tentang Hukum dan Negara [General Theory on Law and State]* (Nusa Media, 2011)

Khan, Atiqur Rahman and Masud Karim, 'E-Banking and Extended Risks: How to Deal with the Challenge? ' (Working Paper, University of Rajshahi, 2010) <http://www.ru.ac.bd/finance/images/stories/working_papers/ebanking-edited.pdf>

Kim, Rachel, '2007 Identity Fraud Report - Consumer Version: How Consumers Can Protect Themselves' (Javelin Strategy & Research, 2007)

Kondabagil, Jayaram, *Risk Management in Electronic Banking: Concepts and Best Practices* (John Wiley & Sons (Asia) 2007)

Kristiyanti, Celina Tri Siwi, *Hukum Perlindungan Konsumen [Consumer Protection Law]* (Sinar Grafika, 2008)

Krivko, M, 'A Hybrid Model for Plastic Card Fraud Detection Systems' (2010) 37(8) *Expert Systems with Applications* 6070

Kusuma, Mahesa Jati, *Hukum Perlindungan Nasabah bank: Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan Informasi dan Transaksi Elektronik (ITE) di Bidang Perbankan [Bank Consumers Protection Law: Legal Measures to Protect Bank Consumers from Information and Electronic Transactions Crime (ITE) in Banking Sector]* (Nusa Media, 2012)

Lawrence, Lary, *An Introduction to Payment Systems* (Aspen Publishers, 1997)

Lee, Dellas W and Timothy R Zinnecker, *Payment Systems, Banking and Documentary Transactions: Problems, Cases and Comments* (Carolina Academic Press, 2003)

Lee, Dong-Tsan, 'Re-examining the Security Issues of ATM Systems' (2004) 2004(2) *Computer Fraud & Security*

- Lemek, Jeremias, *Mencari Keadilan: Pandangan Kritis Terhadap Penegakan Hukum di Indonesia* [Searching for Justice: Critical View toward Law Enforcement in Indonesia] (Galang Press, 2007)
- Levi, Michael and John Burrows, 'Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey' (2008) 48(3) *British Journal of Criminology* 293
- Levi, Michael and Jim Handley, *Criminal Justice and the Future of Payment Card Fraud* (Institute for Public Policy Research, 2002)
- Levitin, Adam J, 'Private Disordering: Payment Card Fraud Liability Rules' (2011) 5 *Brooklyn Journal of Corporate, Financial and Commercial Law*
- Lewis, Wayne K and Steven H Resnicoff, *Negotiable Instruments and Other Payment Systems: Problems and Materials* (LexisNexis, 2004)
- Litan, Robert E and Martin Neil Baily, 'Introduction' in Robert E Litan and Martin Neil Baily (eds), *Moving Money: The Future of Consumer Payments* (Brookings Institution Press, 2009)
- Madan, M S and M A Reid, 'Data Processing Aspects of the Integrated Circuit and Magnetic Stripe Cards' (1992) 22(1) *Information & Management* 41
- Makarim, Edmon, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik* [Electronic Provider Liability] (RajaGrafindo Persada, 2010)
- Makhijani, Dyah Nastiti K, 'Payment Systems in Indonesia' in *Payment Systems in EMEAP Economies* (Executives' Meeting of East Asia-Pacific Central Banks and Monetary Authorities (EMEAP) 2002)
- Mali, Pooja et al, 'Multilevel ATM Security Based on Two Factor Biometrics' (2012) 1(8) *International Journal of Engineering Research and Technology (IJERT)*
- Malphrus, Steve, 'Perspectives on Retail Payments Fraud' (2009) XXXIII *Economic Perspectives* 31
- Manan, Bagir, *Menegakkan Hukum Suatu Pencarian* [Raising the Law: A Search] (Asosiasi Advokat Indonesia, 2009)
- Mann, Ronald J, *Payment Systems and Other Financial Transactions; Cases, Materials, and Problems* (Aspen Publishers, 3rd ed, 2006)
- Mann, Ronald J., 'Making Sense of Payments Policy in the Information Age' (2005) 93 *Georgetown Law Journal*
- Mannan, Mohammad and P C van Oorschot, 'Reducing Threats from Flawed Security APIs: The Banking PIN Case' (2009) 28(6) *Computers & Security*
- Marzuki, Peter Mahmud, *An Introduction to Indonesian Law* (Setara Press, 2011)

- Marzuki, Peter Mahmud, *Pengantar Ilmu Hukum [An Introduction to Law]* (Kencana, 2008)
- Masters, Gerry and Philip Turner, 'Forensic Data Recovery and Examination of Magnetic Swipe Card Cloning Devices' (2007) 4 *Digital Investigation*
- Matyas, Vaclav et al, 'Authorizing Card Payments with PINs' (2008) 41(2) *Computer* 64
- Marciano, Alain and Giovanni B Ramello, 'Consent, Choice, and Guido Calabresi's Heterodox Economic Analysis of Law' (2014) 77(2) *Law and Contemporary Problems* 97
- McCullagh, Andrian and William Caelli, 'Non-Repudiation in the Digital Environment' (2000) 5(8) *First Monday, Peer-Reviewed Journal on the Internet*
- McCullagh, Andrian, 'Legal Aspects of Electronic Contract and Digital Signatures' in Anne Fitzgerald et al (eds), *Going Digital 2000* (Prospect Media Pty Ltd, 2nd ed, 2000)
- Mertokusumo, Sudikno, *Hukum Acara Perdata Indonesia [Indonesia's Proceeding Law]* (Liberty Yogyakarta, 2006)
- Mertokusumo, Sudikno, *Mengenal Hukum: Suatu Pengantar [Knowing the Law: An Introduction]* (Universitas Atma Jaya Yogyakarta, 2010)
- Meyer, Carl H and Stephen M Matyas, *Cryptography: A Guide for the Design and Implementation of Secure Systems* (John Wiley & Sons, 1982)
- Miller, Geoffrey P, 'Law and Economics versus Economic Analysis of Law' (2011) 19(2) *American Bankruptcy Institute Law Review* 459
- Miller, Fred H and Alvin C Harrell, *The Law of Modern Payment Systems* (Thomson West, 2003)
- Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, 'Final Report Model Criminal Code on Chapter 3 - Credit Card Skimming Offences' (2006)
<[http://www.lawlink.nsw.gov.au/lawlink/SCAG/ll_scag.nsf/vwFiles/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf/\\$file/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf](http://www.lawlink.nsw.gov.au/lawlink/SCAG/ll_scag.nsf/vwFiles/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf/$file/MCLOC_MCC_Chapter_3_Credit_Card_Skimming_Report.pdf)>
- Mohamad, Hanna, 'Background Paper: Plastic Card Fraud' (NSW Government, 2011)
- Mohamad, Karnoto et al, *Mendorong Langkah Maju Menuju Less Cash Society [Encouraging Step Forward toward Less Cash Society]* (Infobank, 2008)
- Mohammed, Lawan Ahmed, 'On the Design of Secure ATM Systems' in Lawan Ahmed Mohammed and Mubarak S. Al-Mutairi (eds), *Cases on ICT Utilization, Practice and Solutions: Tools for Managing Day-to-Day Issues* (IGI Global, 2010)

- Morse, Edward A and Vasant Raval, 'PCI DSS: Payment Card Industry Data Security Standards in Context' (2008) 24 *Computer Law and Security Review: International Journal of Technology and Practice* 540
- Muhamad, Karnoto, '*Focus: Rating 118 Bank Versi Infobank 2015* [2015 Infobank Version Rating 118 Banks]', *Infobank* July 2015 2015
- Muhammad, Abdulkadir, *Hukum Perdata Indonesia [Indonesia Civil Law]* (Citra Aditya Bakti, 2010)
- Murdoch, S J, 'Reliability of Chip & PIN Evidence in Banking Disputes' (2009) 6(12) *Digital Evidence and Electronic Signature Law Review* 1
- Murdock, Hernan, 'The Three Dimensions of Fraud' (2008) 65 *The Internal Auditor* 81
- Nakajima, Masashi, *Payment System Technologies and Functions: Innovations and Developments* (Business Science Reference, 2011)
- Narasimhan, R, *Frauds in Banks* (ICFAI University Press, 2005)
- Nitsure, Rupa Rege, *E-Banking: Challenges and Opportunities* (ICFAI University Press, 2006)
- Nsouli, Saleh M and Andrea Schaechter, 'Challenges of the E-Banking Revolution' (2002) 39(3) *Finance and Development*
<<http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm>>
- Nugroho, Susanti Adi, *Proses Penyelesaian Sengketa Konsumen Ditinjau Dari Hukum Acara Serta Kendala Implementasinya [Consumer Dispute Settlement Process from Procedural Law Perspective and its Implementation Constrains]* (Kencana Prenada Media Group, 2006)
- Nurdin, Boy, *Kedudukan dan Fungsi Hakim Dalam Penegakan Hukum di Indonesia [The Position and Function of Judges in Law Enforcement in Indonesia]* (PT Alumni, 2012)
- Nuryanti, Ida and Susiati Dewi, 'Chapter 3: the Development of E-Payment and Challeges in Indonesia ' in Vincent Lim Choon Seng (ed), *The Development of E-Payments and Challenges for Central Banks in the SEACEN Countries* (South East Asian Central Banks (SEACEN) Research and Training Centre, 2008)
- Organisation for Economic Co-operation and Development (OECD), 'OECD Policy Guidance on Online Identity Theft' (2008)
- Owen, Darrell E et al, 'Indonesia - Information and Communications Technologies (ICT) Assessment (Technical Report)' (USAID/ECG, 16 January 2001)
- Parker, Donn B, *Fighting Computer Crime: A New Framework for Protecting Information* (John Wiley and Sons, 1998)

Pennathur, Anita K, "'Clicks and Bricks': e-Risk Management for Banks in the Age of the Internet' (2001) 25 *Banking and Finance*

Phair, Nigel, *Cybercrime: The Reality of the Threat* (E-Security Publishing, 2007)

Pingitzer, Jurgen C and Bruce J Summers, 'Small-Value Transfer Systems' in Bruce J Summers (ed), *The Payment System: Design, Management, and Supervision* (International Monetary Fund, 1994)

Pipkin, Donald L, *Information Security: Protecting the Global Enterprise* (Prentice Hall PTR, 2000)

Pompe, Sebastiaan, *The Indonesian Supreme Court: A Study of Institutional Collapse* (Cornell Southeast Asia Program, 2005)

Posner, Richard A, 'Values and Consequences: An Introduction to Economic Analysis of Law' (The University of Chicago Law School, 1998)

Priliasari, Erna, '*Mediasi Perbankan Sebagai Wujud Perlindungan Terhadap Nasabah Bank* [Banking Mediation as Promulgation of Banking Customer Protection]' (2008) 5(2) (Juni) *Jurnal Legislasi Indonesia*

PT. Bank Negara Indonesia (Persero) Tbk, *Ketentuan Umum dan Persyaratan Pembukaan Rekening* [General Terms and Conditions for Account Opening] (2012)

Pusat Riset dan Edukasi Kebanksentralan, '*Hasil Survey Pemetaan Kejahatan Identity Theft dan Fraud Pada Alat Pembayaran Menggunakan Kartu: Pencegahan, Mitigasi dan Perlindungan Konsumen di Indonesia* [Survey Result on Taxonomy of Identity Theft and Fraud on Payment Card Instrument: Prevention, Mitigation and Consumer Protection in Indonesia] (BI-Fraud Survey)' (Bank Indonesia, 2015)

Radhakrishna, Gita, 'Liability Issues in Internet Banking in Malaysia' (2009) 7 *IUP Journal of Bank Management*

Radu, Christian, *Implementing Electronic Card Payment Systems* (Artech House, 2003)

Rahardjo, Satjipto, *Penegakan Hukum Progresif* [Progressive Law Enforcement] (Kompas, 2010)

Rahardjo, Satjipto, *Sisi-sisi Lain dari Hukum di Indonesia* [The Other Sides of Law in Indonesia] (Kompas, 2003)

Ramamoorti, Sridhar, 'The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component into Fraud and Forensic Accounting Curricula' (2008) 23(4) *Issues in Accounting Education* 521

Ramasasthy, Anita, 'Confusion and Convergence in Consumer Payments: Is Coherence in Error Resolution Appropriate' (2008) 83 *Chi.-Kent L. Rev.* 813

Rambure, Dominique and Alec Nacamuli, *Payment Systems: From the Salt Mines to the Board Room* (Palgrave Macmillan, 2008)

Ramli, Ahmad M, Pager Gunung and Indra Apriadi, *Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik [Toward Legal Certainty in Information and Electronic Transaction]* (Departemen Komunikasi dan Informatika Republik Indonesia 2006)

Reavley, Nigel, 'Flexibility, Fraud and Two-Factor Authentication' (2007) 19 *Card Technology Today* 12

Roberds, William, 'The Impact of Fraud on New Methods of Retail Payment' (1998) First Quarter *Federal Reserve Bank of Atlanta Economic Review*

Rochet, Jean Charles and Jean Tirole, 'Externalities and Regulation in Card Payment Systems' (2006) 5(1) *Review of Network Economics*

Rosenberg, Arnold S, 'Better Than Cash? Global Proliferation of Debit and Prepaid Cards and Consumer Protection Policy ' (Working Paper No 766, Bepress Legal Series, 2005)

Rusch, Linda J, 'Reimagining Payment Systems: Allocation of Risk for Unauthorized Payment Inception' (2009) 83(2) *Chicago-Kent Law Review* 561

Rusch, Linda J and Stephen L Sepinuck, *Payment Systems: Problems, Materials, and Cases* (West, 4th ed, 2011)

Rustad, Michael and Cyrus Daftary, *E-Business Legal Handbook* (Aspen Law & Business, 2001)

Rutledge, Susan L et al, 'Good Practices for Consumer Protection and Financial Literacy in Europe and Central Asia: A Diagnostic Tool' (The World Bank, 2010)

Samsul, Inosentius, '*Pengembangan Model Penyelesaian Sengketa Perbankan Dalam Perspektif Perlindungan Kepentingan Konsumen [Development of Banking Dispute Settlement Model From Consumer Protection Perspective]*' (2009) 7(1) (January) *Buletin Hukum Perbankan dan Kebangsentralan*

Samsul, Inosentius, *Perlindungan Konsumen: Kemungkinan Penerapan Tanggung Jawab Mutlak [Consumer Protection: the Possibility to Apply Absolute Liability]* (Universitas Indonesia, 2004)

Samudera, Teguh, *Hukum Pembuktian Dalam Acara Perdata [Evidence Law in the Law on Civil Procedure]* (Alumni, 1992)

Saville, Julie and Nancy Loomis, 'Why Wait for EMV to Solve Your Fraud Problems? One-Time Use Card Numbers Can Reduce Debit Fraud Now' (First Data Corporation, 2010) <<http://www.firstdata.com/downloads/thought-leadership/one-time-card-star-cert-wp.pdf>>

Schaechter, Andrea, 'Issues in Electronic Banking: An Overview - IMF Policy Discussion Paper' (International Monetary Fund, 2002)

Schreft, Stacey L, 'Risks of Identity Theft: Can the Market Protect the Payment System?' (2007) 92(4) *Economic Review - Federal Bank of Kansas* 5

Sembiring, Sentosa, *Hukum Perbankan: Edisi Revisi [Banking Law: Revision Edition]* (Mandar Maju, 2012)

Setiawan, Aneka Masalah Hukum dan Hukum Acara Perdata [*Various Legal Problems and the law on Civil Procedure*] (Alumni, 1992)

Setiawan, Rachmat, *Tinjauan Elementer Perbuatan Melawan Hukum [Basic Overview of Tort]* (Alumni, 1982)

Shofie, Yusuf, *Kapita Selekta Hukum Perlindungan Konsumen di Indonesia [Consumer Protection Law in Indonesia]* (PT Citra Aditya Bakti, 2008)

Shofie, Yusuf, *Perlindungan Konsumen dan Instrumen-instrumen Hukumnya [Consumer Protection and Its Legal Instruments]* (Citra Aditya Bakti, 2009)

Siahaan, NHT, *Hukum Konsumen: Perlindungan Konsumen dan Tanggung Jawab Produk [Consumer Law: Consumer Protection and Product Liability]* (Panta Rei, 2005)

Sidabalok, Janus, *Hukum Perlindungan Konsumen di Indonesia [Consumer Protection Law in Indonesia]* (PT Citra Aditya Bakti, 2010)

Simanjuntak, P N H, *Pokok-Pokok Hukum Perdata [The Civil Law Cores]* (Djambatan, 2009)

Smart Card Alliance, 'Fraud in the US Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud' (2009) <http://www.smartcardalliance.org/resources/lib/Fraud_EMV_Contactless_20091007.pdf>

Smith, Russell G and Peter Grabosky, 'Plastic Card Fraud' (Paper presented at the Conference Crime against Business, Melbourne, 1998)

Soeroso, R, *Pengantar Ilmu Hukum [Introduction to Law]* (Sinar Grafika, 2004)

Stallings, William and Lawrie Brown, *Computer Security: Principles and Practice* (Prentice Hall, 2nd ed, 2012)

Steennot, Reinhard, 'Allocation of Liability in Case of Fraudulent Use of an Electronic Payment Instrument: The New Directive on Payment Services in the Internal Market' (2008) 24(6) *Computer Law and Security Report* 555

Stewart, Pam and Anita Stuhmcke, *Australian Principles of Tort Law* (Federation Press, 2nd ed, 2009)

- Storer, Charles, 'Global Cash Management and Security' in Brian Welch (ed), *Electronic Banking and Treasury Security* (Woodhead Publishing 1999)
- Subekti, R, *Hukum Pembuktian [The Law of Evidence]* (PT Pradnya Paramita, 2005)
- Sukarmi, *Cyberlaw, Kontrak Elektronik Dalam Bayang-Bayang Pelaku Usaha [Electronic Contract Within Business Business actorship]* (Pustaka Sutra, 2008)
- Sullivan, Richard J, *The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States* (Federal Reserve Bank of Kansas City, 2009)
- Sullivan, Richard J, 'Can Smart Cards Reduce Payments Fraud and Identity Theft?' (2008) 93 *Economic Review (Kansas City)* 35
- Sullivan, Richard J, 'The Changing Nature of US Card Payment Fraud: Industry and Public Policy Options' (2010) 95 *Economic Review* 101
- Sullivan, Richard J, 'Risk Management and Nonbank Participation in the US Retail Payments System' (2008) 92 *Economic Review-Federal Reserve Bank of Kansas City* 5
- Summers, Bruce J, 'Fraud Containment' (2009) 33(1) *Economic Perspectives* 17
- Summers, Bruce J, 'The Payment System in a Market Economy' in Bruce J Summers (ed), *The Payment System: Design, Management, and Supervision* (International Monetary Fund, 1994)
- Sutantio, Retnowulan and Iskandar Oeripkartawinata, *Hukum Acara Perdata Dalam Teori dan Praktek [Civil Law Proceeding in Theory and Practice]* (CV Mandar Maju, 2009)
- Sutedi, Adrian, *Tanggung Jawab Produk Dalam Hukum Perlindungan Konsumen [Product Liability in Consumer Protection Law]* (Ghalia Indonesia, 2008)
- Symantec, 'Internet Security Threat Report : 2011 Trend' (www.symantec.com, 2012) <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf>
- Tan, Harry S K, 'E-Fraud: Current Trends and International Developments' (2002) 9 *Journal of Financial Crime* 347
- Tandjung, Zaky, Maurice Burke and Herbert Smith, 'Effective Dispute Resolution in Indonesia' (2006) July/August *AsiaLaw*
- Tedder, Krista, 'Now You See It, Now You Don't: A Review of Fraud Costs and Trends' (A First Data White Paper, First Data, 2009)
- Tim Buku Media Indonesia, Tim Penulis Universitas Islam Indonesia and Tim Buku Bank Indonesia, *Era Baru Transformasi Bank Sentral [New Era of Central Bank Transformation]* (Media Indonesia Publishing, 2010)

Tim Perizinan dan Informasi Sistem Pembayaran, Biro Pengembangan dan Kebijakan Sistem Pembayaran, Direktorat Akunting dan Sistem Pembayaran,, 'Laporan Sistem Pembayaran dan Pengedaran Uang 2010. "Arah dan Kebijakan Sistem Pembayaran dalam Menyongsong Era Integrasi Ekonomi serta Upaya Meningkatkan Kualitas Uang dan Keandalan Manajemen Pengelolaan Kas" [Payment System Annual Report 2010. "Payment System Direction and Policy in the Era of Economic Integration and Efforts to Improve the Quality and Reliability of Cash Management"]' (Bank Indonesia, 2010)

Tyree, Alan and Andrea Beatty, *The Law of Payment Systems* (Butterworths, 2000)

Tyree, Alan L, *Banking Law in Australia* (LexisNexis Butterworths, 4th ed, 2002)

Tyson, Richard, 'Counterfeit Card Fraud Soars in the UK' (2001) 13(4) *Card Technology Today* 2

United Nations Commission on International Trade Law (UNCITRAL), 'UNCITRAL Legal Guide on Electronic Funds Transfers' (United Nations, 1987)

United Nations Commission on International Trade Law (UNCITRAL), 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment' (United Nations 2001)

Veljanovski, Cento, *Economic Principles of Law* (Cambridge University Press, 2007)

Vickery, Roger and Wayne Pendleton, *Australian Business Law: Compliance and Practice* (Pearson Education Australia, 2009)

Vrîncianu, Marinela and Liana Anica Popa, 'Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests' (2010) *The AMFITEATRU Economic Journal* 388

Walsh, Nigel, 'ATM Fraud Prompts Card Rethink?' (2005) 17(2) *Card Technology Today* 10

Watt, Robert, *Concise Legal Research* (Federation Press, 4th ed, 2001)

Weerasooria, W S, *Banking Law and the Financial System in Australia* (Butterworths, 5th ed, 2000)

Widiyono, Try, *Aspek Hukum Operasional Transaksi Produk Perbankan di Indonesia [Legal Aspect of Operational Transaction Banking Products in Indonesia]* (Ghalia Indonesia, 2006)

Williams, Phil, 'Organized Crime and Cybercrime: Synergies, Trends, and Responses' (2001) <<http://www.crime-research.org/library/Cybercrime.htm>>

Winarta, Frans H, 'Legal Consistency in Indonesia: What Justice is All About' in Thang D Nguyen (ed), *The Indonesian Dream: Unity, Diversity and Democracy in Times of Distrust* (Marshall Cavendish, 2004)

Zhang, Jie et al, 'Improving Multiple-Password Recall: An Empirical Study' (2009) 18(2) *European Journal of Information Systems*

Zulham, *Hukum Perlindungan Konsumen [Consumer Protection Law]* (Kencana, 2013)

Case Law

Australian Safeway Stores Pty Ltd v Zaluzna (1986) 162 CLR 479

Cook v Cook (1986) CLR 376

Donoghue v Stevenson [1932] AC 562

Goldman v Hargrave (1967) 1 AC 645

Kosciusko Thredbo Pty Ltd v Smith (2001) NSWCA 355

Overseas Tankship (UK) Ltd v Miller Steamship Co. Pty (1967) AC 617 (PC)

Overseas Tankship (UK) Ltd v Morts Dock & Engineering Co (1961) AC 388

Tuan Bahari v PT Bank Negara Indonesia (Persero) Tbk [Supreme Court of Republic of Indonesia], 718 K/Pdt.Sus/2008, 10 December 2008.

Wynbergen v Hoyts Corporation Pty Ltd (1997) 149 ALR 25

Legislation

Civil Liability Act 2002 (NSW)

Electronic Funds Transfer Act of 1978 (EFTA), 15 USC 1693

Kitab Undang-Undang Hukum Perdata [Civil Code]

Undang-Undang Dasar Republik Indonesia 1945 [Constitution of the Republic of Indonesia 1945]

Undang-Undang Nomor 11 Tahun 1953 Tentang Undang-Undang Pokok Bank Indonesia [Law Number 11 of 1953 on Bank Indonesia Core Act] (Indonesia)

Undang-Undang Nomor 13 Tahun 1968 Tentang Bank Sentral [Law No 13 of 1968 on Bank Sentral] (Indonesia)

Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan [Law No 21 of 2011 on Financial Service Authority] (Indonesia)

Undang-Undang Republik Indonesia Nomor 3 Tahun 2011 Tentang Transfer Dana [Law No. 3 of 2011 on Fund Transfer] (Indonesia) ('LFT')

Undang-undang Republik Indonesia Nomor 7 Tahun 1992 Tentang Perbankan Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 10 Tahun 1998 [Law No 7 of 1992 on Banking as Amended by Law No 10 of 1998] (Indonesia) ('LB')

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen [Law No 8 of 1999 on Consumer Protection] (Indonesia) ('LCP')

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik [Law No 11 of 2008 on Electronic Information and Transactions] (Indonesia) ('LIET')

Undang-Undang Republik Indonesia Nomor 12 Tahun 2011 Tentang Pembentukan Peraturan Perundang-Undangan [Law of Republic of Indonesia Number 12 of 2011 on Making Regulations] ('LMR')

Undang-Undang Republik Indonesia Nomor 23 Tahun 1999 Tentang Bank Indonesia Sebagaimana Telah Diubah Terakhir Dengan Undang-Undang Republik Indonesia Nomor 6 Tahun 2009 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2008 Tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 1999 Tentang Bank Indonesia Menjadi Undang-Undang [Law No. 23 of 2009 on Bank Indonesia as latest amended by Law No. 6 of 2009 on Stipulation of Government Regulation in Lieu of Law No. 2 of 2008 on Second Amendment to the Law No. 23 of 1999 on Bank Indonesia Into Act] (Indonesia) ('LBI')

Undang-Undang Republik Indonesia Nomor 30 Tahun 1999 Tentang Arbitrase dan Alternatif Penyelesaian Sengketa [Law of Republic of Indonesia No 30 of 1999 on Arbitration and Alternative Disputes Resolution] (Indonesia)

Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman [Law Number 48 of 2009 on Judicial Power]

Undang-Undang Darurat Nomor 1 Tahun 1951 Tentang Tindakan-Tindakan Sementara Untuk Menyelenggarakan Kesatuan Susunan Kekuasaan dan Acara Pengadilan-Pengadilan Sipil [Emergency Law Number 1 of 1951 on Temporary Actions to Perform the Unity of Ordinary Courts' Jurisdiction Power and Proceeding]

Other Sources

Abidin, Zainal, *Menelisik Pembahasan RUU KUHP [Investigating the Criminal Code Bill Process]* <<https://docs.google.com/document/d/1.../edit?usp=sharing>>

Aditiasari, Dana, *Bank Mandiri Akan Ganti Seluruh Dana Nasabah yang Dibobol [Mandiri Bank to Make Restitution for All Consumer Funds Which had been Robbed]* (3 September 2014) Detik.com <<http://finance.detik.com/read/2014/06/03/134152/2598382/5/bank-mandiri-akan-ganti-seluruh-dana-nasabah-yang-dibobol?f990101mainnews>>

Administrator, *Thursday Thinkpiece: Mason on Digital Signatures* (August 22 2013) Slaw Canada's Online Legal Magazine <<http://www.slaw.ca/2013/08/22/thursday-thinkpiece-mason-on-digital-signatures/>>

American Bankers Association (ABA), *Security in Electronic Banking* (2010) <http://www.aba.com/Issues/Issues_SecurityElectronic.htm>

American Bankers Association (ABA), *Security in Electronic Banking* (2012) <http://www.aba.com/Issues/Index/Pages/Issues_SecurityElectronic.aspx>

Arnold, Kylene, *Parts of an Automatic Teller Machine* (2013) eHow Money <http://www.ehow.com/info_8322362_parts-automatic-teller-machine.html>

Australian Law Reform Commission (2015) Australian Government <<http://www.alrc.gov.au/>>

Australian Crime Commission, *Banks, Law Enforcement and Retailers Warn Merchants to Secure EFTPOS terminals to Prevent Skimming* (2010) <<http://www.crimecommission.gov.au/media/banks-law-enforcement-and-retailers-warn-merchants-to-secure-eftpos-terminals-to-prevent-skimm>>

Australian Crime Commission, *Card Fraud* (2011) <<http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/card-fraud>>

Australian Payments Clearing Association, *Regulations for Consumer Electronic Clearing System (CS3)* (2012) <http://www.apca.com.au/docs/payment-systems/cecs_regulations.pdf>

Australian Securities & Investments Commission (ASIC), *ePayments Code* (29 January 2014) <<http://www.asic.gov.au/epaymentscode>>

Azhari, H M, *Perlindungan Hukum Bagi Nasabah Perbankan Syariah [Legal Protection For Sharia Banking Consumer]* (2009) <<http://www.patanahgrogot.net/utama/images/stories/pdf/artikelazhari.pdf>>

Aziz, Zeti Akhtar, *Electronic Payment in Malaysia* (2003) Bank for International Settlement, <<http://www.bis.org/review/r030516e.pdf>>

Baker & McKenzie, *Dispute Resolution Around the World: Indonesia* (2010) Baker & McKenzie <http://www.bakermckenzie.com/files/Uploads/Documents/Global%20Dispute%20Resolution/Dispute%20Resolution%20Around%20the%20World/dratw_indonesia_2009.pdf>

Bank Indonesia, *API's Six Pillars (Enam Pilar API)* (2010) <http://www.bi.go.id/NR/rdonlyres/2502404A-6622-46A4-9030-00CF3FC86A7A/1378/enam_pilar.pdf>

Bank Diminta Perbaiki Sistem Pengamanan [Banks Asked to Improve Its Security System] (23 January 2010) Hukumonline.com
<<http://www.hukumonline.com/berita/baca/lt4b5a35f0f1afb/bank-diminta-perbaiki-sistem-pengamanan>>

Bobol Data ATM, Dua Kasir Mall Ditangkap [ATM Data Theft, Two Mall Cashiers Busted] (24 November 2011) Beritadewata.com
<http://beritadewata.com/Hukum_dan_Kriminal/Kriminal/Bobol_Data_ATM,_Dua_Kasir_Mall_Ditangkap.html>

Bell, Claes, *4 Places Where You Don't Want To Swipe Your Debit Card*, *Business Insider* (4 January 2012) <http://articles.businessinsider.com/2012-01-04/news/30587769_1_debit-card-card-terminals-skimmers>

Bennett-Smith, Meredith, 'Safest ATM PINs: Analysis Reveals Four-Digit Combinations Almost No One Is Using', *The Huffington Post* (online), 20 September 2012 <http://www.huffingtonpost.com/2012/09/20/the-worlds-safest-atm-pin-four-digit-combination_n_1901430.html>

BusinessDictionary.com, *Tort Liability* (2013) www.businessdictionary.com
<<http://www.businessdictionary.com/definition/tort-liability.html>>

Carl, Michael and Dewi Savitri Reni, *A Guide to Dispute Resolution in Indonesia: Litigation Process* (30 September 2011) SSEK Indonesian Legal Consultant
<<http://blog.ssek.com/index.php/2011/09/a-guide-to-indonesian-dispute-resolution-litigation-process/>>

Commonwealth Bank, *EFTPOS Skimming* (2013)
<<http://www.commbank.com.au/business/merchant-services/other-services/protecting-you-and-your-customers.html#EFTPOS>>

Consumer International, *In Search of Good Practices in Financial Consumer Protection* (12 July 2013) Consumer International, <<http://www.consumersinternational.org/news-and-media/resource-zone/in-search-of-good-practices-in-financial-consumer-protection/#.UkPxuT-tPSg>>

ConsumerReports.org, *Debit-Card 'Skimming' Scams* (16 January 2010) Media Indonesia Online <<http://www.indonesiamedia.com/2010/01/16/debit-card-skimming-scams/>>

CUTS International, *Consumer Rights and Its Expansion: Rights and Responsibilities* (1999) CUTS Centre for Consumer Action Research and Training (CART)
<<http://www.cuts-international.org/consumer-rights.htm>>

Cvrcek, Dan, Jan Krhovjak and Vashek Matyas, 'PIN (and Chip) or Signature: Beating the Cheating?' (Paper presented at the Security Protocols, Cambridge, UK, 2005)

Damanik, Caroline, Mahal, *Realisasi "Magnetic" ke "Chip" Pelan-Pelan [Expensive, the Realisation from "Magnetic" to "Chip" Slowly]* (2010) Kompas.com

<<http://megapolitan.kompas.com/read/2010/01/23/09164112/Mahal.Realisasi.Magnetic.ke.Chip.Pelan-pelan>>

Daniel, Ramson, *Low Security Kartu ATM Mandiri [Low Security of Mandiri's ATM]* (22 March 2012) Myzone: Ruang Jurnalisme Anda <<http://myzone.okezone.com/content/read/2012/03/22/6883/low-security-kartu-atm-mandiri>>

Daniel, Wahyu, *ATM Sejumlah Nasabah Diblokir, Ini Penjelasan Bank Mandiri [Numbers of Consumer's ATM Blocked, this is Bank Mandiri's Explanation]* (13 May 2014) detik.com <<http://finance.detik.com/read/2014/05/12/205424/2580730/5/atm-sejumlah-nasabah-diblokir-ini-penjelasan-bank-mandiri>>

Diaz, Jesus, *This ATM Keyboard Will Steal Your Card PIN and You Will Never Notice It* (5 January 2011) Gizmodo <<http://gizmodo.com/5725859/this-is-how-cyber+criminals-steal-your-money>>

Diebold Incorporated, *Playing Defense: Trends in ATM Attacks* (2007) <http://www.diebold.com/atmsecurity/files/DBD_WhitePaper_Island.pdf>

Diebold Incorporated, *White Paper: Battling Card Fraud through Chip and PIN Technology* (2011)

Drimer, Saar, Steven J Murdoch and Ross Anderson, 'Thinking inside the Box: System-Level Failures of Tamper Proofing' (Paper presented at the IEEE Symposium on Security and Privacy, Oakland, CA, 2008) <http://ieeexplore.ieee.org.ezproxy.uow.edu.au/xpls/abs_all.jsp?arnumber=4531159&tag=1>

Duffy, Peter, 'CITY LORE; Willie Sutton, Urbane Scoundrel', *The New York Times* (online), 17 February 2002 <<http://www.nytimes.com/2002/02/17/nyregion/city-lore-willie-sutton-urbane-scoundrel.html>>

e-lawresources.co.uk, *Contributory Negligence* (e-lawresources.co.uk <<http://www.e-lawresources.co.uk/Contributory-negligence.php>>

Empat Pembobol ATM Diadili [Four ATM Thieves Prosecuted] (27 Agustus 2012) Natanews: Dimensi Baru Informasi <<http://www.natanews.com/521/empat-pembobol-atm-diadili/>>

Fajri, Hidayatul, 'Kasir Restoran Bobol ATM, Rp 123 Juta Raib [Cashiers Restaurant Stole ATM, Rp123 Million Drained]', *Kompas* (online), 8 May 2012 <<http://megapolitan.kompas.com/read/2012/05/08/17564064/Kasir.Restoran.Bobol.ATM..Rp.123.Juta.Raib>>

Far, *Uang Rp76 Juta Raib di Bank Mandiri [Rp76 Million Disappears from Bank Mandiri]* (14 May 2013) SumutPos <<http://sumutpos.co/2013/05/58129/uang-rp76-juta-raib-di-bank-mandiri>>

Financial Fraud Action UK, *Fraud The Fact 2012: The Definitive Overview of Payment Industry Fraud and Measures to Prevent It* (2012) <<http://www.financialfraudaction.org.uk/downloads.asp?genre=facts%20and%20figures>>

Flaherty, Mary Pat, 'Bank Expert Discusses ATM Skimming - and how to detect it', *The Washington Post* (online), 6 April 2010 <<http://voices.washingtonpost.com/crime-scene/alexandria/atm-skimming-how-would-you-know.html>>

Group, Skynet Media, *Teknik & Modus Card Trapping [Technique and Modus of Card Trapping]* (2011) Mafia Kartu Kredit <<http://www.mafiakartukredit.com/2012/03/teknik-modus-card-trapping.html>>

Harnay, Sophie and Alain Marciano, 'Posner, Economics and the Law: From "Law and Economics" to an Economic Analysis of Law' (2009) 31(2) *Journal of the History of Economic Thought* 215

Haryanto, Andri, *Wartawan 'KPK' Terlibat Pembobolan ATM Diringkus Polisi ['KPK' Journalist Involved in ATM Theft, Apprehended by Police]* (24 April 2013) Detik.com

Hassanah, Hetty, *Tinjauan Hukum Mengenai Perbuatan Melawan Hukum Dalam Transaksi Jual Beli Melalui Internet (E-Commerce) Dihubungkan Dengan Buku III KUH Perdata [Tort Law Review on E-Commerce in Connection to Section III Indonesia Civil Code]* (2006) 9 <http://www.google.com.au/search?sourceid=navclient&ie=UTF-8&rlz=1T4ADFA_enAU349AU349&q=Tinjauan+hukum+mengenai+perbuatan+melawan+hukum+dalam+transaksi+jual+beli+melalui+internet>

Heriani, Fitri Novia, *BI Fokus Mediasi Kasus Perbankan [BI Focus on Mediation for Banking Cases]* (4 April 2012) Hukumonline.com <<http://www.hukumonline.com/printedoc/lt4f7c3e18704f3>>

Hill, Gerald and Kathleen Hill, *Liability* (13 February 2013) Fine Communications <<http://dictionary.law.com/Default.aspx?selected=1151>>

How ATM Machines Work (2013) eHow tech <http://www.ehow.com/how-does_4564295_do-atm-machines-work_.html>

Hutasoit, Moksa, *Awas, Penipuan Lewat ATM Marak di Depok! [Beware, Many ATM frauds in Depok!]* (19 June 2010) Detik.com <<http://news.detik.com/read/2010/06/19/180214/1381958/10/awas-penipuan-lewat-atm-marak-di-depok?nd992203605>>

Indonesia, Bank, *Ikhtisar Undang-Undang No. 23 Tahun 1999 Tentang Bank Indonesia [Excerpt of Law of 1999 on Bank Indonesia] (Indonesia)* (2008) Bank Indonesia <<http://www.bi.go.id/NR/rdonlyres/C7402D01-A030-454A-BC75-9858774DF852/13303/ikhtisar.pdf>>

Institute for Legal Reform (2014) U.S. Chamber of Commerce <<http://www.instituteforlegalreform.com/>>

- INTERPOL, *Payment Cards* (2010)
<<http://www.interpol.int/Public/CreditCards/Default.asp>>
- Investopedia, *Dictionary: Brick and Mortar* (2012)
<<http://www.investopedia.com/terms/b/brickandmortar.asp#ixzz1aJkP6Zm9>>
- InvestorWords, *Contractual Liability* (2013) www.investorwords.com
<http://www.investorwords.com/19034/contractual_liability.html>
- Janssen, Cory, *Brute Force Attack* (2013) technopedia
<<http://www.techopedia.com/definition/18091/brute-force-attack>>
- Johnson, Nicholas J, *Lebanese Loops* (2013) Australia's Honest Con Man: Encyclopedia of Scams <<http://scams.wikispaces.com/Lebanese+Loops>>
- Julita, *Difference between Customer and Consumer* (12 January 2011)
DifferenceBetween.net <<http://www.differencebetween.net/language/difference-between-customer-and-consumer/>>
- Kertapati, Didi Tri, *Pembobolan Dana Nasabah: Pelaku Diduga Masuk Sindikat Internasional [Consumers' Fund Theft: Alleged Perpetrators' Suspected as a Member of International Syndicate]* (26 January 2010) Detik.com <<http://news.detik.com/read/2010/01/26/173650/1286539/10/pelaku-diduga-masuk-sindikata-internasional>>
- Kejahatan Card Trapping Memacetkan Mesin ATM Untuk Menguras Uang ATM (Warning) [Card Trapping Crime Jammed ATM Machine to Drain ATM Cash (Warning)]* (15 October 2012) Direktorat Reserse Kriminal Umum, Polda Metropolitan Jakarta Raya, <<http://reskrimum.metro.polri.go.id/read/article/8203/19/Kejahatan-Card-Trapping-Memacetkan-Mesin-ATM-Untuk-Menguras-Uang-ATM-Warning>>
- Khafifah, Nur, *Banyak Suap, Kinerja Lembaga Peradilan Masih Mengecewakan [Many Bribes, the Performance of the Judiciary is Still Disappointing]* (2013) detik.com <<http://news.detik.com/read/2013/04/09/130408/2215371/10/banyak-suap-kinerja-lembaga-peradilan-masih-mengecewakan?9911012>>
- Kirk, Jeremy, *ATM Malware Spreading Around the World* (2009)
<http://www.cio.com/article/494341/ATM_Malware_Spreading_Around_the_World>
- Kirk, Jeremy, *Criminals Turn to 'Card-Trapping' at ATM Machines to Get Cash* (19 October 2011) CIO <http://www.cio.com.au/article/404671/criminals_turn_card-trapping_atm_machines_get_cash/>
- Kirk, Jeremy, *Fraudsters Find Holes in Debit Card Fraud Detection* (2010) Computerworld
<http://www.computerworld.com/s/article/9193378/Fraudsters_find_holes_in_debit_card_fraud_detection?taxonomyId=17&pageNumber=1>
- Kitten, Tracy, *3 Reasons Skimmers Are Winning* (10 May 2012) Bank Info Security
<<http://www.bankinfosecurity.com/3-reasons-skimmers-are-winning-a-4752/op-1>>

Kitten, Tracy, *3 Tips to Foil POS Attacks* (2011) Bank Info Security
<<http://www.bankinfosecurity.com/3-tips-to-foil-pos-attacks-a-3617>>

Kitten, Tracy, *ATM Skimming Threats Evolve* (5 May 2011) Bank Info Security
<http://www.bankinfosecurity.com/articles.php?art_id=3612&rf=2011-05-06-eb>

Kitten, Tracy, *Enhanced Malware Targets Retailers: Stored Card Data on Networks, POS Systems Primary Target* (2013) Bank Info Security
<<http://www.bankinfosecurity.com/enhanced-malware-targets-retailers-a-5604?rf=2013-03-13-eb&elq=fef6911eb340477d8853befa86ada91c&elqCampaignId=6124>>

Kitten, Tracy, *Grocer Confirms POS Skimming Attack: Customers, Card Issuers Watch for Fraudulent Activity* (4 January 2012) Bank Info Security
<http://www.bankinfosecurity.com/articles.php?art_id=4376&rf=2012-01-04-eb&elq=6f859884d23941cab391ff197d886b3c&elqCampaignId=1109>

Kitten, Tracy, *Heartland Breach: Legal Update* (6 April 2011) Bank Info Security
<http://www.bankinfosecurity.com/articles.php?art_id=3510&rf=2011-04-07-eb>

Kitten, Tracy, *Illegal ATM Software to Blame for Most ATM Hacks, Solution Provider Says* (28 July 2009) ATM Marketplace
<<http://www.atmmarketplace.com/article/128364/Illegal-ATM-software-to-blame-for-most-ATM-hacks-solutions-provider-says>>

Kitten, Tracy, *Michaels Breach Bigger than Reported* (12 May 2011) Bank Info Security
<http://www.bankinfosecurity.com/articles.php?art_id=3628&rf=2011-05-14-eb>

Kitten, Tracy, *Michaels Breach: Who's Liable?* (22 May 2011) Bank Info Security
<<http://www.bankinfosecurity.com/michaels-breach-whos-liable-a-3668>>

Kitten, Tracy, *POS Fraud: How Hackers Strike* (14 December 2011) Bank Info Security
<http://www.bankinfosecurity.com/articles.php?art_id=4324&rf=2011-12-14-eb&elq=d0d8cc583b6b4e5b868f84ef253808b6&elqCampaignId=977>

Kitten, Tracy, *POS Skimming Scam Stopped* (2 May 2011) Bank Info Security
<<http://www.bankinfosecurity.com/pos-skimming-scam-stopped-a-3592>>

Koubaridis, Andrew, 'EFTPOS Skimmers: 4 Arrests in Scam', *New Zealand Herald* (online), 10 April 2012
<http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10797766>

Krebs, Brian, *ATM Skimmers, Part II* (2 February 2010) www.krebsonsecurity.com
<<http://krebsonsecurity.com/2010/02/atm-skimmers-part-ii/>>

Krebs, Brian, *Beware Card - and Cash Trapping at the ATM* (20 November 2012)
<<http://krebsonsecurity.com/tag/card-trap/>>

Krebs, Brian, *Cyber Crooks Leave Traditional Bank Robbers in the Dust* (13 March 2010) <<http://krebsonsecurity.com/2010/03/cyber-crooks-leave-bank-robbers-in-the-dust/>>

Krebs, Brian, *Green Skimmers Skimming Green* (2011) <<http://krebsonsecurity.com/2011/03/green-skimmers-skimming-green/>>

Krebs, Brian, *Pro Grade (3D Printer-Made?) ATM Skimmer* (2011) <https://krebsonsecurity.com/2011/12/pro-grade-3d-printer-made-atm-skimmer/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+KrebsOnSecurity+%28Krebs+on+Security%29>

Krebs, Brian, *Would You Have Spotted the Fraud?* (15 January 2010) www.krebsonsecurity.com <<http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/>>

Legal Information Institute, *Res Ipsa Loquitur* (<http://www.law.cornell.edu/wex/res_ipsa_loquitur>

Lema, Ansy, *Perlindungan Terhadap Nasabah Bank Masih Lemah [Banks Consumer Protection Still Weak]* (15 February 2010) *Perspektif Baru* <<http://www.perspektifbaru.com/wawancara/725>>

Lindsey, Tim, *Indonesia Trial Process and Legal System: Background Notes* (2009) Melbourne Law School - Asian Law Centre <http://alc.law.unimelb.edu.au/files/indo_trial_process.pdf>

Lormel, Dennis, 'Terrorism and Credit Card Information Theft: Connecting the Dots' (2008) <http://www.ipsaintl.com/2008_2/September-2008_3.html>

Maftuhah, Gina Nur, *Pencurian Data Body Shop Terjadi di Jakarta & Padang [Body Shop Data Theft Happened in Jakarta & Padang]* (25 March 2013) Okezone.com <<http://economy.okezone.com/read/2013/03/25/457/780852/pencurian-data-body-shop-terjadi-di-jakarta-padang>>

Maftuhah, Gina Nur, *Salahi Aturan, Pencurian Data di Body Shop Langsung di Stop [Violates the Rules, Data Theft in the Body Shop was Stopped Immediately]* (25 March 2013) Okezone.com <<http://economy.okezone.com/read/2013/03/25/457/780892/salahi-aturan-pencurian-data-di-body-shop-langsung-di-stop>>

Malakedsuwan, Pattama and Kenneth J Stevens, 'A Model of E-Fraud' (Paper presented at the 7th Pacific Asia Conference on Information Systems, Adelaide, 2003)

MasterCard, *MasterCard Zero Liability* (2012) <<http://www.mastercard.com.au/zero-liability.html>>

McGlasson, Linda, *Top 4 Skimming Threats: From Hand-Held POS Devices to Dummy ATMs* (2010) Bank Info Security <<http://www.bankinfosecurity.com/top-4-skimming-threats-a-3054>>

Mercator Advisory Group, *Credit Card Fraud Update: Silos Versus The Balloon Effect* (2007)

<http://www.mercatoradvisorygroup.com/index.php?doc=credit&action=view_item&id=171&catid=3>

Mini00 DX4 Portable Magnetic Stripe Swipe PVC Card Reader (23 February 2013)

ebay <http://www.ebay.com.au/itm/Mini00-DX4-Portable-Magnetic-Stripe-Swipe-PVC-Card-Reader-/251003524960?pt=AU_CashRegisterAccessories&hash=item3a70f9d760>

MSCR710 (MyCardReader.com <<http://mycardreader.com/18-mscr710.html>>

Muhamad, Karnoto, '*Adu Pelayanan di Tengah Ancaman* [Service Competition in the Middle of Threat]', *Infobank* May 2013

MVT/Yoz, *BPSK Enggan Putusannya Diuji Pengadilan* [*BPSK Reluctant its Decision Being Review by Court*] (26 April 2011)

<<http://hukumonline.com/berita/baca/lt4db6805fb81c8/bpsk-enggan-putusannya-diuji-pengadilan>>

Napi Asal Malaysia Otak Pembobol ATM [Recidivist From Malaysia Became Mastermind of ATM Theft]', *Kompas* (online), 19 September 2008

<<http://health.kompas.com/read/2008/09/19/03593524/Napi.Asal.Malaysia.Otak.Pembobol.ATM>>

Nasution, AZ, *Aspek Hukum Perlindungan Konsumen: Tinjauan Singkat UU Nomor 8 Tahun 1999-L.N. 1999 No 42* [*Consumer Protection Legal Aspect: Brief Analysis Law Number 8 of 1999*] (2010) Masyarakat Pemantau Peradilan Indonesia 12

<http://www.pemantauperadilan.com/index.php?option=com_content&task=view&id=121&Itemid=12>

NCR, *Is ATM Security a Challenge in Kenya and All Over the World?* (2011)

<http://aitec.usp.net/Banking%20&%20Mobile%20Money%20COMESA,%202-3%20March%202011,%20Nairobi/TopDare_NCR_BankingMobileMoneyCOMESA2-3Mar2011.pdf>

Nisaputra, Rezkiana, *Visa Siap Amankan Transaksi Kartu Kredit di Indonesia* [*Visa Ready to Safeguard Credit Card Transactions in Indonesia*] (24 May 2013)

Okezone.com <<http://economy.okezone.com/read/2013/04/03/457/785755/visa-siap-amankan-transaksi-kartu-kredit-di-indonesia>>

Niven, David, 'Comments on Institutions' Dispute Resolution Procedures and the Ombudsman Proposal' (Paper presented at the Electronic Funds Transfer: Trade Practices Commission Workshop, Melbourne, 1989)

OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (16 September 2000) OECD

<<http://www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm>>

Olga Kharif and Bianca Vázquez Toness, *Why US Retailers Are Still Vulnerable to Card Fraud* Bloomberg Business, 10 April 2014
<<http://www.bloomberg.com/bw/articles/2014-04-10/u-dot-s-dot-retailers-behind-schedule-for-card-payment-system-upgrade>>

Oracle Corporation, *US Card Fraud* (2010) Bank Gateway.com <<http://www.banking-gateway.com/microsites/oracle/US%20Card%20Fraud.pdf>>

Organisation for Economic Co-operation and Development (OECD), *G20 High-Level Principles on Financial Consumer Protection* (16 September 2012 2011) OECD
<www.oecd.org/daf/fin/financial-markets/48892010.pdf>

Organisation for Economic Co-operation and Development (OECD), *OECD Recommendation on Consumer Dispute Resolution and Redress* (12 July 2007) OECD
<<http://www.oecd.org/sti/consumer/38960101.pdf>>

Pangabeau, Edward, *Modus yang Dipakai si Pembobol Kartu Kredit di Gerai Body Shop [Modus Operandi Employed by Credit Card Theft Perpetrator in Body Shop Merchant]* (31 May 2013) Liputan6.com
<<http://bisnis.liputan6.com/read/601128/modus-yang-dipakai-si-pembobol-kartu-kredit-di-gerai-body-shop>>

Pembobol ATM Asal Srilanka Dicidaduk [ATM Thief from Sri Lanka Apprehended] (24 June 2012) Kompas.com
<<http://lipsus.kompas.com/topikpilihanlist/2133/1/100.hari.jokowi-basuki/read/xml/2008/06/24/11101760/Pembobol.ATM.Asal.Sri.Lanka.Dicidaduk>>

Pembobolan ATM: BI Instruksikan Bank Evaluasi System IT [ATM Theft: BI Instructs Banks to Evaluate Their IT System] (2010) Indosiar.com
<http://www.indosiar.com/fokus/bi-instruksikan-bank-evaluasi-sistem-it_84020.html>

'*Penegakan Hukum: Separuh Lebih Responden Tak Puas [Law Enforcement: More than Half of Respondents are not Satisfied]*', *Kompas* 8 April 2013, 2

Penemuan Hukum [Legal Discovery] (10 April 2010)
<<http://wonkdermayu.wordpress.com/kuliah-hukum/penemuan-hukum-atau-rechtsvinding/>>

Peraturan Bank Indonesia Nomor 6/30/PBI/2004 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan kartu [Bank Indonesia Regulation Number 6/30/2004 Concerning Operation of Card-Based Payment Instrument Activities]

Peraturan Bank Indonesia Nomor 16/1/PBI/2014 Tentang Perlindungan Konsumen Jasa Sistem Pembayaran [Bank Indonesia Regulation Number 16/1/PBI/2014 Concerning Consumer Protection on Payment System Services]

Peraturan Bank Indonesia Nomor: 3/10/PBI/2001 Tentang Penerapan Prinsip Mengenal Nasabah [Bank Indonesia Regulation Number: 3/10/PBI/2001 Concerning Implementation of Know Your Customer Principles]

Peraturan Bank Indonesia Nomor: 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor 14/2/PBI/2012 Tentang Perubahan Atas Peraturan Bank Indonesia Nomor 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu [Bank Indonesia Regulation Number: 11/11/PBI/2009 Concerning Card Based Payment Instrument Activity as amended by Bank Indonesia Regulation Number 14/2/PBI/2012 Concerning Amendment of Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning Operation of Card-Based Payment Instrument Activities] (BIR-CBPI)

Peraturan Bank Indonesia Number 13/25/PBI/2011 Tentang Prinsip Kehati-hatian Bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain [Bank Indonesia Regulation Number 13/25/PBI/2011 Concerning Prudential Principle for Commercial Bank which Outsource Some Parts of Its Works to Other Party] ('BIR-Outsource to Other Party')

'Police Bust ATM Skimming Racket' *Jakarta Post*, 4 November 2015,
<<http://jakartaglobe.beritasatu.com/news/police-bust-atm-skimming-racket/>>

Polri Diakui Berhasil Ungkap Jaringan Pemalsuan Kartu Kredit Terbesar Dunia [Republic of Indonesia Police (Polri) Admitted has Success to Revealed World Biggest Credit Card Counterfeiting Network] (12 March 2008) Antara News.Com
<<http://www.antaranews.com/view/?i=1205297983&c=NAS&s=>>

Surat Edaran Bank Indonesia Nomor 13/28/DPNP Tanggal 9 Desember 2011 Perihal Penerapan Strategi Anti Fraud bagi Bank Umum [Bank Indonesia Circular Letter Dated 9 December 2011 Concerning Implementation of Anti-Fraud Strategi for Commercial Bank]

Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 Tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah [Bank Indonesia Regulation Number: 7/6/PBI/2005 Concerning Transparency of Banking Product Information and the Use of Bank Customers' Personal Data] ('BIR-TBPI&UBCPD')

Peraturan Bank Indonesia Nomor 8/4/PBI/2006 Tentang Pelaksanaan Good Corporate Governance Bagi Bank Umum sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor 8/14/PBI/2006 [Bank Indonesia Regulation Number 8/4/PBI/2006 Concerning Implementation of Good Corporate Governance for Commercial Bank as amended by Bank Indonesia Regulation Number 8/14/PBI/2006] ('BIR-GCG')

Peraturan Bank Indonesia Nomor: 7/7/PBI/2005 Tentang Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor: 10/10/PBI/2008 [Bank Indonesia Regulation Nomor: 7/7/PBI/2005 Concerning Resolution of Customer Complaints as amended by Bank Indonesia Regulation Number 10/10/PBI/2008] ('BIR RCC')

Peraturan Bank Indonesia Nomor: 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum [Bank Indonesia Regulation Number: 9/15/PBI/2007 Concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks] ('BIR-RMUITCBs')

Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik [Government Regulation of the Republic of Indonesia Number 82 of 2012 on Electronic System and Electronic Transaction] (Indonesia) ('GR-OEST')

Permana, Dian Ade, *Rekaman CCTV Gelap, Petugas Terjunkan TIM* [CCTV Record Dark, Law Enforcer Deploy Team] (20 March 2009) Wonogiripos.com <<http://www.wonogiripos.com/2009/jogjapolitan/kota-jogja/rekaman-cctv-gelap-petugas-terjunkan-tim-130451>>

PIN, 'Empat Pembobol ATM ditangkap: Polisi, Jangan Panik Jika Kartu ATM Tertelan' [Four ATM Thieves Busted: Police, Do Not Panic When ATM Card Get Swallowed]', *Kompas* 27 September 2013, 27

Post and Telecommunication Directorate, Informatic and Communication Department - Republic of Indonesia, *Penggunaan UU ITE Dalam Penanggulangan Aksi Pembobolan ATM Bank* [The Usage of IET Act to Overcome Banks' ATM Theft] (2010) <http://www.postel.go.id/update/id/baca_info.asp?id_info=1416>

PT Bank Permata (Persero) Tbk, 'Formulir Pembukaan Produk Terpadu [Integrated Product Opening Form]' (2012)

Purnomo, Herdaru, *BI: Pengguna ATM Tak Perlu Panik, Kerugian Ditanggung Bank* [BI: ATM Users do not Need to Panic, Banks Bear the Loss] (20 January 2010) Detik.com <<http://finance.detik.com/read/2010/01/20/181324/1282733/5/>>

Purnomo, Herdaru, *Duh! Pembobolan Transaksi Kartu Hampir Capai 16.000 Kasus* [Ouch! Payment Card Fraud Almost Reaches 16.000 Cases] (2 January 2012) detik.com <<http://finance.detik.com/read/2012/01/02/144723/1804731/5/duh-pembobolan-transaksi-kartu-hampir-capai-16000-kasus?f9911023>>

Purnomo, Herdaru, *Pembobolan Via Alat Pembayaran Kartu Sudah Capai Rp. 12 Miliar* [Payment Card Theft Damaged Reached Rp12 billion] (8 June 2011) Detik.com <<http://finance.detik.com/read/2011/06/08/080958/1655426/5/pembobolan-via-alat-pembayaran-kartu-sudah-capai-rp-12-miliar>>

Purnomo, Herdaru, *Perbankan Nasional Butuh Rp 2 Triliun Untuk Beralih ke Kartu Chip* [National Banks Need Rp2 Trillion to Switch to Chip Card] (2010) Detik.com <<http://finance.detik.com/read/2010/01/22/120138/1283899/5/perbankan-nasional-butuh-rp-2-triliun-untuk-beralih-ke-kartu-chip>>

Putri, Tri Artining, 'Sindiket Malaysia Pembobol ATM Dibekuk' [Malaysia's ATM Theft Syndicate is Apprehended]', *Koran Tempo* 4 March 2014

Sindiket Malaysia Pembobol ATM Dibekuk [Malaysia's ATM Theft Syndicate is Apprehended]', *Koran Tempo*, 4 March 2014,

Rachman, Anita and Emmy Fitri, *ATM Skimming Attacks Signal Bank Security Shortcomings* (22 January 2010) JakartaGlobe

<<http://www.thejakartaglobe.com/archive/atm-skimming-attacks-signal-bank-security-shortcomings/>>

Rajagukguk, Erman, *Perbuatan Melawan Hukum [Unlawful Act/Tort]* (2009) <<http://webcache.googleusercontent.com/search?q=cache:meNPWduRDH8J:www.ermanhukum.com/Makalah%2520ER%2520pdf/PERBUATAN%2520MELAWAN%2520HUKUM.pdf+&cd=1&hl=en&ct=clnk&gl=id&client=firefox-a>>

Ratnawati, Theresia Endang, *Pemberdayaan Hukum Untuk Mendukung Perkembangan Teknologi Dalam Transaksi Melalui Internet [Law Empowerment for Technology Development Support in Internet Transaction]* (Doctoral Degree Thesis, Diponegoro University, 2006)

REI et al, *Bank Harus Bayar Nasabah [Bank Has to Pay Consumer]* (22 January 2010) KOMPAS.COM (online) <<http://bisniskeuangan.kompas.com/read/2010/01/22/07010927/Bank.Harus.Bayar.Nasabah>>

Santosa, Mas Achmad, *Development of Alternative Dispute Resolution (ADR) in Indonesia* (2003) ASEAN Law Association (ALA) - Indonesia <http://www.aseanlawassociation.org/docs/w4_indo.pdf>

Septiyaning, Indah, *Dilengkapi Anti Skimmer, ATM Bank Mandiri Aman [Equipped with Anti Skimmer, Mandiri Bank is Secure]* (26 January 2010) Boyolalipos.com <<http://www.boyolalipos.com/2010/dilengkapi-anti-skimmer-atm-bank-mandiri-aman-12955>>

Setiaji, Stefanus Arief, *Kejahatan Bank: Pembobolan Kartu ATM Naik Pada 2012 [Banking Fraud: ATM Card Theft Increased in 2012]* (2013) Bisnis.com <<http://en.bisnis.com/articles/kejahatan-bank-pembobolan-kartu-atm-naik-pada-2012>>

Setiawan, Iwan, *Data Fraud Kartu Pembayaran Perbankan [Banking Payment Card Fraud Data]* (2007) Yahoo!Groups <<http://groups.yahoo.com/group/BI-Cyclist/message/235>>

Setiawan, Iwan, 'Pembobolan ATM Bank [Theft from Bank ATMs]', *Gatra* (Jakarta - Indonesia), 24 February 2010

Sharpe, Anna, 'The Legal Framework in Relation to EFT Contracts and Disputes, Including Onus of Proof, Bankers' Duty of Care and Evidentiary Problems, and the Adequacy/Effectiveness of the Law in Resolving EFT Disputes' (Paper presented at the Electronic Funds Transfer: Trade Practices Commission Workshop, Melbourne, 1989)

Siciliano, Robert, *Flash Attacks: Big Money for Payment Card Scammers* (2011) Infosec Island <<http://www.infosecisland.com/blogview/10006-Flash-Attacks-Big-Money-for-Payment-Card-Scammers.html>>

Sidel, Robin, 'Theft of Debit-Card Data from ATMS Soars: Thieves are stealing information to make counterfeit plastic', *Wall Street Journal*, 19 May 2015, <<http://www.wsj.com/articles/theft-of-debit-card-data-from-atms-soars-1432078912>>

Simamora, Orlina, 'Pembobolan Lewat ATM Mandiri [ATM Mandiri Theft]', *Kompas* (Jakarta), 20 November 2006

Simbolon, Hotman, 'Transaksi dengan Kartu Mandiri [Transaction with Mandiri Card]', *Kompas* (Jakarta), 13 December 2006

Siregar, Sarsin, *Evi Yulisnawati Minta Putusan BPSK Medan Direalisasikan [Evi Yulisnawaty Asked CDSB-Medan's Verdict to be Fulfilled]* (27 March 2013) MedanBisnis

<http://medanbisnisdaily.com/news/read/2013/03/27/20328/evi_yulisnawaty_minta_putusan_bpsk_medan_direalisasikan/#.Ux72UoXInxA>

Siregar, Sarsin, *Perlindungan Nasabah Jangan Sekedar Retorika [Consumer Protection Should Not be just Rhetoric]* (26 March 2013) MedanBisnis
<http://medanbisnisdaily.com/news/read/2013/03/26/20104/perlindungan_nasabah_jangan_sekadar_retorika/#.Ux70NoXInxA>

Suardana, Gede, *Kasir Mall di Bali Terlibat Jaringan Pembobol ATM [Mall Cashier in Bali Involved in ATM Fraudster's Network]* (24 September 2011) detiknews
<<http://news.detik.com/read/2011/11/24/172907/1775045/10/kasir-mall-di-bali-terlibat-jaringan-pembobol-atm>>

Suardana, Gede, *Pembobol ATM Diancam 15 Tahun Penjara [ATM Fraudsters Threatened 15 Years in Prison]* (23 June 2010) Detik.com
<<http://news.detik.com/read/2010/06/23/180654/1385062/10/pembobol-atm-diancam-15-tahun-penjara>>

Suardana, Gede, *Pembobolan Rekening Nasabah: Mesin Pembayaran BCA di Hard Rock Hotel Bali Diganti [Consumers' Account Theft: BCA EFTPOS Machine at Hard Rock Hotel Bali Replaced]* (2010) Detik.com
<<http://news.detik.com/read/2010/01/20/230403/1282860/10/mesin-pembayaran-bca-di-hard-rock-hotel-bali-diganti?nd771104bcj>>

Suardana, Gede, *POLDA Bali akui Kesulitan Ungkap Kasus Pembobolan ATM [Bali Local Police Department Admitted They Had Difficulties to Revealed ATM Theft Cases]* (1 February 2010) <<http://news.detik.com/read/2010/02/01/144856/1290356/10/polda-bali-akui-kesulitan-ungkap-kasus-pembobolan-atm>>

Suardana, Gede, *WN Malaysia Pembobol ATM di Kuta Dibekuk [Malaysian Citizen ATM Theft in Kuta was Arrested]* (2 August 2011) Detik.com
<<http://news.detik.com/read/2011/08/02/123639/1694686/10/wn-malaysia-pembobol-atm-di-kuta-dibekuk>>

Subagja, Indra, *Bank Mandiri: 4 Nasabah yang Lapor ke Polda Bukan Korban Skimming [Mandiri Bank: 4 Consumers That Report to Police Station were not Skimming Victim]* (25 January 2010) Detik.com
<<http://news.detik.com/read/2010/01/25/183554/1285861/10/bank-mandiri-4-nasabah-yang-lapor-ke-polda-bukan-korban-skimming>>

Subagja, Indra, *Tersangka Pembobol ATM itu Dibekuk Saat Bercinta di Hotel di Alam Sutera* [ATM Theft Suspect was Apprehended While Making Love in Alam Sutera Hotel] (25 June 2013) Detik.com

Surat Edaran Bank Indonesia No. 14/20/DNPN Perihal Prinsip Kehati-hatian bagi Bank Umum yang Melakukan Penyerahan Sebagian Pelaksanaan Pekerjaan Kepada Pihak Lain [Bank Indonesia Circular Letter No. 14/20/DPNP Concerning Prudential Principle for Commercial bank which Outsource Some Parts of Its Works to Other Party]

Surat Edaran Bank Indonesia No. 15/23/DASP Perihal Penyelenggaraan Transfer Dana [Bank Indonesia Circular Letter No. 15/23/DASP Concerning Fund Transfer Operation]

Surat Edaran Bank Indonesia Nomor 7/24/DPNP Perihal Penyelesaian Pengaduan Nasabah sebagaimana telah diubah dengan Surat Edaran Bank Indonesia Nomor 10/13/DPNP [Bank Indonesia Letter Number 7/24/DPNP Concerning Resolution of Customer Complaints as amended by Bank Indonesia Letter Number 10/13/DPNP]

Surat Edaran Bank Indonesia Nomor 7/25/DPNP Perihal Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah [Bank Indonesia Decree Number 7/25/DPNP Concerning Transparency of Bank Product Information and the Use of Bank Customers' Personal Data]

Surat Edaran Bank Indonesia Nomor 9/30/DPNP Perihal Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum [Bank Indonesia Decree Number 9/30/DPNP Concerning Risk Management in the Use of Information Technology by Commercial Banks] ('*BID-RMUITCB*')

Surat Edaran Bank Indonesia Nomor 11/10/DASP Perihal Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu sebagaimana telah diubah dengan Surat Edaran Bank Indonesia Nomor 14/17/DASP [Bank Indonesia Decree Number 11/10/DASP Concerning The Operation of Card-Based Payment Instrument Activities as Amended with Bank Indonesia Decree Number 14/17/DASP] ('*BID-CP & Security*')

Surat Edaran Bank Indonesia Nomor 14/23/DASP Perihal Perubahan Atas Surat Edaran Bank Indonesia Nomor 13/22/DASP perihal Implementasi Teknologi Chip dan Penggunaan Personal Identification Number pada Kartu ATM dan/atau Kartu Debet yang diterbitkan di Indonesia [Bank Indonesia Circular Letter Number 14/23/DASP Concerning Amendment of Bank Indonesia Circular Letter Number 13/22/DASP Concerning Implementation Chip Technology and the Use of Personal Identification Number on ATM and/or Debit Card Issued in Indonesia]

Tabalujan, Benny S, *The Indonesian Legal System: An Overview* (2 December 2002) LLRX.Com <<http://www.llrx.com/features/indonesia.htm>>

Tarigan, Mitra, *Sepertiga Kasus Skimming di Dunia Terjadi di Indonesia* [One Third of World Skimming Case Happened in Indonesia] (2 July 2015) Tempo.co <<http://nasional.tempo.co/read/news/2015/07/02/063680461/sepertiga-kasus-skimming-di-dunia-terjadi-di-indonesia>>

Telford, Pat and Peter Kulik, *Ten Immutable Laws of ATM Security* (2011) ATM Industry Association (ATMIA)
<<https://www.atmia.com/clientuploads/directory/whitepaper/TenImmutableLawsOfATMSecurity2011.pdf>>

Tertina, Martha and Rhama T W, '*Merchant Dilarang Double Swipe Kartu Pembayaran* [Store Prohibited Double Swipe Payment Cards]', *Koran Tempo* 15 April 2013, B2

Thertina, Martha and R R Ariyani, '*YLKI: Regulasi Kerahasiaan Data Pribadi Mendesak* [YLKI: Privacy Regulation is Urgent]', *Koran Tempo* 5 April 2013, B2

Thieves Create More Sophisticated ATM Card Skimmers (27 April 2012) Mashable
<http://www.youtube.com/watch?v=_2H-_zAudn8>

Trustwave, *Automated Teller Machine (ATM) Malware Analysis Briefing* (28 May 2009) www.wired.com
<http://www.wired.com/images_blogs/threatlevel/2009/06/trustwave-security-alert-atm-malware-analysis-briefing.pdf>

Tyree, Alan L, *E-Commerce and Retail Banking* (2000)
<<http://www2.austlii.edu.au/~alan/bla-2000.html>>

United Nations Commission on International Trade Law (UNCITRAL), '*UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*' (United Nations, 1996)

Visa, *Counterfeit Fraud* (2010)
<http://www.visa.ca/en/personal/pdfs/counterfeit_fraud.pdf>

Visa, *Zero Liability* (2011)
<http://usa.visa.com/personal/security/visa_security_program/zero_liability.html?it%B Ccj/personal/security/visa_security_program/index.htmljZero%20Liability*>

Waspada Kejahatan di ATM [Beware on Crime at the ATM] (15 July 2012) *Harian Terbit* <<http://www.harianterbit.com/2012/07/15/waspada-kejahatan-di-atm/>>

White, Paul, *The Regulation of Electronic Funds Transfer in Australia: An Integrated Multidisciplinary Approach* (DBA Thesis, Victoria University, 2007)

Wulan, Wahyu Satriani Ari, '*BCA Blokir Penarikan dari Toronto dan Australia* [BCA Blocked Withdrawal from Toronto and Australia]', *Kompas* (online), 26 January 2010
<<http://news.detik.com/read/2010/01/26/173650/1286539/10/pelaku-diduga-masuk-sindikatan-internasional>>

Wulan, Wahyu Satriani Ari, '*Inilah Ciri ATM Anti-'Skimming'* [This is Typical ATM Anti-'Skimming']', *Kompas* (online), 22 January 2010
<<http://nasional.kompas.com/read/2010/01/22/12220871/Inilah.Ciri.ATM.Antiskimming>>

Zetter, Kim, *New ATM Malware Captures PINs and Cash-Updated* (6 April 2009)
www.wired.com <<http://www.wired.com/threatlevel/2009/06/new-atm-malware-captures-pins-and-cash>>

Zuhdi, Lukman Hakim, '*Pembobolan ATM, Salah Siapa?* [ATM Theft, Who is at Fault?]', *Tabloid INDONESIA MONITOR* 27 January - 2 February 2010

APPENDICES

University of Wollongong



INITIAL APPLICATION APPROVAL

In reply please quote: HE12/151

Further Enquiries Phone: 4221 3386

KC:CJ

4 May 2012

Mr Iwan Setiawan

Dear Mr Setiawan

Thank you for your response dated 30 April 2012 to the HREC review of the application detailed below. I am pleased to advise that the application has been **approved**.

Ethics Number: HE12/151

Project Title: Regulation of Unauthorised Electronic Funds Transfer (EFT) and Consumer Protection in Indonesia: A critical analysis of law and practice

Researchers: Mr Iwan Setiawan, Professor Andrew Goldsmith, Dr Charles Chew

Approval Date: 3 May 2012

Expiry Date: 2 May 2013

The University of Wollongong/Illawarra Shoalhaven Local Health District Social Sciences HREC is constituted and functions in accordance with the NHMRC *National Statement on Ethical Conduct in Human Research*. The HREC has reviewed the research proposal for compliance with the *National Statement* and approval of this project is conditional upon your continuing compliance with this document.

A condition of approval by the HREC is the submission of a progress report annually and a final report on completion of your project. The progress report template is available at <http://www.uow.edu.au/research/rso/ethics/UOW009385.html>. This report must be completed, signed by the appropriate Head of School, and returned to the Research Services Office prior to the expiry date.

As evidence of continuing compliance, the Human Research Ethics Committee also requires that researchers immediately report:

- proposed changes to the protocol including changes to investigators involved
- serious or unexpected adverse effects on participants
- unforeseen events that might affect continued ethical acceptability of the project.

Please note that approvals are granted for a twelve month period. Further extension will be considered on receipt of a progress report prior to expiry date.

Research Services Office University of Wollongong NSW 2522 Australia
Telephone: +61 2 4221 3386 Facsimile: +61 2 4221 4338
research-services@uow.edu.au www.uow.edu.au/research

If you have any queries regarding the HREC review process, please contact the Ethics Unit on phone 4221 3386 or email rso-ethics@uow.edu.au.

Yours sincerely

A/Professor Garry Hoban
**Chair, Social Sciences
Human Research Ethics Committee**

Cc: Professor Andrew Goldsmith, Faculty of Law



PARTICIPATION INFORMATION SHEET FOR BANKS' OFFICERS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

PURPOSE OF THE RESEARCH:

The aim of the research is to examine the adequacy and effectiveness of Indonesia's law in dealing with increasing frauds in ATM/Debit Card transactions (unauthorised ATM/Debit Card transaction). In particular, this research will investigate how to impose fair civil and criminal liabilities for unauthorised ATM/Debit transactions in Indonesia, especially when there is no clear evidence in regard to who actually accessed the EFT system. This research is expected to create fair, detailed and better fraud liabilities regulation and practice, and also improve bank's consumer protection and confidence for banking Industries in Indonesia.

INVESTIGATORS:

Prof. Andrew Goldsmith Faculty of Law/ Centre for Transnational Crime Prevention <i>agoldsmi@uow.edu.au</i>	Dr. Charles Chew Faculty of Law <i>charles@uow.edu.au</i>	Iwan Setiawan, Faculty of Law/ Centre for Transnational Crime Prevention, <i>is708@uow.edu.au</i>
---	---	---

METHOD & DEMANDS ON PARTICIPANTS:

If you choose to be included you will be asked to participate in a one – two hour interview by Mr. Iwan Setiawan. On this visit the researcher will conduct face-to-face interview that will be audio taped to ascertain the factors that enable or inhibit unauthorised consumers ATM/Debit card transaction (EFT fraud) in your institution, along with its ramification such as how to apportioned liability for the money lost caused by the frauds. Since the unauthorised ATM/Debit card transactions contain difference aspects such as legal (private, criminal, cyber, and consumer protection law) and technical aspects relating to card based payment system (magnetic stripe, chip, switching network, fraud method such as skimmer, sniffing, etc), you are welcome to bring colleagues from different department to support you during the interview.

Typical questions in the interview include:

1. Do you delivered ATM/Debit card transactions record to your consumers in regular basis? If yes, in what form and how often?
2. Do you record any of unauthorised ATM/Debit card transaction that affects your consumers?
3. What sorts of fraud methods have been employed by fraudsters to defraud your consumer's ATM/Debit Card?
4. Could you explain how your bank keeps update with the development/evolution of e-banking fraud methods and the security features technology to tackle it?
5. If your ATM booth is equipped with CCTV camera, are you recording all transactions 24/7? How long will the recording data be stored in your database?
6. How do you manage the legal relationship and adequate security standard of your card based payment system with your affiliate third parties such as merchants, sharing ATMs banks and switching companies?
7. Could you explain in brief how is your complaint handling mechanism especially toward unauthorised ATM/Debit card transaction claim by your consumer?
8. Could you explain what sort of actions by consumers you would consider as negligent/fault conduct?
9. Do you have an opinion why law enforcers prefer to use old criminal law (KUHP) in prosecuting ATM/Debit card perpetrators instead of new and more severe cyberlaw as in Information and Electronic Transaction Law (UU ITE)?

VOLUNTARY PARTICIPATION:

Your involvement in the study is voluntary and you may withdraw your participation from the study and any data that you have provided up until three months (90 days) since the interviewing date. Refusal to participate in the study will not affect your relationship with the University of Wollongong.

CONFIDENTIALITY:

The interview basically is conducted by the de-identifiable method. It means that no individual or organization/institution will be identified (unless there is consent). All data and information that is collected during the interview will remain confidential. The data and information will be stored securely at Centre for Transnational Crime Prevention, University of Wollongong. The data and information that have been obtained from you during the interview will be analysed along with that of the other participants in this study and used in the preparation of a thesis and associated academic publications.

CONSENT TO PARTICIPATE:

A consent form is attached. You need to complete and sign the consent form and return it at the time of the interview. Once you have completed the form, you will be considered to have given your consent to be involved in the research.

BENEFITS:

This study will not provide direct benefits to you personally. However, through participating in this research, you may be providing benefit to your organization/institution and potential better card based payment system regulation in the future that could benefit both banking industries and improve consumer protection in Indonesia.

POSSIBLE RISKS, INCONVENIENCES & DISCOMFORTS:

Apart from the one – two hours of your time for the interview, we can foresee no risks for you. During the interview you will have the right to decide which questions to answer and which not. As mentioned before, there will be de-identifiable method in collecting and processing data, both for individuals and organisations/institutions. Therefore, individual and collective interests will be protected for the entire process of the research, including after the completion of the research. The interview will focus on how laws and technical mechanisms are implemented at the practical level.

ETHICS REVIEW & COMPLAINTS:

If you have any further questions about this study, please contact Professor Goldsmith or Dr. Chew (details provided above). You will also have the opportunity to ask questions to the researcher before, during and after the interview.

This study has been reviewed by the Human Research Ethics Committee (HREC), social sciences of the University of Wollongong. If you have any concerns or complaints regarding the way this research has been conducted, you can contact the UOW Ethics Officer on +61 (2) 4221 3386 or email: rso-ethics@uow.edu.au.

Thank you for your interest in this study.



QUESTIONNAIRE FOR BANKS' OFFICERS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

1. When was the first time your ATM and Debit card product published in Indonesia?
2. Could you please tell me how many consumers' saving account that you have in your bank?
3. How many consumers' saving accounts that also equipped with ATM/Debit cards?
4. From your consumers' saving accounts that also equipped with ATM/Debit card, how many of them that also having an Internet Banking account?
5. Can your consumers open a saving account without having an ATM/Debit card?
6. Whether your consumers of ATM/Debit card must have used the ATM/Debit card along with their pass-book saving account in withdrawal cash at bank teller?
7. Do you delivered ATM/Debit card transactions record to your consumers in regular basis? If yes, in what form and how often?
8. Do you automatically notify consumers immediately, i.e. via SMS to their mobile once there is transaction occurring in their account?
9. If none of the above notification methods apply, how does a customer know about their ATM/Debit card transaction records?
10. Do you record any of unauthorised ATM/Debit card transaction that affects your consumers?
11. What sorts of fraud methods have been employed by fraudsters to defraud your consumer's ATM/Debit Card?
12. Are you consider all those ATM/Debit card fraud methods that commonly employed by fraudster such as skimming, card trapping, etc. as a foreseeable risk?
13. Do you have data about ATM/Debit card fraud that has affected your consumer and how much its damages (if possible yearly data in the last five years or more)?
14. Could you explain how your bank keeps update with the development/evolution of e-banking fraud methods and the security features technology to tackle it?
15. Why your bank has been relying quite a long time on magnetic stripe as a storage data on the ATM/Debit card which notoriously has been long know with its vulnerabilities and inherent foreseeable risks for card counterfeiting by various relatively easy method?

16. Do you use ATM and Debit Card system with 'neural networking' system that commonly employed in credit card system to help bank fraud management detect unauthorised ATM/Debit card transaction immediately?
17. If your ATM booth is equipped with CCTV camera, are you recording all transactions 24/7? How long will the recording data be stored in your database?
18. Are consumers' PIN and ATM/Debit card data encrypted during transmission from electronic agent site (ATM/EDC) to banks' data centre and vice versa?
19. Which fraud prevention method (physical/logical) have you employed to prevent particular consumer's ATM/Debit card data/ATM-Debit card being stolen at your particular point of compromised (PoC):

PoC	Targeted Object	Fraud Method	Fraud Prevention has employed & percentage of coverage to all your PoC?	Remark
ATM Machine	Card Data in mag. stripe	Skimming		
	ATM/Debit card	Card trapping/ Lebanese loop		
	PIN	Pin pad overlay/ key logger		
	ATM/Debit card data/PIN	Insert sniffing device in ATM machine		
Bank database centre	Consumers ATM/Debit card + PIN	Cracking or insider attack		
ATM booth	PIN	Pin hole camera		
	PIN	Fake CS phone sticker + social engineering		
	PIN	Shoulder surfing		
ATM Network	Card data + PIN	Sniffing/man in the middle attack		
Merchants	Debit card data + PIN at EFT-POS	Insert sniffing device in EFT POS machine		

	machine			
Merchants	Debit card data at mag-stripe	Illegal skimming using skimmer		
		‘Legal’ skimming using cashiers cash register machine		
	PIN	Pin hole camera		
		Peep by cashier		
Merchant database centre	Debit card data + PIN	Cracking or insider attack		

20. Do you think consumer’s PIN in ATM/Debit card transaction is equal to consumer’s signature in paper based transactions (such as signature in cheque)?
21. Do you think merely ATM/Debit card with :
 - a). magnetic stripe + PIN Data; or
 - b).Chip + PIN Data;
 have already fulfilled ‘non repudiation’ aspect of IT security and legal requirement?
22. Do you have any plan to migrate to chip based card payment system for your ATM/Debit Card?
23. Do you think chip based payment card is infallible?
24. How do you manage the legal relationship and adequate security standard of your card based payment system with your affiliate third parties such as merchants, sharing ATMs banks and switching companies?
25. Is your bank allowed your counterpart’s merchants to ‘swipe’ consumer’s card to their cash machine/computer register instead of just at EFT-POS/EDC terminal? (Are you aware of all consumer debit card data (track 1 and 2) then also stored at merchants computer)?
26. Explain in which way your consumer could report the occurrence of unauthorised ATM/Debit card transaction?
27. Is the ‘bank’s hot line’ available for 24/7?
28. Is all conversation happen in bank’s hot-line be recorded?
29. Could you specify all these banks’ hot line access (phone numbers, email address, etc).
30. Could you explain in brief how is your complaint handling mechanism especially toward unauthorised ATM/Debit card transaction claim by your consumer?
31. Is there any expired date for unauthorised ATM/Debit card transaction claim by consumer?

32. How you resolve unauthorised ATM/Debit card case where the point of compromised to consumers data has happened in other banks or third parties electronic agent (ATM/EDC), i.e in ATMs sharing or ATM owned by switching companies. Who will be liable for the consumers' loss?
33. In the event consumers' ATM/Debit card data were being compromised in your own electronic agent site (ATM/EFT-POS/EDC) where impossible to distinguished whether the fraudster were first party or third party, how you resolve the problem and who should bear all the loss?
34. When unauthorised ATM/Debit card transactions occurs that drain consumers' funds in his/her account within your bank, how and in what grounds do you apportioned liabilities between bank, consumer and/or third parties, in the event of:
 - a). consumer negligence/faulty;
 - b) Third party (affiliation institution) negligence/fault;
 - c). Bank negligence/fault;
 - d) Bank, third party, and/or consumer sharing negligence/fault;
35. Could you explain what sort of actions by consumers you would consider as negligent/fault conduct?
36. Do you distinguished negligence with gross negligence?
37. What is your policy regarding unauthorised ATM/Debit card transaction that still occur after consumer has notified you?
38. In what circumstances will the consumer money that had been stolen by fraudster be replaced by the bank?
39. According to your experiences after investigating unauthorised ATM/Debit card claimed by consumers, who were the most common perpetrators revealed: bank's/counterparts party employee, consumers itself, consumer's acquaintances, or unknown third party?
40. What is your stance in terms of liability regarding unauthorised ATM/Debit card transactions that have happened under conditions below:
 - It was conducted *with* consumer consent by consumer acquaintances such as spouse, family member, work colleagues, 'office boy/girl', and alike.
 - It was conducted *without* consumer consent by consumer acquaintances such as spouse, family member, work colleagues, 'office boy/girl', and alike.
 - It was conducted under duress or threatening;
 - It was conducted by unknown third party/fraudsters;
 - It was conducted under hypnosis.
41. In the disputes between bank and consumer regarding unauthorised ATM/Debit card transactions, who should have burden of proof? Why?
42. When your ATM/Debit card has Visa/MasterCard logo in it, is there any 'zero liabilities rules' apply by Visa/MasterCard to the cards if unauthorised ATM/Debit Card has occurred?

43. Why do you still have indemnity clause in your consumer-banking contract which limit your liability and deliver most liability to your consumer, which might be in conflict with the provisions of the Indonesian Consumer Protection Act?
44. If fraud liabilities that relatively have no regulation should be regulating, which regulation model is do you think best for banking industries in Indonesia: legislation act (UU), Bank Indonesia Regulation (PBI) or banks' bye laws/code of conduct?
45. When contentious disputes occurred between you and your customer over unauthorised ATM/Debit card transaction and could not be resolved internally, which legal settlement is more preferable for you between court, Consumer Settlement Disputes Body (Badan Penyelesaian Sengketa Konsumen), or Banking Mediation Directorate (Direktorat Mediasi Perbankan – Bank Indonesia) and why?
46. One of the Indonesia' Supreme Court decision constitute bank's failure to secure its ATM booth that enable fraudulent activities have consequences for banks to cover all consumer's damages. What do you think about this decision?
47. As can be read in many articles in national news papers/on-line news, it's very common bank withdrawal consumers' claim over unauthorised ATM/Debit card transactions only by the fact that 'purported' consumer using the right card data and PIN. What is your opinion about this phenomenon?
48. Different countries have different regulation over unauthorised ATM/Debit card transaction. In United States, in principle, banks will always be liable for unauthorised ATM/Debit card transactions, regardless of any negligent conduct by the consumers. In Australia and European Union countries, consumers only should liable for unauthorised ATM/Debit card transaction if he/she has conducted gross negligence. Other than that, banks are forbidden by regulation to use ATM/Debit card data including right PIN number as the only factor to authorise the ATM/Debit card transactions. What do you think if these regulations are going to be implemented in Indonesia?
49. Could you explain in what ways and how often you have consumer education programmes?
50. Does your consumer education programmes includes state of the art of ATM/Debit card fraud methods?
51. How do you gauge that your consumer education programmes can effectively reach all segment of your consumer?
52. Could you provide me some examples (letters, brochures, leaflets, etc) of your consumer education programmes?
53. Do you think all these ATM/Debit fraud wave that recently happened in Indonesia will impact on consumers' confidence in saving their money in the bank and/or conducting ATM/Debit card transactions?

54. According to your knowledge, do you know whether or not transnational crime actors (international criminal networks) are involved in ATM/Debit fraud in Indonesia?
55. Do you have any civil litigation experience regarding consumer's claim over unauthorised ATM/Debit card transactions in the past ten years?
56. Do you have any experienced that one or more fraudsters that defraud your bank have been convicted by criminal court? If yes, could you provide me a copy/ of the court verdicts?
57. In general, are you satisfied with some district court criminal verdict over unauthorised ATM/Debit card perpetrators in Indonesia?
58. Do you have an opinion why law enforcers prefer to use old criminal law (KUHP) in prosecuting ATM/Debit card perpetrators instead of new and more severe cyberlaw as in Information and Electronic Transaction Law (UU ITE)?



PARTICIPATION INFORMATION SHEET FOR BANK/SECURITY EXPERTS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

PURPOSE OF THE RESEARCH :

The aim of the research is to examine the adequacy and effectiveness of Indonesia’s law in dealing with increasing frauds in ATM/Debit Card transactions (unauthorised ATM/Debit Card transaction). In particular, this research will investigate how to impose fair civil and criminal liabilities for unauthorised ATM/Debit transactions in Indonesia, especially when there is no clear evidence in regard to who actually accessed the EFT system. This research is expected to create fair, detailed and better fraud liabilities regulation and practice, and also improve bank’s consumer protection and confident for banking Industries in Indonesia.

INVESTIGATORS :

Prof. Andrew Goldsmith Faculty of Law/ Centre for Transnational Crime Prevention <i>agoldsmi@uow.edu.au</i>	Dr. Charles Chew Faculty of Law <i>charles@uow.edu.au</i>	Iwan Setiawan, Faculty of Law/ Centre for Transnational Crime Prevention, <i>is708@uow.edu.au</i>
---	---	---

METHOD & DEMANDS ON PARTICIPANTS:

If you choose to be included you will be asked to participate in a one – two hour interview by Mr. Iwan Setiawan. On this visit the researcher will conduct face-to-face interview that will be audio taped to ascertain the factors that enable or inhibit unauthorised consumers ATM/Debit card transaction (EFT fraud) in your institution, along with its ramification such as how to apportioned liability for the money lost caused by the frauds. Since the unauthorised ATM/Debit card transactions contain difference aspects such as legal (private, criminal, cyber, and consumer protection law) and technical aspects relating to card based payment system (magnetic stripe, chip, switching network, fraud method such as skimmer, sniffing, etc), you are welcome to bring colleagues from different department to support you during the interview.

Typical questions in the interview:

1. What is your comment concerning unauthorised ATM/Debit Card transactions that are on the rise in Indonesia?
2. What sorts of fraud methods have been employed by fraudsters to steal banks' consumer's ATM/Debit card data?
3. Which fraud prevention methods should be implemented by banks in Indonesia in order to prevent unauthorised ATM/Debit card transactions to occur by various fraud methods?
4. Do you think the implementation of ATM security features such as anti-skimmer devices, jitter; etc by banks in Indonesia could overcome unauthorised ATM/debit card problems?
5. Do you think chip based payment card will be infallible, therefore consumers will be always liable in the event of unauthorised ATM/Debit Card transactions?
6. Do you think consumer's PIN in ATM/Debit card transaction is equal to consumer's signature in paper based transactions (such as signature in cheque)?

VOLUNTARY PARTICIPATION:

Your involvement in the study is voluntary and you may withdraw your participation from the study and any data that you have provided up until three months (90 days) since the interviewing date. Refusal to participate in the study will not affect your relationship with the University of Wollongong.

CONFIDENTIALITY:

The interview basically is conducted by the de-identifiable method. It means that no individual or organization/institution will be identified (unless there is consent). All data and information that is collected during the interview will remain confidential. The data and information will be stored securely at Centre for Transnational Crime Prevention, University of Wollongong. The data and information that have been obtained from you during the interview will be analysed along with that of the other participants in this study and used in the preparation of a thesis and associated academic publications.

CONSENT TO PARTICIPATE:

A consent form is attached. You need to complete and sign the consent form and return it at the time of the interview. Once you have completed the form, you will be considered to have given your consent to be involved in the research.

BENEFITS:

This study will not provide direct benefits to you personally. However, through participating in this research, you may be providing benefit to your organization/institution and potential better card based payment system regulation in the future that could benefit both banking industries and improve consumer protection in Indonesia.

POSSIBLE RISKS, INCONVENIENCES & DISCOMFORTS:

Apart from the one – two hours of your time for the interview, we can foresee no risks for you. During the interview you will have the right to decide which questions to answer and which not. As mentioned before, there will be de-identifiable method in collecting and processing data, both for individuals and organisations/institutions. Therefore, individual and collective interests will be protected for the entire process of the research, including after the completion of the research. The interview will focus on how laws and technical mechanisms are implemented at the practical level.

ETHICS REVIEW & COMPLAINTS:

If you have any further questions about this study, please contact Professor Goldsmith or Dr. Chew (details provided above). You will also have the opportunity to ask questions to the researcher before, during and after the interview.

This study has been reviewed by the Human Research Ethics Committee (HREC), social sciences of the University of Wollongong. If you have any concerns or complaints regarding the way this research has been conducted, you can contact the UOW Ethics Officer on +61 (2) 4221 3386 or email: rso-ethics@uow.edu.au.

Thank you for your interest in this study.



QUESTIONNAIRE FOR BANK/SECURITY EXPERTS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

1. What is your comment concerning unauthorised ATM/Debit Card transactions that are on the rise in Indonesia?
2. What sorts of fraud methods have been employed by fraudsters to steal banks' consumer's ATM/Debit card data?
3. What are the most common fraud methods that have been employed by fraudsters to defraud bank's consumer's ATM/Debit Card?
4. Which fraud prevention methods should be implemented by banks in Indonesia in order to prevent unauthorised ATM/Debit card transactions to occur by various fraud methods such as 'skimming'+ pin hole camera, pin-pad overlay, social engineering using 'fake customer service/call centre sticker', shoulder surfing, and 'Lebanese loop'?
5. Why has the bank been relying only on the magnetic stripe technology as a storage data on the ATM/Debit card when it has been known for a long time to be very vulnerable to card counterfeiting?
6. Do you think the implementation of neural network method is useful for bank in order to help bank fraud management detect unauthorised ATM/Debit card transactions immediately?
7. Do you think the implementation of ATM security features such as anti-skimmer devices, jitter; etc by banks in Indonesia could overcome unauthorised ATM/debit card problems?
8. Do you think installation of security cameras in every ATM booth is important?
9. Do you think banks in Indonesia have adequate security standard in their card based payment system?
10. When unauthorised ATM/Debit card transactions have occurred, which party is more likely have to bear the fraud loss? Why?
11. Different countries have different regulations over unauthorised ATM/Debit card transaction. In United States, in principle, banks are liable for unauthorised ATM/Debit card transactions, regardless of any negligent conduct by the consumers. In Australia and European Union countries, consumers are only liable for unauthorised ATM/Debit card transaction if he/she has conducted gross negligence. Other than that, banks are forbidden by regulation to use ATM/Debit card data including right PIN number as the only factor to authorise the ATM/Debit card transactions. What do you think if these regulations are to be implemented in Indonesia?

12. Do you think chip based payment card will be infallible, therefore consumers will be always liable in the event of unauthorised ATM/Debit Card transactions?
13. What is your opinion regarding merchants' practices to swipe consumer's card to their cash machine/computer register instead of just at EFT-POS/EDC terminal?
14. Do you think all these ATM/Debit fraud wave that recently happened in Indonesia will impact on consumers' confidence in saving their money in the bank and/or conducting ATM/Debit card transactions?
15. Do you have any suggestions for banks and Banks Indonesia in order to reduce unauthorised ATM/Debit card transactions in Indonesia?
16. Could you explain typology of ATM/Debit card fraudsters?
17. Do you consider of ATM/Debit card fraud as high technology crime or just low technology crime?
18. According to your knowledge, are consumers' PIN and ATM/Debit card data encrypted during transmission from electronic agent site (ATM/EDC) to banks' data centre and vice versa?
19. Do you think consumer's PIN in ATM/Debit card transaction is equal to consumer's signature in paper based transactions (such as signature in cheque)?
20. Do you think merely ATM/Debit card with :
 - a). magnetic stripe + PIN Data; or
 - b).Chip + PIN Data;Have already fulfilled 'non repudiation' aspect of IT security and legal requirement?
21. According to your knowledge, are transnational crime actors (international criminal networks) involved in ATM/Debit fraud in Indonesia?
22. Do you have any suggestions to consumers or banks to prevent their electronic banking transactions being victimized by fraudster?



PARTICIPATION INFORMATION SHEET FOR BANK'S CONSUMERS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

PURPOSE OF THE RESEARCH:

The aim of the research is to examine the adequacy and effectiveness of Indonesia's law in dealing with increasing frauds in ATM/Debit Card transactions (unauthorised ATM/Debit Card transaction). In particular, this research will investigate how to impose fair civil and criminal liabilities for unauthorised ATM/Debit transactions in Indonesia, especially when there is no clear evidence in regard to who actually accessed the EFT system. This research is expected to create fair, detailed and better fraud liabilities regulation and practice, and also improve bank's consumer protection and confidence for banking Industries in Indonesia.

INVESTIGATORS:

Prof. Andrew Goldsmith Faculty of Law/ Centre for Transnational Crime Prevention <i>agoldsmi@uow.edu.au</i>	Dr. Charles Chew Faculty of Law <i>charles@uow.edu.au</i>	Iwan Setiawan, Faculty of Law/ Centre for Transnational Crime Prevention, <i>is708@uow.edu.au</i>
--	---	---

METHOD & DEMANDS ON PARTICIPANTS:

If you choose to be included you will be asked to participate in a one – two hour interview by Mr. Iwan Setiawan. On this visit the researcher will conduct face-to-face interview that will be audio taped to ascertain the factors that enable or inhibit unauthorised consumers ATM/Debit card transaction (EFT fraud) in your institution, along with its ramification such as how to apportioned liability for the money lost caused by the frauds. Since the unauthorised ATM/Debit card transactions contain difference aspects such as legal (private, criminal, cyber, and consumer protection law) and technical aspects relating to card based payment system (magnetic stripe, chip, switching network, fraud method such as skimmer, sniffing, etc), you are welcome to bring colleagues from different department to support you during the interview.

Typical questions in the interview:

1. Do you have to use your ATM/Debit card along with your pass-book to withdrawn your money from bank's teller?
2. Does your bank send your ATM/Debit card or saving account detail transaction report regularly to you, such as monthly reports? In what way and how often does the bank send this report?
3. Do you think your bank's ATM/Debit card systems are infallible?
4. Do you use your birthday date or part of your birthday date as your PIN?
5. Have you experienced unauthorised ATM/Debit card transaction?
6. What do you know about the magnetic stripe in your ATM/Debit card?
7. Do you think the bank's education programmes are adequate enough to make you understand about e-banking risk and the way how to avoid them?

VOLUNTARY PARTICIPATION:

Your involvement in the study is voluntary and you may withdraw your participation from the study and any data that you have provided up until three months (90 days) since the interviewing date. Refusal to participate in the study will not affect your relationship with the University of Wollongong.

CONFIDENTIALITY:

The interview basically is conducted by the de-identifiable method. It means that no individual or organization/institution will be identified (unless there is consent). All data and information that is collected during the interview will remain confidential. The data and information will be stored securely at Centre for Transnational Crime Prevention, University of Wollongong. The data and information that have been obtained from you during the interview will be analysed along with that of the other participants in this study and used in the preparation of a thesis and associated academic publications.

CONSENT TO PARTICIPATE:

A consent form is attached. You need to complete and sign the consent form and return it at the time of the interview. Once you have completed the form, you will be considered to have given your consent to be involved in the research.

BENEFITS:

This study will not provide direct benefits to you personally. However, through participating in this research, you may be providing benefit to your organization/institution and potential better card based payment system regulation in the future that could benefit both banking industries and improve consumer protection in Indonesia.

POSSIBLE RISKS, INCONVENIENCES & DISCOMFORTS:

Apart from the one – two hours of your time for the interview, we can foresee no risks for you. During the interview you will have the right to decide which questions to answer and which not. As mentioned before, there will be de-identifiable method in collecting and processing data, both for individuals and organisations/institutions. Therefore, individual and collective interests will be protected for the entire process of the research, including after the completion of the research. The interview will focus on how laws and technical mechanisms are implemented at the practical level.

ETHICS REVIEW & COMPLAINTS:

If you have any further questions about this study, please contact Professor Goldsmith or Dr. Chew (details provided above). You will also have the opportunity to ask questions to the researcher before, during and after the interview.

This study has been reviewed by the Human Research Ethics Committee (HREC), social sciences of the University of Wollongong. If you have any concerns or complaints regarding the way this research has been conducted, you can contact the UOW Ethics Officer on +61 (2) 4221 3386 or email: rso-ethics@uow.edu.au.

Thank you for your interest in this study.



QUESTIONNAIRE FOR CONSUMERS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

1. What is your bank's name where you have ATM/Debit Card facility?
2. Did you read all terms and condition in your contract with bank when opening a saving account with ATM/Debit card features?
3. Do you have to use your ATM/Debit card along with your pass-book to withdrawn your money from bank's teller?
4. Does your bank send your ATM/Debit card or saving account detail transaction report regularly to you, such as monthly reports? In what way and how often does the bank send this report if any?
5. Does your bank notify you immediately by SMS every time you finished your ATM/Debit card transactions?
6. Do you have Internet banking facility where you can see all your detail ATM/Debit card transactions? If yes, how many months backward can you retrieve the monthly report?
7. Do you think your bank's ATM/Debit card systems are infallible?
8. How many digits are your ATM/Debit cards PIN?
9. Did you change the default PIN from your bank to your own series of number as your new PIN?
10. Do you change your ATM/Debit card PIN regularly?
11. Do you use your birthday date or part of your birthday date as your PIN?
12. Do you use easy numbers to remember such as 1234 as your PIN?
13. Do you put your PIN record inside your wallet or purse/bag or even stick it to your ATM/Debit card to help you write down PIN during ATM/Debit card transaction? If yes, whether this PIN record
 - Disguise? Or
 - Not disguise.
14. Will you revealed your PIN if someone from the banks asks you to, as prerequisite for one particular banks' service?
15. Do you know your bank's consumer service / hot line number? Do you record this number in your mobile phone?
16. Have you ever asked a favor from your trusted person to withdraw or transfer money using your ATM/Debit card and PIN (such as spouse, children, best friends, girl/boy friend or your trusted 'office boy/girl' in the office)?
17. Have you experienced unauthorised ATM/Debit card transaction?
18. If the answer of question 17 is 'yes', could you explain how your money was lost from your bank and whether or not bank replaced your money?

19. Do you know that conducting electronic banking including ATM/Debit card transaction has certain risk including fraud risk?
20. Do you know that fraudster targeted bank's consumer ATM/Debit card data in order to make unauthorised ATM/Debit card transactions?
21. If your answer to questions 19 and 20 is 'yes', how do you know this knowledge:
 - From my bank;
 - From Bank Indonesia as a central bank;
 - From other source such as email from experts, mailing list, news paper article, etc.
22. Do you examine ATM booth and ATM machine carefully to find something unusual before conducting ATM/Debit card transaction?
23. Do you know what is these terminology mean:
 - pin-hole camera;
 - skimmer;
 - pin-pad overlay;
 - card trapping;
 - fake CS stickers; or
 - Shoulder surfing.
24. Do you always cover the PIN-pad at the ATM booth or merchant's EFT-POS EDC before conducting ATM/Debit card transactions? Why?
25. What will you do if for some reason, your ATM/Debit card got stuck inside the ATM machine:
 - Call the bank's consumer service number sticker as shown at the ATM booth;
 - Ask help from 'a good Samaritan' around the ATM booth;
 - Check the ATM machine especially the card entrance hole in ATM machine to find anything that unusual such as black sticky tape, black ribbon, or alike.
 - Something else, please explain....
26. If case like number 25 happened to you and you call your bank's customer service (CS) number as shown in the stickers at the ATM booth, and according to the CS the only way to secure your ATM/Debit card is to give your PIN to the CS in order to enable the CS to cancel your card and issue a new one, would you give your PIN?
27. What do you know about magnetic stripe in your ATM/Debit card?
28. What do you know about chip based payment card?
29. Would you perform an ATM/Debit card transaction at another bank's ATM/EFT-POS? Why?
30. Indonesia has suffered from massive ATM fraud back in 2010 such as what happened in Bali which caused damaged more than 10 billion Rupiahs. Do you think such fact will affect your confidence to conduct ATM/Debit card transactions?
31. In many cases as you might have read from mass-media, many bank's consumers claim that unauthorised ATM/Debit card transaction have been rejected by banks on the grounds that consumers have obligation to secure its ATM/Debit card and PIN secrecy, and the transactions are deem valid because the right card and PIN have been used. What do you think about this fact?

32. In contrast with statement number 31, in many other countries such as US and Australia, banks in most of the cases is obligated by law or by code of conduct to replace consumer's damage caused by unauthorised ATM/Debit card transaction – except if it can be proved that the consumer is at fault due to gross negligence. Do you thing this kind of regulation could increase your confidence on conducting EFT transactions in Indonesia?
33. According to you, in regard of unauthorised ATM/Debit card transactions, which party is deemed should be liable for the damages?
34. If a consumer is negligent or careless when using his/her ATM/Debit card so that the fraudster is able to obtain the consumer's EFT data including PIN, do you thing its fair and right if consumer should bear all or some part of his/her loss of money?
35. Have you heard about:
- Bank Indonesia's Directorate of Mediation and Investigation;
 - Consumer Settlement Disputes Body; or
 - Civil Court;
- which of these bodies have capability to help resolve contentious disputes between consumer and the bank concerning unauthorised ATM/Debit card transactions?
36. If your answer to question number 35 is "yes", which institution is more preferable for you to settle the disputes: court, Consumer Settlement Disputes Body (Badan Penyelesaian Sengketa Konsumen), or Banking Mediation Directorate (Direktorat Mediasi Perbankan – Bank Indonesia) and why?
37. Banks in Indonesia have obligation to educate its consumer about many aspect of banking including e-banking fraud. Have you received any kind of e-banking risk education programme during your account relationship with your bank? If yes, how did you get this education programme:
- Via bank's TV programme;
 - Via bank's news paper programme;
 - Via bank's letter;
 - Via bank's statement;
 - Via bank's email;
 - Via bank's SMS;
 - Via bank's flyers or pamphlet;
 - Via bank's other sources:
38. Do you think bank's education programmes are adequate enough to make you understand about e-banking risk and the way how to avoid them?



PARTICIPATION INFORMATION SHEET FOR LAW ENFORCERS OFFICERS

TITLE:

**“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection
in Indonesia: A Critical Analysis of Law and Practice”**

PURPOSE OF THE RESEARCH :

The aim of the research is to examine the adequacy and effectiveness of Indonesia’s law in dealing with increasing frauds in ATM/Debit Card transactions (unauthorised ATM/Debit Card transaction). In particular, this research will investigate how to impose fair civil and criminal liabilities for unauthorised ATM/Debit transactions in Indonesia, especially when there is no clear evidence in regard to who actually accessed the EFT system. This research is expected to create fair, detailed and better fraud liabilities regulation and practice, and also improve bank’s consumer protection and confident for banking Industries in Indonesia.

INVESTIGATORS :

Prof. Andrew Goldsmith Faculty of Law/ Centre for Transnational Crime Prevention <i>agoldsmi@uow.edu.au</i>	Dr. Charles Chew Faculty of Law <i>charles@uow.edu.au</i>	Iwan Setiawan, Faculty of Law/ Centre for Transnational Crime Prevention, <i>is708@uow.edu.au</i>
---	---	---

METHOD & DEMANDS ON PARTICIPANTS:

If you choose to be included you will be asked to participate in a one – two hour interview by Mr. Iwan Setiawan. On this visit the researcher will conduct face-to-face interview that will be audio taped to ascertain the factors that enable or inhibit unauthorised consumers ATM/Debit card transaction (EFT fraud) in your institution, along with its ramification such as how to apportioned liability for the money lost caused by the frauds. Since the unauthorised ATM/Debit card transactions contain difference aspects such as legal (private, criminal, cyber, and consumer protection law) and technical aspects relating to card based payment system (magnetic stripe, chip, switching network, fraud method such as skimmer, sniffing, etc), you are welcome to bring colleagues from different department to support you during the interview.

Typical questions in the interview:

1. Do you record any of the unauthorised ATM/Debit card transaction cases that have been brought to you on a national scale?
2. What are the most common fraud methods that have been employed by fraudsters to defraud bank's consumer's ATM/Debit Card?
3. Could you explain typology of ATM/Debit card fraudsters?
4. According to your knowledge/experience, whether or not transnational crime actors (international criminal networks) are involved in ATM/Debit fraud in Indonesia?
5. According to several criminal court verdicts over some ATM/Debit Card fraudster, all the fraudster of unauthorised ATM/Debit card transactions including those responsible for ATM fraud deluge in Jakarta and Bali in 2010 - have been convicted by old criminal code provisions (KUHP), even though relatively new 'cyber crime law' such as Information and Electronic Transactions Law (UU ITE) which have more severe punishment for fraudster of unauthorised ATM/Debit card transactions, have been enacted in 2008 (according to Indonesia law system, special law should be prevail over general law). Could you explain why law enforcers prefer to use old provisions in KUHP instead of UU ITE?

VOLUNTARY PARTICIPATION:

Your involvement in the study is voluntary and you may withdraw your participation from the study and any data that you have provided up until three months (90 days) since the interviewing date. Refusal to participate in the study will not affect your relationship with the University of Wollongong.

CONFIDENTIALITY:

The interview basically is conducted by the de-identifiable method. It means that no individual or organization/institution will be identified (unless there is consent). All data and information that is collected during the interview will remain confidential. The data and information will be stored securely at Centre for Transnational Crime Prevention, University of Wollongong. The data and information that have been obtained from you during the interview will be analysed along with that of the other participants in this study and used in the preparation of a thesis and associated academic publications.

CONSENT TO PARTICIPATE:

A consent form is attached. You need to complete and sign the consent form and return it at the time of the interview. Once you have completed the form, you will be considered to have given your consent to be involved in the research.

BENEFITS:

This study will not provide direct benefits to you personally. However, through participating in this research, you may be providing benefit to your organization/institution and potential better card based payment system regulation in the future that could benefit both banking industries and improve consumer protection in Indonesia.

POSSIBLE RISKS, INCONVENIENCES & DISCOMFORTS:

Apart from the one – two hours of your time for the interview, we can foresee no risks for you. During the interview you will have the right to decide which questions to answer and which not. As mentioned before, there will be de-identifiable method in collecting and processing data, both for individuals and organisations/institutions. Therefore, individual and collective interests will be protected for the entire process of the research, including after the completion of the research. The interview will focus on how laws and technical mechanisms are implemented at the practical level.

ETHICS REVIEW & COMPLAINTS:

If you have any further questions about this study, please contact Professor Goldsmith or Dr. Chew (details provided above). You will also have the opportunity to ask questions to the researcher before, during and after the interview.

This study has been reviewed by the Human Research Ethics Committee (HREC), social sciences of the University of Wollongong. If you have any concerns or complaints regarding the way this research has been conducted, you can contact the UOW Ethics Officer on +61 (2) 4221 3386 or email: rso-ethics@uow.edu.au.

Thank you for your interest in this study.



QUESTIONNAIRE FOR LAW ENFORCERS OFFICERS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

1. Do you record any of the unauthorised ATM/Debit card transaction cases that have been brought to you on a national scale?
2. What are the most common fraud methods that have been employed by fraudsters to defraud bank's consumer's ATM/Debit Card?
3. Do you think installation of security cameras in every ATM booth is important?
4. Do you think banks in Indonesia have adequate security standard in their card based payment system?
5. Could you explain typology of ATM/Debit card fraudsters?
6. According to your knowledge/experience, whether or not transnational crime actors (international criminal networks) are involved in ATM/Debit fraud in Indonesia?
7. Do you think of ATM/Debit card fraud as high technology crime or just low technology crime?
8. Do you think consumer's PIN in ATM/Debit card transaction is equal to consumer's signature in paper based transactions (such as signature in cheque)?
9. Do you think merely ATM/Debit card with :
 10. a). magnetic stripe + PIN Data; or
 11. b).Chip + PIN Data;
12. Have already fulfilled 'non repudiation' aspect of IT security and legal requirement?
13. Do you have any suggestions to consumers or banks to prevent their electronic banking transactions especially ATM/Debit card transactions being victimized by fraudster?
14. According to several criminal court verdicts over some ATM/Debit Card fraudster, all the fraudster of unauthorised ATM/Debit card transactions including those responsible for ATM fraud deluge in Jakarta and Bali in 2010 - have been convicted by old criminal code provisions (KUHP), even though relatively new 'cyber crime law' such as Information and Electronic Transactions Law (UU ITE) which have more severe punishment for fraudster of unauthorised ATM/Debit card transactions, have been enacted in 2008 (according to Indonesia law system, special law should be prevail over general law). Could you explain why law enforcers prefer to use old provisions in KUHP instead of UU ITE?



PARTICIPATION INFORMATION SHEET FOR MEDIATION OFFICERS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

PURPOSE OF THE RESEARCH :

The aim of the research is to examine the adequacy and effectiveness of Indonesia’s law in dealing with increasing frauds in ATM/Debit Card transactions (unauthorised ATM/Debit Card transaction). In particular, this research will investigate how to impose fair civil and criminal liabilities for unauthorised ATM/Debit transactions in Indonesia, especially when there is no clear evidence in regard to who actually accessed the EFT system. This research is expected to create fair, detailed and better fraud liabilities regulation and practice, and also improve bank’s consumer protection and confidence for banking Industries in Indonesia.

INVESTIGATORS:

Prof. Andrew Goldsmith Faculty of Law/ Centre for Transnational Crime Prevention <i>agoldsmi@uow.edu.au</i>	Dr. Charles Chew Faculty of Law <i>charles@uow.edu.au</i>	Iwan Setiawan, Faculty of Law/ Centre for Transnational Crime Prevention, <i>is708@uow.edu.au</i>
---	---	---

METHOD & DEMANDS ON PARTICIPANTS:

If you choose to be included you will be asked to participate in a one – two hour interview by Mr. Iwan Setiawan. On this visit the researcher will conduct face-to-face interview that will be audio taped to ascertain the factors that enable or inhibit unauthorised consumers ATM/Debit card transaction (EFT fraud) in your institution, along with its ramification such as how to apportioned liability for the money lost caused by the frauds. Since the unauthorised ATM/Debit card transactions contain difference aspects such as legal (private, criminal, cyber, and consumer protection law) and technical aspects relating to card based payment system (magnetic stripe, chip, switching network, fraud method such as skimmer, sniffing, etc), you are welcome to bring colleagues from different department to support you during the interview.

Typical questions in the interview:

1. Could you provide general data about mediation process that involved disputes between bank and its consumer regarding unauthorised consumer ATM/Debit card transactions?
2. What sort of theory, regulation or principle have you used in determining who should be liable for consumer's lost caused by unauthorised ATM/Debit card transactions?
3. What sort of circumstances or condition are commonly used as compelling factors in order to 'decide' whether banks, consumers, or both of them should be liable for the lost?
4. If both bank and consumer share negligence or faulty conduct, how do you apportion liability between these two parties?

VOLUNTARY PARTICIPATION:

Your involvement in the study is voluntary and you may withdraw your participation from the study and any data that you have provided up until three months (90 days) since the interviewing date. Refusal to participate in the study will not affect your relationship with the University of Wollongong.

CONFIDENTIALITY:

The interview basically is conducted by the de-identifiable method. It means that no individual or organization/institution will be identified (unless there is consent). All data and information that is collected during the interview will remain confidential. The data and information will be stored securely at Centre for Transnational Crime Prevention, University of Wollongong. The data and information that have been obtained from you during the interview will be analysed along with that of the other participants in this study and used in the preparation of a thesis and associated academic publications.

CONSENT TO PARTICIPATE:

A consent form is attached. You need to complete and sign the consent form and return it at the time of the interview. Once you have completed the form, you will be considered to have given your consent to be involved in the research.

BENEFITS:

This study will not provide direct benefits to you personally. However, through participating in this research, you may be providing benefit to your organization/institution and potential better card based payment system regulation in the future that could benefit both banking industries and improve consumer protection in Indonesia.

POSSIBLE RISKS, INCONVENIENCES & DISCOMFORTS:

Apart from the one – two hours of your time for the interview, we can foresee no risks for you. During the interview you will have the right to decide which questions to answer and which not. As mentioned before, there will be de-identifiable method in collecting and processing data, both for individuals and organisations/institutions. Therefore, individual and collective interests will be protected for the entire process of the research, including after the completion of the research. The interview will focus on how laws and technical mechanisms are implemented at the practical level.

ETHICS REVIEW & COMPLAINTS:

If you have any further questions about this study, please contact Professor Goldsmith or Dr. Chew (details provided above). You will also have the opportunity to ask questions to the researcher before, during and after the interview.

This study has been reviewed by the Human Research Ethics Committee (HREC), social sciences of the University of Wollongong. If you have any concerns or complaints regarding the way this research has been conducted, you can contact the UOW Ethics Officer on +61 (2) 4221 3386 or email: rs0-ethics@uow.edu.au.

Thank you for your interest in this study.



QUESTIONNAIRE FOR MEDIATION OFFICERS

TITLE:

“Regulation of Unauthorised Electronic Funds Transfer and Consumer Protection in Indonesia: A Critical Analysis of Law and Practice”

1. Could you provide general data about mediation process that involved disputes between bank and its consumer regarding unauthorised consumer ATM/Debit card transactions?
2. What sort of theory, regulation or principle have you used in determining who should be liable for consumer's lost caused by unauthorised ATM/Debit card transactions?
3. What sort of circumstances or condition are commonly used as compelling factors in order to 'decide' whether banks, consumers, or both of them should be liable for the lost?
4. Magnetic stripe technology that has been used as storage data in bank's ATM/Debit card for a long time are very vulnerable to compromised by fraudster (have no encryption or security layer) and banks are fully aware of it as foreseeable risk. What do you think about this fact in relation with bank's liability as an electronic banking provider?
5. Do you think consumer's PIN in ATM/Debit card transaction is equal to consumer's signature in paper based transactions (such as signature in cheque)?
6. Do you think merely ATM/Debit card with :
 - a). magnetic stripe + PIN Data; or
 - b).Chip + PIN Data;
7. Have already fulfilled 'non repudiation' aspect of IT security and legal requirement?
8. Do you have opinion whether or not ATM/Debit card with magnetic stripe technology + PIN could/could not satisfy 'non repudiation' requirement required by central bank or other security standards?
9. Do you think 'negligent' and 'fault' between banks and consumers are important factor in determining who should be liable for unauthorised ATM/Debit card transactions?
10. Could you share what sort of action or inaction that can be constituted as 'negligence' and 'fault'? For instance, many unauthorised ATM/Debit card frauds were successful because fraudster managed to collect consumers' data by successfully putting skimmer, pinpad overlay, pin hole camera, card trapping device (Lebanese loop), fake consumer care telephone number stickers at bank's ATM booth/merchant's Electronic Data Capture (EDC). However, banks always defended this fact by showing that it's impossible for bank to supervise its entire

ATM booth/merchant's EDC because of its huge numbers of machines. What do you think about this matter?

11. If both bank and consumer share negligence or faulty conduct, how do you apportion liability between these two parties?
12. Different countries have different regulations over unauthorised ATM/Debit card transactions. In United States, in principle, banks will always be liable for unauthorised ATM/Debit card transactions, regardless of consumer negligence being the cause of the unauthorised ATM/Debit card transaction. In Australia and European Union countries, consumers are only liable for unauthorised ATM/Debit card transactions if he/she has conducted gross negligence. Other than that, banks are forbidden by regulations to use ATM/Debit card data including right PIN number as the only factor to authorise the ATM/Debit card transactions. What do you think if these regulations are going to be implemented in Indonesia?
13. Banks very commonly still have indemnity clausal in their consumer-banking contract which limit bank's liability and deliver most liability on to consumer shoulders, which are in conflict with the provisions of the Indonesian Consumer Protection Act? Do you think this bank's clausal should be null and void?
14. How is your recommendation regarding fraud liability if there is neither clear evidence regarding bank nor consumer negligence that enabled unauthorised ATM/Debit card transaction?
15. Do you think all these ATM/Debit fraud wave that recently happened in Indonesia will impact on consumers' confidence in saving their money in the bank and/or conducting ATM/Debit card transactions?