TOWARDS A BETTER CREDIT CARD FRAUD PREVENTION STRATEGY IN INDONESIA

Hendi Yogi Prabowo

Abstract

For years, credit card fraud has been a major problem in the Indonesian payments system. Numerous efforts have been made to mitigate this payment crime. Nevertheless, the high fraud losses recorded in particular by banks and other parties in credit card networks suggests that more actions still need to be taken. For this, formulation of a sound fraud prevention strategy is paramount to the success in combating credit card fraud in a payments system. Such a strategy will ensure that available resources are allocated effectively and efficiently. This article, which is based on the author’s PhD research, seeks to assess the soundness of the credit card fraud prevention strategy in the Indonesian payments system. For analytical purpose, references are made to similar practices in other countries such as the United States, the United Kingdom and Australia. The study was conducted using document review and interviews and was focusing on the period of 2003 through 2007. The discussions in this article conclude that just as in other countries such as the United States, the United Kingdom and Australia, the essentials of credit card fraud prevention practice in the Indonesia comprise six key areas of resource allocation: understanding of the real problems; fraud prevention policy; fraud awareness; technology-based protection, identity management; and legal deterrence. These six key areas are mainly supported by four pillars: user; institution; network; and government and industry. However, credit card fraud prevention practice in Indonesia is still at a lower level of robustness than those in the benchmark countries. Deficiencies in the credit card fraud prevention practice in Indonesia are indicated, inter alia, by a lack of reliable fraud data collection, management and distribution mechanisms as well as a lack of effective and efficient identity management practice. Deficiencies and weaknesses in the system should be identified and action taken to make it more consistent with credit card fraud prevention practices of other countries.

INTRODUCTION

Over a decade, credit card fraud has been a major problem in the Indonesian payments system. In addition to being costly, the offence is believed to have been used to support other crimes such as terrorism. Efforts have been made to address this issue among which is by putting in place fraud prevention measures to diminish offenders’ crime opportunity. The discussions in this paper focus on highlighting the trends in credit card fraud and its prevention in the Indonesian payments system particularly in the period of 2003 - 2007. References are also made to such practices.

1 Author is the Director of the Centre for Forensic Accounting Studies at the Department of Accounting of the Islamic University of Indonesia. He obtained his Masters degree and PhD in Forensic Accounting from the University of Wollongong Australia.

2 Some events which occurred after 2007 are included in the discussions because they are related to or are part of the events which occur within the study’s time period.
in the US, the UK and Australia in building a framework of an ideal credit card fraud prevention structure for Indonesia.

**PREVALENCE AND COSTS**

Indonesian banks bear tens of billions of rupiahs of losses from credit card fraud every year (Kompas.com, 2008b). According to the Indonesia Credit Card Association (AKKI), during the period July 2003 to April 2006, 89 cases of credit card fraud occurred, with losses of $US4.6 million, of which, 82 cases were committed through a counterfeit card fraud scheme (that is, creating forged cards by using stolen information), and the rest involved application fraud (Alwie & Anthony, 2008). According to Mr Dodit Probojakti of AKKI, Indonesian banks recorded $US4.4 – $US5 million of losses from credit card fraud during 2007 (Kompas.com, 2008b).

According to Bank Indonesia (2007b, p. 30), application fraud and counterfeit card are the most common schemes of credit card fraud in the country. In terms of application fraud, Bank Indonesia believes that careless cardholder selection process is commonly the primary cause of credit cards falling into the wrong hands (cardholders with bad track records), which leads into the misuse of the cards (Bank Indonesia, 2007b, p. 30). As stated by Mr Dodit Probojakti of AKKI, the majority of counterfeit card fraud cases were in the form of credit cards issued by legitimate issuers being forged by criminal syndicates (Kompas.com, 2008b). This was largely because most (if not all) credit cards in Indonesia (at least until the issuance of Bank Indonesia Regulation Number 7/52/PBI/2005 Concerning the Operation of Card-Based Payment Instrument Activities) were magnetic stripe based (Bank Indonesia, 2007b, p. 30).

Financial loss from credit card fraud is not the only problem faced by the Indonesian payments system, because, according to Mr. Muhammad Helmi of AKKI, credit

---

3 A member of the AKKI executive board.
4 A member of the AKKI executive board.
5 Chairman of the AKKI of the time.
card fraud can also damage Indonesia’s image in the e-commerce world (Ridwan, 2005). This is evidenced by the fact that for the last few years, online merchants such as Amazon.com and eBay have put Indonesia on their list of ‘dangerous’ countries to make online transactions with. eBay, for example, has had many experiences of online credit card fraud offenders (carders) from Indonesia who made online transactions using unlawfully obtained credit card information (Sodikin, 2006b). Such designations diminish the benefits Indonesia could otherwise enjoy from the development of world e-commerce. Referring to the experience of Malaysia, Police Brigadier General Indradi Thanos of the Indonesian National Police at the seminar on credit card fraud in Bogor (15 April 2008) contends that should Indonesian be considered a credit card warning country, all credit card users are warned not to make transactions in the country that will impact negatively on banks and the industries within (Suara Karya Online, 2008).

**Table 1 Types of Credit Card Fraud in Indonesia**

<table>
<thead>
<tr>
<th>Using Credit Card</th>
<th>fraudulent application</th>
</tr>
</thead>
<tbody>
<tr>
<td>using real card</td>
<td>non-received card</td>
</tr>
<tr>
<td></td>
<td>lost/stolen card</td>
</tr>
<tr>
<td>using forged card</td>
<td>altered card (re-embossed/re-encoded)</td>
</tr>
<tr>
<td></td>
<td>totally counterfeit</td>
</tr>
<tr>
<td></td>
<td>white plastic card</td>
</tr>
<tr>
<td>Using Sales Drafts</td>
<td>record of charge (ROC) pumping</td>
</tr>
<tr>
<td></td>
<td>altered amount</td>
</tr>
<tr>
<td>Using Stolen Data</td>
<td>Skimming</td>
</tr>
</tbody>
</table>

---

6 Malaysia had previously been known as among the worst countries in the world for counterfeit card fraud. However, since the implementation of smart card technology, it has since been considered a very hostile environment for credit card fraud offenders. For example, according to the Visa Asia-Pacific’s Head of Payment Security Services, Mr Ingo Noka, at a conference on IT governance in Singapore (May 2006), Visa’s loss from counterfeit card fraud was approximately $US400,000 in November 2004. As at September 2005, there were no significant indications of counterfeit card fraud in Malaysia, and the country had already replaced its magnetic striped credit cards with chip-based cards in 2005 (Yeo, 2006).
<table>
<thead>
<tr>
<th>Other Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>wire tapping</td>
</tr>
<tr>
<td>inline tapping</td>
</tr>
<tr>
<td>mail, telepone and internet order</td>
</tr>
<tr>
<td>EDC modification</td>
</tr>
<tr>
<td>fictitious merchant</td>
</tr>
<tr>
<td>common purchase points (CPP)</td>
</tr>
<tr>
<td>credit card generator (CCG)</td>
</tr>
<tr>
<td>Ghost Phantom Terminal</td>
</tr>
</tbody>
</table>


In practice, categorising credit card fraud is often difficult, because of the complexity and the dynamics of the offence (e.g. one offence may involve multiple schemes). This creates challenges for law enforcers in investigating and prosecuting offences and offenders. This prompted the Indonesian Police, in cooperation with Bank Indonesia and other Indonesian banks and financial institutions to issue *The Field Manual for the Investigation of Credit Card Crime* (translated title)\(^7\). Based on this manual, four major classifications of credit card fraud in Indonesia exist using these modus operandi: using credit cards, using sales drafts, using stolen data and other methods (see Table 1) (Indonesian National Police, 1998, p. 14).

**PATTERN-SETTERS IN PREVENTION PRACTICES**

The Author, based on his PhD study on credit card fraud prevention practices in, among others, the United States, the United Kingdom and Australia\(^8\), argues that the basic structure of a good payments fraud prevention practice resembles a house with four pillars that support six key areas\(^9\) (Prabowo, 2010). Author dubbed such a

---


\(^8\) In his study, Prabowo (2010) analysed the trends in credit card fraud prevention practices in the United States, the United Kingdom, Australia and Indonesia. The ‘Four-Pillared House of Payments Fraud’ model was formulated based on the practices in the United States, the United Kingdom and Australia against which similar practices in Indonesia is evaluated.

\(^9\) This is also supported by Mr Dodit Probojakti of the AKKI in a discussion with author (Probojakti, 2008a). Mr Probojakti was of the opinion that generally, there are four pillars (three main pillars and one supporting pillar) within the credit card fraud prevention practices in Indonesia: customers, issuers, schemes and other stakeholders (e.g. regulators, consumer protection bodies and so on) (Probojakti, 2008a).
framework as ‘Four Pillared-House of Payments Fraud Prevention Practice’ (Prabowo, 2010).

![Figure 1 The Four-Pillared House of Payments Fraud Prevention Practice](Source: Prabowo (2010, p. 362)

A fieldwork conducted in Indonesia in 2008 for the study found that generally the same pattern applies to Indonesia, but with somewhat lesser robustness (see the following discussions).

The first key area is ‘understanding of the real problems’, in which fraud data collection, management and distribution is a major part. A discussion with Mr Dodit Probojakti of the Indonesia Credit Card Association (AKKI)\(^{10}\) suggests that day-to-day monitoring has been carried out by credit card issuers in Indonesia by various means (such as neural-based technology, for example, the Falcon system) to spot unusual transactions, as well as other procedures (such as ‘know your customer’\(^{11}\))

---

\(^{10}\) A member of the AKKI executive board.

\(^{11}\) As part of the efforts to circumvent the problems of money laundering, ‘know your customer’ (KYC) represents the obligation of financial institutions (e.g. banks and insurance companies) to record information about their customers, including ensuring the reliability of that information (Innovations Software Technology, 2009, p. 4).
that should provide cardholders and financial institutions with a degree of protection against fraud (Probojakti, 2008a).

Over the years, efforts to administer fraud data collection have been demonstrated by Bank Indonesia’s publishing of such data as part of its payments system annual reports. Additionally, the issuance of Bank Indonesia Regulation Number 7/52/PBI/2005 Concerning the Operation of Card-Based Payment Instrument Activities (e.g. Article 61) created an obligation for bank and non-bank financial institutions that operate card-based payment instruments to provide monthly fraud reports to Bank Indonesia (Bank Indonesia, 2005b, p. 43). However, author believes that the lack of technical explanation (e.g. how to categorise offences and calculate losses) may have affected the reliability of the data, because it may lead to different interpretations by different institutions. This was confirmed by Ms Ida Nuryanti of Bank Indonesia during a discussion with author (Nuryanti, 2008). Ms Nuryanti believes that reliable fraud data is of great importance for Bank Indonesia in formulating policies to regulate the credit card industry (Nuryanti, 2008). Bank Indonesia, since the issuance of Bank Indonesia Regulation Number 7/52/PBI/2005 Concerning the Operation of Card-Based Payment Instrument Activities, and recently, Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities, has published its card fraud statistics as part of its payments system annual reports. For examples of card fraud statistics, see Table 2, Table 3 and Table 4.

12 For examples, see Bank Indonesia (2007a, p. 142; 2007b, p. 30; 2008b, p. 30).
13 For the original text, see Bank Indonesia (2005b). The regulation was later on amended by Bank Indonesia Regulation Number 10/8/PBI/2008 on the Amendment on Bank Indonesia Regulation Number 7/52/PBI/2005 on Card-Based Payment Instrument Operation. In April 2009 Bank Indonesia issued Regulation Number 11/11/PBI/2009 concerning Operation of Card-Based Payment Instrument Activities as the new regulation on card-based payment instruments (Bank Indonesia, 2009b).
14 A senior legal analyst of Bank Indonesia.
15 Some publications exist of fraud data based on the data submitted by banks and other financial institutions to Bank Indonesia. Nevertheless, the author believes that the absence of regulations that create obligations to report fraud that can result in incompleteness of the submitted data would affect the reliability of the data in question.
Table 2 Card Fraud 2006

<table>
<thead>
<tr>
<th>Types of Fraud</th>
<th>Number of Incidents</th>
<th>Losses ($US)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeiting</td>
<td>5,267</td>
<td>2,783,440</td>
</tr>
<tr>
<td>Lost/Stolen</td>
<td>48,797</td>
<td>211,310</td>
</tr>
<tr>
<td>Card Not Received</td>
<td>369</td>
<td>124,630</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>748</td>
<td>483,120</td>
</tr>
<tr>
<td>Mail/Phone Order</td>
<td>643</td>
<td>45,540</td>
</tr>
<tr>
<td>Internet Transaction</td>
<td>451</td>
<td>6,930</td>
</tr>
<tr>
<td>Cash Advance</td>
<td>25</td>
<td>880</td>
</tr>
<tr>
<td>Application</td>
<td>252</td>
<td>173,910</td>
</tr>
<tr>
<td>Deception</td>
<td>161</td>
<td>90,860</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>44</td>
<td>8,250</td>
</tr>
<tr>
<td>Other</td>
<td>143</td>
<td>66,440</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>56,900</strong></td>
<td><strong>3,995,310</strong></td>
</tr>
</tbody>
</table>


Table 3 Card Fraud 2007

<table>
<thead>
<tr>
<th>Fraud</th>
<th>Percentage of Incidents (%)</th>
<th>Losses (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft</td>
<td>95.18</td>
<td>19.00</td>
</tr>
<tr>
<td>Card-Not-Received</td>
<td>2.71</td>
<td>1.25</td>
</tr>
<tr>
<td>Counterfeit Card</td>
<td>0.96</td>
<td>61.00</td>
</tr>
<tr>
<td>Deception</td>
<td>0.14</td>
<td>8.15</td>
</tr>
<tr>
<td>Application Fraud</td>
<td>0.06</td>
<td>9.07</td>
</tr>
<tr>
<td>Internet Fraud</td>
<td>0.03</td>
<td>0.01</td>
</tr>
<tr>
<td>Other</td>
<td>0.48</td>
<td>1.21</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>


Table 4 Card Fraud 2008 (Number of Identified Cases)

<table>
<thead>
<tr>
<th>Fraud Type</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeit</td>
<td>33</td>
<td>11</td>
</tr>
<tr>
<td>Fraud Applications</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Lost/Stolen</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>42</strong></td>
<td><strong>26</strong></td>
</tr>
</tbody>
</table>

The examples of card fraud statistics in Table 2, Table 3 and Table 4 were published as part of Bank Indonesia’s payments system annual reports for 2006, 2007 and 2008. The data are inconsistently arranged and presented in the reports, and essential information, such as descriptions of the categories of offences is lacking; therefore, the fraud data collection mechanisms still need to be improved, despite the currently existing regulations that obligates financial institutions to report any fraud incidents. Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities, has not made significant improvements to the mechanism of fraud data collection, management and distribution, as evidenced by, for example, the lack of clear guidance about how to calculate and categorise card fraud.

In comparison, the fraud data from the FTC, the APACS and the APCA are always presented in consistent and systematic ways that include descriptions about how and from whom the data were gathered, as well as the calculation methods (at least in general) and offence categorizations. Additionally, should inconsistencies ever occur (e.g. changes in data collection methods) explanation on the matter will be stated in the report16.

As mentioned above, the obligation to report fraud incidents to Bank Indonesia came into existence after the issuance of Bank Indonesia Regulation Number 7/52/PBI/2005 Concerning the Operation of Card-Based Payment Instrument Activities, and were later re-established under Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities. In Australia, for example, such an obligation is important in maintaining the completeness — and thus the reliability — of data and information on fraud. In the APCA’s fraud data collection mechanism, for example, all APCA member institutions automatically become fraud data sources, and are obligated to provide such data as required (Australian Payments Clearing Association, n.d.). Regardless,

16 For example, see Federal Trade Commission (2007a, p. 9) which explain changes in data collection method between the 2003 and 2006 identity theft survey reports.
the existence of the obligation to report fraud incidents does not in itself solve the problems of the lack of reliable data, because further technical guidance on how to perform such tasks is also of a high level of importance. The analysis of the relevant Bank Indonesia regulations and a discussion with Ms Ida Nuryanti\textsuperscript{17} of Bank Indonesia during the fieldwork both suggest that such technical guidance is yet to be developed to avoid misinterpretations in the data collection process in Indonesia.

Despite the existence of the central bank, an industry body such as the AKKI should support the ‘four-pillared house’ as part the fourth pillar, particularly by providing (or at least supporting) fraud data collection, management and distribution. As evidenced by the roles of the APCA in Australia, an industry body is in a strategic position to perform such a function, due to its relationship to the sources of fraud data and information (e.g. banks and non-bank financial institutions) (Prabowo, 2010).

Further inquiries into the performance of the AKKI suggest that, despite the fact that the institution has been in operation for years\textsuperscript{18} and has made major contributions to solving multiple credit card fraud cases, it could have performed better, had several internal problems been solved in the first place. A noticeable problem during the author’s visit to the AKKI office was that of the available human resources: only a handful of full-time staff, in addition to part-time managerial members, were in charge of running the institution. This was confirmed by Mr Dodit Probojakti of the AKKI in a discussion with the author (Probojakti, 2008b). Furthermore, as shown on its website (accessed on 24 April 2009), there were only two-full time staff in the AKKI’s organisational structure, and several unfilled positions.

According to Mr Probojakti, the limited financial resources is among the major problems in developing human resources at the AKKI, because the institution is generally funded by its members (Probojakti, 2008b). As for the AKKI’s statements in the mass media, particularly in relation to financial losses figures from credit card

\textsuperscript{17} A senior legal analyst of Bank Indonesia.
\textsuperscript{18} The AKKI was established in 1988 (Indonesia Credit Card Association, 2007a).
fraud incidents, Mr Probojakti states that such information were requested on a strictly confidential basis from credit card schemes (such as Visa and MasterCard), and were generally given in the forms of total figures only, thus limiting the author’s ability to conduct trend analyses on the data (Probojakti, 2008b).

Referring to the APCA’s *Payment Fraud Methodology Paper*, a payments system institution that conducts fraud data collection, management and distribution should consider certain important matters in performing this task, including data items and definition, scope and coverage, data reporting and timing, data processing and release (Australian Payments Clearing Association, n.d.). In terms of data items and definition, the APCA categories credit card fraud statistics into lost/stolen card, card never received, fraudulent application, counterfeit/skimming, card not present (CNP) and other (Australian Payments Clearing Association, n.d.). These categories have been defined and used consistently over the years. The scope and coverage of fraud data collection must be clearly defined regarding from whom the data are collected as well as the coverage thereof.

Data reporting and timing refers to the procedures regarding how data are reported and how timing issues impact on output from the collections (Australian Payments Clearing Association, n.d.). For example, APCA’s member institutions report credit and charge card fraud data as gross actual losses, and a three-month period after the end of reporting period is required for fraud to be discovered and all relevant details thereof acquired (Australian Payments Clearing Association, n.d.). For data processing, to maintain consistency and to avoid missing values and other faults that may impair the reliability of the data and information, each individual submission is checked by the APCA and, when necessary, respondents are contacted to verify and/or correct their data and information (Australian Payments Clearing Association, n.d.). Even after the data are aggregated (after they are received and checked) to produce final totals, the data series is still be checked for consistency (Australian Payments Clearing Association, n.d.). After the above matters are sorted out, the release of the statistics should also be arranged in a way that avoids (or at least
minimises) the lead and lag effects from timing differences in discovering, reporting and/or resolving fraud events (Australian Payments Clearing Association, n.d.). Over the years, the APCA’s statistics are also provided to institutions such as the Australian Federal Police and the Australian Crime Commission Australian Payments Clearing Association (Australian Payments Clearing Association, n.d.).

In terms of fraud prevention policy, several efforts have been made in Indonesia, particularly by Bank Indonesia as the central bank, to set a standard for fraud risk management especially regarding card-based payment instruments. This was achieved by the issuance of several regulations, such as Bank Indonesia Regulation Number 7/52/PBI/2005 Concerning the Operation of Card-Based Payment Instrument Activities (no longer in effect), Bank Indonesia Regulation Number 10/8/PBI/2008 Concerning the Amendment to Bank Indonesia Regulation Number 7/52/PBI/2005 Concerning Card-Based Payment Instrument Operation (no longer in effect) and Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities (currently in effect). Other central bank regulations that directly or indirectly contribute to the mitigation of fraud risks in the payments system include, but are not limited to:

- Bank Indonesia Regulation Number 3/10/PBI/2001 Concerning the Implementation of Know-Your-Customer Principles (Bank Indonesia, 2001a)
- Bank Indonesia Regulation Number 3/23/PBI/2001 Concerning the Amendment to Bank Indonesia Regulation Number 3/10/PBI/2001 Concerning the Application of Know-Your-Customer Principles (Bank Indonesia, 2001b)
- Bank Indonesia Regulation Number 5/21/PBI/2003 Concerning the Second Amendment to Bank Indonesia Regulation Number 3/10/PBI/2001 Concerning the Application of Know-Your-Customer Principles (Bank Indonesia, 2003)
• Bank Indonesia Regulation Number 9/15/PBI/2007 on Risk Management in the Use of Information Technology by Commercial Banks\textsuperscript{19} (Bank Indonesia, 2007c).

Such regulations, when implemented properly, should establish minimum standards for card fraud prevention activities, and may help to reduce offence displacement problems (e.g. target displacement), because all the supposedly potential victims are on the same level of difficulties to be victimised\textsuperscript{20}. According to Bank Indonesia Circular Letter Number 11/10/DASP Concerning Card Based-Payment Instrument Operations\textsuperscript{21}, in terms of card-based payment instrument security, an issuer has the obligation to prevent and minimise card fraud to preserve public trust (Bank Indonesia, 2009c, p. 34). Such an obligation covers the entire related technology infrastructures, including the security of the card security and the security of the entire system of card data processing (Bank Indonesia, 2009c, pp. 34-35).

For card security, Bank Indonesia has mandated the implementation of chip technology with the ability to store and/or to process data, so that various additional applications can be added for the sake of the security of transaction data processing (Bank Indonesia, 2009c, p. 34). The due date for the conversion to chip technology was 31 January 2009\textsuperscript{22} (Bank Indonesia, 2009c, pp. 35-36). In terms of data processing, this includes improvements on the security electronic data capture (EDC) devices as well as the supporting transaction processing system of the issuers, acquirers and/other third-party processors by providing hardware and systems that can process chip cards (Bank Indonesia, 2009c, pp. 34-35).

---

\textsuperscript{19} The regulation established that a bank has the obligation to report any critical events, abuses, and/or offences in the management of information technology that may or had already caused significant financial losses and/or disturbances on the operation of the bank (Bank Indonesia, 2007c).

\textsuperscript{20} The displacement theory proposes that diminishing crime opportunity to prevent crime will only move it around (New South Wales Attorney General’s Department, n.d.(a)).

\textsuperscript{21} A circular letter is generally issued to provide further explanations and guidance to the corresponding Bank Indonesia regulation.

\textsuperscript{22} The initial due date was the 31 December 2008 as stipulated by Bank Indonesia Regulation Number 7/52/PBI/2005 concerning Operation of Card-Based Payment Instrument Activities (Bank Indonesia, 2005a, p. 11). However, later, due to the difficulties experienced by the industry participants in preparing themselves for the migration, the date was changed to 31 December 2009 (Bank Indonesia, 2008a, pp. 41-42).
Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities (article 27.(3).a), as further explained by Bank Indonesia Circular Letter Number 11/10/DASP Concerning Card Based-Payment Instrument Operations, establishes that, despite all efforts to prevent card fraud, should fraud incidents occur, financial institutions are required to submit their reports to Bank Indonesia (Bank Indonesia, 2009b, p. 19; 2009c, pp. 50-60). As stipulated by Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities (elucidation, Article 15.(1)), issuers and acquirers (e.g. banks and non-bank financial institutions) must also be financially prepared to fulfil any future payment obligations arising from credit card fraud incidents (Bank Indonesia, 2009b, p. 9).

Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities set the standard for fraud risk management in credit card industry in Indonesia, among which is the use of the chip technology23. However, the experience of the credit card industry in the UK suggests that the Indonesian payments system should prepare for the possibility of offence displacements, where credit card fraud offenders no longer commit counterfeit card fraud but instead focus on other schemes such as card-not-present fraud and application fraud, or may even target other card-based payment instruments, such as the ATM card (Prabowo, 2010, pp. 200-370)24.

---

23 As explained by the Circular Letter No. 11/10/DASP concerning Card-Based Payment Instrument Operation (Bank Indonesia, 2009c, p. 34).

24 The author’s review on Bank Indonesia Regulation Number 11/11/PBI/2009 did not find any part of the regulation that creates an obligation for ATM card issuers to switch to smartcard (chip) technology. According to the acting Governor of Bank Indonesia, Mr Darmin Nasution, Bank Indonesia has not yet mandated the use of chips on ATM cards (Khoiriyah, 2010). Therefore, the magnetic stripe technology is still in use for this type of payments card that exposes cardholders to the higher risk of payments fraud. Responding to the seemingly increasing ATM skimming cases, Bank Indonesia, as stated in its 2010 Annual Report, mandated the National Payment System Communication Forum (FKSPN) to formulate a national standard for chip based – ATM/Debit cards in Indonesia (Bank Indonesia, 2011, p. 30). Technically, as agreed by the FKSPN, the formulation of such a standard is to be carried out by the Issuer Forum whose members are three switching companies: PT. Artajasa Pembayaran Electronis, PT Alto Network, and PT Rintis Sejahtera (Bank Indonesia, 2011, p. 30).
These issues highlight the need for more regulations on the fraud risk management, which in turn covers more areas, such as online credit card fraud transactions and ATM card fraud. In other words, future Bank Indonesia regulations on fraud risk management should cover more (if not all) areas of payments instruments to minimise crime opportunity in the payments system. Regulations on ‘what’ should be achieved in terms of fraud prevention should also be accompanied by clear guidelines on ‘how’ to achieve this. For example, as discussed above, Bank Indonesia should provide more explanations on how financial institutions should arrange their credit card fraud data before submitting them to the central bank to avoid confusion and misunderstanding. In Australia, for example, the APCA, in its Payment Fraud Statistics Methodology Paper, describes the procedures used consistently throughout the years and by which the periodic fraud statistics are constructed.

In terms of fraud awareness, several events such as seminars and training events have been held often as collaborations among institutions such as Bank Indonesia, the Indonesian National Police, the Indonesia Credit Card Association (AKKI) and commercial banks to enhance knowledge and understanding on the modus operandi, prevention measures and investigation techniques of credit card fraud in Indonesia. For example, a seminar on credit card fraud in the payments system was held on 16 December 2009 at the Postgraduate Study Program of STIE Perbanas Surabaya, whose speakers included Mr Mahmud (Head of Bank Indonesia, Surabaya Office), Mr Dodit Probojakti (a member of the AKKI executive board) and Mr Winang Budoyo (an economist from Bank CIMB Niaga) (STIE Perbanas Surabaya, 2009). The seminar was attended by banking practitioners, academics, students, police and credit card users, and aimed to enhance the knowledge of practitioners, students and credit card users on the modus operandi and prevention of credit card fraud (STIE Perbanas Surabaya, 2009).

The Work Group on Public Education on Banking (2007) states that many problems exist between the banking industry and society in banking operations. Among the causes of such problems is the lack of society’s knowledge about banking matters
Bank Indonesia has expressed its commitment to educating society on banking matters by launching the *Blueprint of Public Education on Banking* in 2007 (Sari, 2007). Among the matters covered by the *Blueprint* was the need to educate society about crimes related to banking products to prevent losses (Work Group on Public Education on Banking, 2007). In early 2008 Bank Indonesia initiated the Let’s Go to the Bank campaign to educate society on banking matters (Nopiansyah, 2008). 2008 was also named the Year of Banking Education (PerbanasNews, 2008, p. 2).

As evidenced by the various training events and seminars held for enhancing knowledge on the issues of credit card fraud and prevention, it appears that some understanding exists of the importance of fraud awareness in tackling credit card fraud in Indonesia. However, because many credit card fraud cases are technology-based crimes that evolve rapidly over time, such initiatives should be continuously carried out and improved frequently, particularly for cardholders, because many offences were successfully perpetrated by offenders because of customers’ ignorance and negligence. The massive ATM fraud in Indonesia in 2010 is an example. The offences were perpetrated in different areas in different provinces in Indonesia (e.g. Jakarta, Bali, East Kalimantan, West Kalimantan and Yogyakarta) in January 2010, and were believed to be perpetrated by organised criminals with estimated total losses of over $US2 million (Gatra, 2010). Although not specifically targeting credit cardholders, the fact that such offences were perpetrated by means of ‘classic’ modus operandi (such as attaching a skimming device and fake customer call centre number to an ATM machine and unlawfully installing a hidden camera) suggest the lack of customer awareness about the issues of payments fraud (Gatra, 2010; Prasetyo, 2010; Kompas.com, 2010).

In the US, improving society’s fraud awareness has been a major agenda, as determined by the countries’ national strategies, including *Combating Identity Theft*:

---

25 Because credit cards can also be used to withdraw funds from ATM machines (cash advances), credit cardholders who use magnetic stripe cards also bear the risk of being victimised by this scheme.
A Strategic Plan (US). The US FTC, for example, has undertaken various initiatives to implement the Strategic Plan, such as a public awareness campaign in December 2007 named Deter, Detect, Defend: AvoID Theft, as well as by means of websites, articles, brochures, speeches, public service announcements and interviews to reach a variety of audiences with a basic message that consumers should take simple steps to reduce the risk of identity theft (President's Identity Theft Task Force, 2008, pp. 17-18). In the UK, during the country’s migration to smartcard technology, the Chip and PIN program released publicly available materials for educational purposes, such as Get Ready for Chip and PIN (an implementation guide for businesses) (Chip and PIN, 2004a) and The Chip and PIN Guide: Remembering Your PIN (Chip and PIN, 2004b). Additionally, after the migration, to educate consumers about how to remember and use their Personal Identification Numbers (PINs) the ‘I♥PIN’ campaign was launched in October 2005 (Chip and PIN, 2005).

In terms of technology-based protection, as stated by Mr Dodit Probojakti of the AKKI, in a discussion with the author, every bank and non-bank financial institution that operates credit card system in Indonesia generally already has its own protection against fraud (Probojakti, 2008a). Recently, because chip technology is recognised worldwide as the best standard of card security, the Indonesian credit card industry has begun to embrace such technology to tackle credit card fraud, as stipulated by Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities, with a chip conversion due date of 31 December 2009 (Bank Indonesia, 2009c, pp. 35-36).

---

26 Recommendation 8 (Initiate a Multi-Year Public Awareness Campaign).
27 A member of the AKKI executive board.
28 According to the Deputy Director of the Directorate of Accounting and Payment System of Bank Indonesia, Mrs Yohana Fransiska Sri Suparni, The time needed for the delivery of the cards to the cardholders caused a few cardholders had not received their cards by 1 January 2010 and thus made the actual percentage of completion in the country’s migration to chip technology slightly less than 100 percent on that date (Warta Kota.co.id, 2010).
Table 5 Chip Card Implementation (December 2008)

<table>
<thead>
<tr>
<th>Issuer Groups</th>
<th>Number of Cards</th>
<th>Number of Chip Cards</th>
<th>% of Chip Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreign Banks</td>
<td>2,839,382</td>
<td>1,556,357</td>
<td>55</td>
</tr>
<tr>
<td>Joint Venture Banks</td>
<td>412,224</td>
<td>145,978</td>
<td>35</td>
</tr>
<tr>
<td>Private National Banks</td>
<td>4,200,747</td>
<td>2,434,972</td>
<td>58</td>
</tr>
<tr>
<td>Government Banks</td>
<td>2,781,607</td>
<td>253,092</td>
<td>9</td>
</tr>
<tr>
<td>Non-banks</td>
<td>1,051,370</td>
<td>299,084</td>
<td>28</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>11,285,330</strong></td>
<td><strong>4,689,483</strong></td>
<td><strong>42</strong></td>
</tr>
</tbody>
</table>

Source: Bank Indonesia (2009a, p. 49).

Table 6 EMV Compliant EDC\(^{29}\)(December 2008)

<table>
<thead>
<tr>
<th>Acquirer Groups</th>
<th>Total Number of EDC</th>
<th>Total EMV Compliant EDC</th>
<th>% of EMV Compliant EDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreign Banks</td>
<td>5,230</td>
<td>3,000</td>
<td>57</td>
</tr>
<tr>
<td>Private National Banks</td>
<td>110,058</td>
<td>87,530</td>
<td>80</td>
</tr>
<tr>
<td>Government Banks</td>
<td>58,683</td>
<td>15,830</td>
<td>27</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>173,971</strong></td>
<td><strong>106,360</strong></td>
<td><strong>61</strong></td>
</tr>
</tbody>
</table>

Source: Bank Indonesia (2009a, p. 50).

According to Mr Wawan Salum\(^{30}\), of ABN Amro, the migration from magnetic stripe-based card to chip-based card requires significant additional investment (Wibowo, 2006). Bank BNI for example, plans to spend $US120 million on card replacement from magnetic stripe-based to chip-based technology (Berita Sore, 2008). Bank Mandiri, as the largest state-owned bank in Indonesia, according to its Director of Consumers at the time, Mr Omar S. Anwar, would have to spend $US2.5 million for the conversion (Channel Magazine, 2008(b), p. 6). Bank Danamon has allocated approximately $US1 million for upgrading their cards to chip-based technology (Channel Magazine, 2008(b), p. 6).

The statistics in Table 5 and Table 6 suggest that industry participants in Indonesia believe that, despite the significant costs of establishing the chip system for fraud prevention, the cost savings from the reduction of fraud losses and other benefits will

---

\(^{29}\)Electronic data capture.

\(^{30}\)Head of consumer finance of ABN Amro of the time.
exceed them, at least in the long run. This was confirmed by Mr Probojakti\textsuperscript{31}, of AKKI, in a discussion with the author (Probojakti, 2008a). He believes that generally, credit card issuers already perceive the benefits of migration to chip-based cards as exceeding its costs, at least in the long run (Probojakti, 2008a). Further, according to Mr Probojakti, with chip-based cards, the issuers can have more benefits than just the decrease in their fraud losses (Probojakti, 2008a). Such benefits, according to Mr Probojakti, can be financial, such as the loyalty programs which can only be enjoyed by chip-based cardholders (Probojakti, 2008a).

Despite the seemingly easier reception of the smartcard technology in Indonesia compared to, for example, the US and Australia, referring to the experience of the UK, Indonesia may need to prepare itself against the possible adverse consequences thereof. For example, APACS fraud statistics indicate that soon after the conversion of credit cards in the UK into chip-based cards was completed, total losses from card fraud (debit and credit card) increased from $US823.6 million in 2003 to $US989 million in 2004 (Association for Payment Clearing Services, 2008b, p. 6). According to the APACS, in its press release of 8 March 2005, the increase was partly caused by offenders trying to seek and maximise new crime opportunities by focusing on card-not-present fraud schemes (Association for Payment Clearing Services, 2005). Therefore, the Indonesian payments system must prepare itself by strengthening other vulnerable areas that may be targeted by credit card fraud offenders after the implementation of the smart card technology in the country, for example, by strengthening online security in the country to anticipate the growth of card-not-present schemes. Additionally, and based on the UK’s experience, chip-based credit cards commonly still use magnetic stripes to anticipate the needs of cardholders travelling to other countries without (or with a slower pace of adoption of) smartcard technology (Everett, n.d.). On the other hand, to accommodate the need of overseas cardholders who still use magnetic stripe cards, magnetic electronic data captures (EDC) are still in use in Indonesia (Surya Online, 2009). Therefore, the risk remains of credit card fraud offenders stealing card data from magnetic stripes and using them

\textsuperscript{31} A member of the AKKI executive board.
to commit fraud in other countries that still accept magnetic stripe cards.\(^\text{32}\) (Association for Payment Clearing Services, 2008a).

The lack of effective identity management in Indonesia has always been a major problem in crime prevention, investigation and prosecution in the country. The ease of acquiring false or multiple identity documents for criminal purposes, for example, is evidenced by the many cases of serious crime in Indonesia, such as money laundering and corruption\(^\text{33}\). Mr Dodit Probojakti, of AKKI\(^\text{34}\), in a discussion with the author, stated that, in practice, credit card issuers have been using various means in their customer identification process, including the use of software, the implementation of the KYC principle, ID checking, audit trails, ‘matching and cross-check’ and field surveys (Probojakti, 2008a). Furthermore, as explained by Mr Probojakti, cooperation among issuers on fraud data and information sharing for background checking has also strengthened existing fraud prevention practices, particularly to ensure that credit cards are issued only to trusted people (Probojakti, 2008a). Finally, as stated by Mr Probojakti, even after an application is approved, issuers still monitor the use of the cards to look for any unusual transaction patterns that may indicate fraudulent activities (Probojakti, 2008a). However, Mr Probojakti also believes that despite these efforts, schemes such as credit card application fraud remains a serious threat, due to the lack of effectiveness in identity management in Indonesia, which allows credit card fraud offenders to obtain multiple identity

\(^{32}\) According to the Deputy Director of the Directorate of Accounting and Payment System of Bank Indonesia, Mrs Yohana Fransiska Sri Suparni, as of 1 January 2010, the magnetic stripes on Indonesian credit cards can no longer be used to make transactions. However, the EDCs can still recognise magnetic stripes from overseas cards and accept them (Surya Online, 2009).

\(^{33}\) The Head of the Directorate of Compliance and Supervisor of the Indonesian Financial Transaction Reports and Analysis Center (INTRAC), Mr Eddy Manindo Harahap, in a discussion with the author, suggested that false personal documents such as identity cards, are major obstacles in the investigations of many crimes in Indonesia (Harahap, 2008). According to Mr Harahap, whenever false identity was involved in a crime, it was generally very difficult to track down, let alone to prosecute, the offender (Harahap, 2008). This was also confirmed by the Supervisor of Asset Declaration Examiners of the Corruption Eradication Commission of Indonesia, Mr Najib Wahito, in a discussion with the author. Mr Wahito was of the opinion that, in many corruption cases, a common way to conceal illegitimate wealth is by having more than one identity with the same name, but different addresses (Wahito, 2008). In many cases of terrorism, it is also common for a terrorist to have more than one false identity card to distance themselves from the authorities (Adi, 2009).

\(^{34}\) A member of the AKKI executive board.
documents easily (Koran Jakarta, 2010). According to Mr Probojakti, on average, a credit card fraud offender has four ID cards (Koran Jakarta, 2010).

Several initiatives have been prepared to circumvent the problems of identity management in crime prevention, investigation and prosecution, among which is the development of the Single Identification Number (SIN) system in Indonesia (National Coordinating Commitee on the Prevention and Eradication of the Crime of Money Laundering, 2007, p. 15). The population administration by means of the SIN system is not a new concept. The US has been using this system in its social security numbers (SSNs) since 1935 (Lusmiarwan & Supangkat, 2005, p. 9). Originally created for tracking workers’ earnings, the SSN is now considered an important means of identification in the US (President’s Identity Theft Task Force, 2007, p. 23). President Susilo Bambang Yudhoyono, through his staff member, Mr Denny Indrayana, expressed his support for this plan, which is believed will benefit Indonesia in many ways, including crime prevention (Khumaini, SBY Desak SIN Segera Diwujudkan (Susilo Bambang Yudhoyono Urges SIN to be Realized), 2009).

Other areas of use of the SIN include police record, taxation, land administration and banking, which all require information on a person’s identity (Henricus & Siringoringo, 2009).

Explained by Lusmiarwan and Supangkat (2005, p. 11), the SIN is a unique identity integrated with a set of multiple data from different government and private institutions so it can be used by different institutions. It has the characteristics of being unique (no duplications exist), standardised (the same identity structure is used nationwide), complete (it has nationwide coverage), permanent (no changes of data occur) and integrated (Lusmiarwan & Supangkat, 2005, p. 11; Suharno, Leksono, & Kurniawan, 2004, p. 6). This means that ideally every citizen will have and use only one ‘single identity’ for a different range of needs, organisations and areas (Lusmiarwan & Supangkat, 2005, p. 12). The information heterogeneity and incompleteness in the identity management in Indonesia with lack of communication among organizations contributes to: inefficiency in data collection due to redundancy.
in the process; spatial nature of the information due to the lack of communication among organizations in maintaining and developing their data; and misunderstanding in interpreting data and information from the same object (Suharno, Leksono, & Kurniawan, 2004, p. 6).

The complexity of current identity management systems in Indonesia would make the centralisation process a very difficult and expensive task. The government plans to spend approximately $US737 million on this project, which will be supervised by the Corruption Eradication Commission of Indonesia (KPK) to avoid violations such as misuse of funds (Wardany, 2009). As stated by the KPK Deputy Chairman for Prevention, Mr M. Jasin, in accordance with the Law No. 23/2006 Concerning the Population Administration System, the Minister of Home Affairs has only five years after the law was enacted to bring the program into realisation (Wardany, 2009). In other words, despite slow progress to date, the SIN program must be finished by 2011 (Wardany, 2009). Despite the technical issues, Swastika (2009) argues that the private interests of institutions are a major cause why the SIN has not existed in Indonesia until now. This is because to establish the SIN system in Indonesia, process–based activities are needed that requires intensive and responsive cross-sectoral cooperation (Swastika, 2009). February 2011 marks the beginning of the nationwide implementation of a national ID system with citizenship numbers as part of the electronic identity cards or E-KTP (Prabowo, 2011). This centralized identity management system, supervised by the Home Ministry, is designed to be able to manage population data for multiple purposes under the same roof (Prabowo, 2011). The program is expected to be completed by 2012 (Khumaini, 2011).

---

35 For example, there are approximately 32 institutions that issue different identity numbers for documents such as ID cards, family cards, passports, driver’s licences, proof of vehicle ownership books (BPKB), birth certificates and electric bills, to name a few, and this often creates confusion (Swastika, 2009).

36 Shortly after the initiation of the E-KTP program, problems in the implementation of the system began to surface one of which is the seemingly lack of resources to complete the program within the predetermined time frame. For example, in the late July 2011 hundreds of E-KTP dedicated computers which were meant to be used for the operation of the program failed to be distributed to over 260 municipalities in Jakarta (Republika, 2011). The machines were initially scheduled to be received by 25 July 2011 but failed to be delivered accordingly (Republika, 2011).
An essential element in SIN system is the establishment of an integrated database of subjects (e.g. people and organization) and objects (e.g. land) (Suharno, Leksono, & Kurniawan, 2004, p. 9). With this database, data and information can be easily accessed, shared, and integrated with other systems. Other benefits include: cross-sectoral information exchange; more accurate information aspects such as social, economics, and environment of a country; ability for assessing income potential for taxation purpose; and removing unnecessary redundancy of information; to name a few (Suharno, Leksono, & Kurniawan, 2004, pp. 9-10).

The integrated database of the SIN system will make it very difficult for fraud offenders to obtain and use multiple and/or false identification documents to commit offences (e.g. for making fraudulent credit card applications). Additionally, should an offence be committed, the authorities may more easily track down and find offenders because all personally identifiable data will be centralised. However, in terms of crime opportunity, centralised identity management may reduce it in some areas, but increase it in others. This is so because the accumulated data within the database will be an attractive target for fraud attacks (London School of Economics, 2005, p. 187; Myhr, 2005, p. 22). Based on a study by the London School of Economics (LSE) on the UK’s national identity program, common factors that increase the security risk of a centralized identity management system include (London School of Economics, 2005, p. 188):

1. The scale and the complexity of the system
2. The number of users
3. The security sensitivity of data held on the system
4. Whether it has connections to other computer systems, especially untrusted ones
5. Whether it is connected to the Internet
6. Whether it is likely to be an attractive target for attack

Therefore, the system has to be very secure to prevent data theft and unauthorized modification and at the same time to protect citizens whose data are stored in the database (London School of Economics, 2005, p. 187). An identity management system should have mechanism to regulate matters such as: processing of personal
data; rights of the data subject; data sharing between administrations; and allowed use of the SIN (Otjacques, Hitzelberger, & Feltz, 2006, p. 7). In terms of processing of personal data, it should be clear as to whether or not and how the authority needs to be notified when personal data is to be processed (Otjacques, Hitzelberger, & Feltz, 2006, p. 5). Rights of data subject include: information and notification right; an access right; and a right to object (Otjacques, Hitzelberger, & Feltz, 2006, p. 6). Data sharing between administrations concerns transfer, sharing, interconnection and exchange of personal data between public agencies or administrative authorities by means of identifier (Otjacques, Hitzelberger, & Feltz, 2006, p. 6). In terms of allowed use of the SIN, a major concern has been its use by private institutions especially for internal needs (Otjacques, Hitzelberger, & Feltz, 2006, p. 6).

To support the development of the SIN system, on 30 January 2009, the Indonesian Automatic Fingerprint Identification System (INAFIS) was created by the Indonesian National Police and inaugurated by President Yudhoyono (Portal Nasional Republik Indonesia, 2009). The system will record data from every Indonesian citizen including newborn children (Portal Nasional Republik Indonesia, 2009). Every citizen will be given a card with chip in it which records the holder’s personal data (Portal Nasional Republik Indonesia, 2009). In supporting the national ID scheme, the fingerprint database will prevent redundancy in enrollment and thus prevent the ownership of multiple national IDs by a single person (Kristanti & Afrianti, 2009).

In terms of legal deterrence in payments fraud prevention practice in Indonesia, prior to the issuance of the Law No. 11/2008 on Electronic Information and Electronic Transactions, the prosecution of credit card fraud offenders is generally conducted using the Indonesian penal code, which the country inherited from the Dutch colonial period, and which is considered insufficient for tackling, in particular, technology-based offences (GLG Expert Contributor , 2008). For example, according to Mr

---

37 For the original text, see the Ministry of Communication and Information Technology of the Republic of Indonesia (2008).
Dodit Probojakti\textsuperscript{38} of the AKKI, the case of counterfeit card fraud perpetrated by Beny Wong, who received a five-year, eight-month jail sentence, was known at the time as the highest sentence ever for a credit card fraud case in Indonesia (Hukumonline.com, 2007). Previously, perpetrators of credit card fraud (such as Herry Komet in Bandung, Tan Wo Siang and Ripin Kasim in Jakarta and Chandra Halim in Surabaya) were sentenced to a maximum of four years in prison (Hukumonline.com, 2007). As stated by the Police Brigadier General Indradi Tanos of the Indonesian Police at the seminar on the law enforcement of credit card in Indonesia (15 April 2006), the weak legal sanctions, as found in the penal code, has made credit card fraud syndicates keep repeating their offences (Sebayang, 2008). Mr Mohamad Helmi of AKKI\textsuperscript{39} contends that the perpetrators of credit card fraud in Indonesia who were prosecuted by using the penal code would receive the maximum sanction of only five to six years of imprisonment; whereas in other countries (such as Malaysia, Singapore and Australia), the sanctions for the same offence are more severe (Ridwan, 2005).

According to the Police Great Commissioner Adjutant Dharma Pongrekun of the Indonesian National Police, regardless of the efforts made by the Indonesian National Police to counter credit card fraud, the relatively light sanctions for offenders has made Indonesia a safe haven for credit card fraud offenders (Hukumonline.com, 2004). Furthermore, as stated by Mr Pongrekun, indications exist that migrations of credit card offenders from Malaysia and Thailand to Indonesia have occurred due to this situation (Hukumonline.com, 2004).

The use of technology to support crime in Indonesia has created new challenges for the law enforcement institutions to conduct investigations into offences and prosecute offenders. A major city in Indonesia, Yogyakarta, for example, was known a few years ago as a haven for online credit card fraud offenders, as well being as among the worst places in the world for online credit card fraud. This was confirmed by the

\textsuperscript{38} AKKI risk management coordinator at the time; currently a member of the executive board of AKKI.

\textsuperscript{39} Chairman of AKKI at the time.
Police Commissioner Adjutant Tri Wiratmo of the Yogyakarta Provincial Police (Polda DIY), who had years of experience in the investigation of credit card fraud in Yogyakarta, in a discussion with the author (Wiratmo, 2008). According to Mr Wiratmo, among the major difficulties of the investigation and prosecution of online credit card fraud offences and online credit card fraud offenders are (Wiratmo, 2008):

- victims are often from different jurisdictions (that is, overseas)
- offenders are very difficult to track down and apprehend, due to their use of technology
- the law at the time had not yet regulated matters such as cybercrime and electronic evidences
- the complexity of the technology enabled crimes that required law enforcers to possess high level of skills and knowledge to conduct the investigations, which often created human resource problems.\(^{40}\)

Efforts have been made to circumvent such problems by, for example, establishing networks of cooperation with the international law enforcement agencies such as Interpol. According to Mr Wiratmo, even with such cooperation, inter-jurisdictional cases will still take a long time to solve (Wiratmo, 2008).

As mentioned above, a major effort made by the Indonesian government in mitigating the threats from technology supported crimes was the passing of the Law No. 11/2008 on Electronic Information and Electronic Transactions in April 2008.\(^ {41}\) According to Mr Mohammad Nuh\(^ {42}\), the law generally covers various aspects of the use of information and communication technology, including crimes within (Ministry of Communication and Information Technology of the Republic of Indonesia, 2008, p. v). Among the important matters regulated by this law is the use of electronic

\(^{40}\) This matter has been addressed by, for example, *The Field Manual Book of the Investigation of Credit Card Crime* and the training events conducted by institutions such as the AKKI and Bank Indonesia (see the above discussion).

\(^{41}\) See Ministry of Communication and Information Technology of the Republic of Indonesia (2008, p. 30).

\(^{42}\) Minister of communication and information technology at the time.
information and/or electronic documents as legitimate legal evidences as the expansion of legitimate legal evidence pursuant to the Law of Procedure (Article 5) (Ministry of Communication and Information Technology of the Republic of Indonesia, 2008, p. 7). With such matters already regulated within, the law has been fully supported by the Indonesian National Police, because previously, it was very difficult (if not impossible) to use electronic documents as evidence (Yanuarti, 2008). According to the Head of the IT and Cybercrime Unit of the Criminal Investigation Bureau (Bareskrim) of the Indonesian National Police, Police Grand Commissioner Petrus Reinhard Golose, the Law No. 11/2008 on Electronic Information and Electronic Transactions is the first ‘legal umbrella’ for law enforcers to tackle electronic crime in cyberspace, and is considered as an outstanding accomplishment (Yanuarti, 2008).

Mr Iwan Setiawan\(^{43}\) of Bank Indonesia, in a discussion with the author, explained that the Law No. 11/2008 on Electronic Information and Electronic Transactions has adopted several international regulations, guidance and practices, such as the UNCITRAL Model Law on Electronic Commerce 1996, the UNCITRAL Model Law on Electronic Signatures 2001 and the European Union’s Convention on Cyber Crime (ETS no. 185, 2001)\(^{44}\) (Setiawan, 2008).

In terms of legal deterrence, the Law No. 11/2008 on Electronic Information and Electronic Transactions imposes higher sanctions, particularly for credit card fraud offenders in terms of jail sentences and fines, which can strengthen the area of legal deterrence. This was confirmed by Mr Dodit Probojakti\(^{45}\) and Mr Ferry Tupanno\(^{46}\), both of AKKI, in a discussion with the author (Probojakti, 2008a; Tupanno, 2008a). According to Mr Probojakti, before 2004, the average jail sentence for credit card fraud offender was approximately one year, and later on became 2.5 years after 2004, with the case of Beny Wong in Bali receiving the highest sentence (five years, eight

\(^{43}\) IT senior system analyst of Bank Indonesia.
\(^{45}\) A member of the executive board of the AKKI.
\(^{46}\) Risk management coordinator of the AKKI.
months) (Probojakti, 2008a). With the maximum of 12 years of imprisonment, the Law No. 11/2008 on Electronic Information and Electronic Transactions is expected to have a better deterrence effect than previous laws.

Despite the numerous criticisms of the Law No. 11/2008 on Electronic Information and Electronic Transactions (for examples, the use of misleading definitions and overly severe sanction)\(^{47}\), all focus on its substance, but do not criticise its existence. Basically, the law itself represents the state’s efforts to fulfil its responsibility to provide maximum protection for information and communication technology utilisation in the Indonesia (Ministry of Communication and Information Technology of the Republic of Indonesia, 2008, p. v).

The existence of cyberlaw in Indonesia to provide sufficient legal deterrence will not be a significant contribution for the payments fraud prevention practice, should law enforcers not be equipped with sufficient skills and experience to conduct investigations and bring offenders to the courts (Elly, 2008). As previously mentioned, the limited human resources for tackling technology-based crimes has always been a major problem for the Indonesian National Police. This is because offenders often possess extensive knowledge of information and communication technology, surpassing those of law enforcers (Elly, 2008). An Indonesian telecommunication and informatics expert, Mr Roy Suryo, states that during 2008, in 32 Provincial Police (Polda) offices, only approximately 12 had cybercrime units, and that this suggests the need for more personnel with sufficient knowledge on technology-related crimes (Lobo, 2008; Suara Pembaruan Daily, 2008). According to the Head of Unit V IT and Cybercrime of the Criminal Investigation Bureau (Bareskrim) of the Indonesian National Police, Police Grand Commissioner Petrus Reinhard Golose, despite the enormity of the problem, the Indonesian National Police as law enforcer is not yet prepared to handle cybercrime cases (Kompas.com, 2008a). Further, Mr Golose states that handling cybercrime cases depends heavily on improving human resources within the police institution itself (Kompas.com, 2008a).

\(^{47}\) For examples, see Effendi (n.d.) and Kompas.com (2009).
According to Mr Golose, this matter not only concerns having police officers who know about using computer, but is also about how to ‘create’ police officers who are capable of investigating computer-related crimes (Kompas.com, 2008a). For this, Mr Golose recommends having special education on cyberspace and the use of computer hardware and software in cybercrime investigations in the Indonesian Police Academy, police school and the Police Science University (Kompas.com, 2008a).

Referring to the experience of the US, such problems are common and will always be encountered by law enforcers in investigating technology-enabled crimes. One of the President’s Identity Theft Task Force’s recommendations in its Strategic Plan is to ‘Enhance training for law enforcement officers and prosecutors’ (Recommendation 30) (President's Identity Theft Task Force, 2008, p. 46). The increase in the number of regional identity theft seminars as well as the review on the curricula for the education and training of federal agencies’ officers are examples of responses to this recommendation (President's Identity Theft Task Force, 2008, pp. 46-47). Referring to the experience of the UK, establishing special units, task forces, or networks to mitigate the threats of payments fraud should also strengthen the area of legal deterrence in payments fraud prevention practices. For example, the Dedicated Cheque and Plastic Crime Unit (DCPCU) was established in 2002 to tackle organised criminal networks that commit cheque and plastic card fraud in the UK, and is supported by investigators from various institutions such as the Metropolitan Police Service (MPS), the City of London Police (CoLP) and civilian investigators (National Fraud Strategic Authority, 2009b, p. 51; Dedicated Cheque and Plastic Crime Unit, n.d.).

Success in the above key areas requires the roles of users, institutions, networks and government and industry as the four ‘pillars’ of the payments fraud prevention. Customers, as part of the user group, can participate in training events and seminars held to improve their awareness on the current fraud issues, which should encourage cautious behaviour when using credit cards and thus provide fewer crime opportunities for offenders. By reporting fraud incidents to their financial institutions
as soon as they occur, customers can also support fraud data collection, management and distribution as part of the efforts to understand the real problems.

Financial institutions, as part of the institution group in the four pillars, can contribute to the above recommendations by allocating resources to acquire the latest credit card fraud prevention technology, conducting customer education programs and becoming part of the fraud data collection, management and distribution process in the country. Credit card associations, as part of the network group, can establish rules of operation for the network participants, including security standards within (e.g. EMV for smart cards and PCI DSS for online transactions), as well as contribute to the fraud data collection, management and distribution process.

In the fourth group, government and industry, Bank Indonesia, as the central bank, in fulfilling its responsibility to promote safety and efficiency in the payments system, can formulate regulations on fraud risk management for the Indonesian credit card industry. Institutions such as the Indonesian National Police are in a position to support credit card fraud prevention in Indonesia by creating deterrents to discourage offenders or potential offenders from committing offences.

The Author believes that the ‘four pillars’ can be strengthened further by advancing the roles of the credit card industry body, the Indonesia Credit Card Association (AKKI). In Australia, for example, the Australian Payments Clearing Association (APCA) has been part of that country’s efforts to mitigate the threats of payments fraud by, for example, continuous monitoring of the trends thereof.

---


49 In the Indonesian payment system, the Indonesia Credit Card Association (AKKI) has been known as the country’s premier credit card industry body, whose primary objectives include (Indonesia Credit Card Association, 2007b):
   - bridging banks and financial institutions that issue credit cards with other parties that are committed to the development of healthy credit card industry
   - supporting the investigation of credit card fraud by providing expert witnesses from the industry practitioners, as well as from the representations of international credit card schemes such as MasterCard and Visa International.
Payments Clearing Association, 2009, p. 3). As the Australia’s payments industry self-regulatory organisation, the APCA has been a major source of payments fraud data and information in Australia, which supports payments fraud prevention in the country. As stated by the APCA (2009, p. 7):

APCA believes that effective systematic prevention is greatly assisted by reliable statistical information about levels of fraudulent activity. …In simple terms, what gets measured, gets managed.

Over the years, discussions have emerged about establishing similar self-regulatory organisation in Indonesia to represent the adoption of self-regulatory system in the country.50 Such a plan has been mentioned by Bank Indonesia in its payments system annual reports (2007 and 2008) (Bank Indonesia, 2008b, pp. 39-66; 2009a, pp. 24-42). Bank Indonesia (2008b, p. 39) contends that the primary objective of the establishment of a credit card industry self-regulatory organisation (SRO) is to allow the industry to decide on its own rules and standards for small and technical matters, on its own. Further, according to Bank Indonesia (2008b, p. 66), the commitment to establish a payments system SRO forms part of the efforts to improve the roles of the stakeholders in the development of payments systems based on market need.

According to Bank Indonesia (2008b, p. 66), by implementing a self-regulatory system, a central bank can focus on macro regulation; whereas the area of micro and technical regulation is covered by the SRO. For example, because Bank Indonesia

50 Mr Dodit Probojakti of the AKKI, in a discussion with the author, was of the opinion that among the first priorities in developing the Indonesian credit card industry in particular, and the Indonesian payments system in general, is the adoption of the self-regulatory system by establishing a self-regulatory organisation (SRO) (Probojakti, 2008a). Further, Mr Probojakti believed that the AKKI is a good candidate to be upgraded into a self-regulatory organisation that will grant the institution several powers to regulate itself (e.g. deciding rules for the credit card industry, such as those related to minimum payment, non-performing loan (NPL) calculation and merchant certification) (Probojakti, 2008a). This was also confirmed by Mr Ferry Tupanno, in a discussion with the author (Tupanno, 2008a). Mr Tupanno stated that in its current state, the AKKI generally has no binding rules, and this causes difficulties, particularly for decision-making process as well as collecting fraud data from its members — despite the available database tools (Tupanno, 2008a). Additionally, Mr Harrold Abraham Gaspersz of the AKKI, in a discussion with the author, suggested that not all credit card fraud cases are addressed by the AKKI, only those of significant value (Gaspersz, 2008b).
Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities does not provide clear technical guidance on the mechanism of fraud data collection, management and distribution, an SRO can fill this gap by setting up such a mechanism to promote the reliability of the generated information. Alternatively, and just as with the case of the APCA\textsuperscript{51}, a future SRO could coordinate the collection of fraud data from its members to be submitted later on to the central bank, as well as to other relevant law enforcement institutions. For this purpose, a future SRO may need to consider establishing an equivalent of the APCA’s fraud committee\textsuperscript{52} to administer the process. Therefore, the formulated rules and standards could promote and maintain the security of the credit card instrument as well as maintaining healthy and efficient competition in the market (Bank Indonesia, 2008b, p. 39). In December 2007 the agreement between the card issuers who were also AKKI members to form an SRO was signed\textsuperscript{53,54} (Bank Indonesia, 2008b, p. 39). Finally, on 20 October 2010, facilitated by Bank Indonesia, a Self Regulatory Organization, the Payment System Association of Indonesia (ASPI) was formed by various banking organizations such as the Indonesia Credit Card Association (AKKI), the Foreign Bank Association of Indonesia, the Indonesian Banks Association (Perbanas) and the Indonesian Sharia Bank Association (Asbisindo) (Bank Indonesia, 2011, p. 35). The ASPI was legalized on 11 November 2010 (Bank Indonesia, 2011, p. 35).

\textsuperscript{51}See Australian Payments Clearing Association (n.d.).

\textsuperscript{52}The APCA’s fraud committee holds a meeting every calendar quarter to monitor the trends in payments fraud in Australia, as well as developing the most appropriate countermeasures based on, among other things, the collected fraud data and information (Australian Payments Clearing Association, n.d.).

\textsuperscript{53}Confirmed by Mr Ferry Tupanno, in a discussion with the author (Tupanno, 2008b). However, as implied in the author’s discussion with Mr Dodit Probojakti of the AKKI, the conflicts of interests occur because many of the AKKI’s professional staff are also employed by other institutions as members of their institutions’ top management level, has made the SRO establishment process progress somewhat slower than expected (Probojakti, 2008a).

\textsuperscript{54}Finally, on 20 October 2010, facilitated by Bank Indonesia, a Self Regulatory Organization, the Payment System Association of Indonesia (ASPI) was formed by various banking organizations such as the Indonesia Credit Card Association (AKKI), the Foreign Bank Association of Indonesia, the Indonesian Banks Association (Perbanas) and the Indonesian Sharia Bank Association (Asbisindo) (Bank Indonesia, 2011, p. 35). The ASPI was legalized on 11 November 2010 (Bank Indonesia, 2011, p. 35).
In terms of payments fraud prevention in Indonesia, theoretically, with greater understanding of the actual problems, a self-regulatory organisation should be able to allocate the existing resources more effectively to design and implement the most appropriate fraud prevention strategy. According to Dr. Brad Pragnell of the APCA in a discussion with author, in an SRO, the parties who make the decisions would also be those who would bear the consequences (e.g. financial costs) thereof (Pragnell, 2010). Therefore, their decisions related to payments fraud prevention should be effective as well as efficient. However, in practice, the nature of a self-regulatory organisation may also create some challenges in achieving its objectives, including those of fraud prevention.

The strengths and weaknesses of a self-regulation system has been the subject of many studies in various disciplines. As defined by Nunez (2007, p. 210):

As the name suggests, self-regulation is essentially a scheme whereby the enforcement of quality is delegated to the suppliers. The whole rationale for self-regulation rests on the notion that suppliers must somehow form an organization (namely a Self-Regulatory Organization (SRO)) in order to monitor the quality provided by its members and disclose evidence of malpractice and product failure to consumers.

Whereas the system itself is considered to be a means to improve performance at lower costs more quickly than traditional command-and-control regulation, evidence such as the collapse of Enron and WorldCom, suggest the need for greater government intervention (Sullivan, 2002, p. 91). The major challenges in operating a self-regulatory organisation (SRO) are often related to how to manage various interests within so as to avoid (or at least minimise) the conflicts thereof. The ICPACE, in its guideline, the Principles of Payments Industry Self-Governance, formulates five principles that characterise a sound self-governance framework for a

---

55 For examples, see Sullivan (2002); Hilary and Lennox (2005); Cunningham and Harris (2006); Lenox (2006); Lenox and Nash (2003); and King and Lenox (2000).

56 The issues of self-regulation in the Enron case centre on the roles of external auditors (Arthur Andersen, LLP) who was unlawfully supporting the misleading accounting practices within the company. Many believed this failure highlighted the need for reforming the accounting industry’s self-regulation — at least in the US. See Vinten (2002); Sullivan (2002); and Hilary and Lennox (2005).

57 According to the Head of Industry Policy of the APACA), Dr Brad Pragnell, in a discussion with the author.

Regarding fraud prevention, the author believes that a major role of a self-regulatory organisation (SRO) is to set the standards of security for its members, for example, by policies or regulations to mandate the use of a certain fraud prevention measure for credit card transaction. However, this would present the SRO with the challenge of ensuring the compliance of its members to the standards. Lenox and Nash (2003, p. 353), referring to the experiences of four US trade associations58, contends that the failure of an SRO in ensuring the compliance of its members will contribute to the failure of the institution in achieving its objectives. Members’ compliance can be achieved by a variety of means, among which are explicit sanctions (Lenox & Nash, 2003, p. 343; King & Lenox, 2000, p. 713). However, sanctions are better administered by independent parties so as to avoid conflicts of interest, because an SRO can be limited in some ways, such as simply because it is ultimately governed by its members (King & Lenox, 2000, p. 713). These also suggest the need to have in place a sound mechanism for monitoring compliance (Lenox & Nash, 2003, p. 354).

RECOMMENDATIONS
In summary, from the above discussions about the ‘four-pillared house’ framework perspective, various efforts have been made, particularly in the Indonesian payments system, involving four key groups (user, institution, network and government and industry) to support the six key areas of payments fraud prevention: understanding the real problems, fraud prevention policy, fraud awareness, technology-based protection, identity management and legal deterrence. In each of these key areas, this study has identified at least one event or measure as a trendsetter, and this has formed the focus of discussions. The following sections examine proposed future improvements for the six key areas, based on the above discussions and the practices in the benchmark countries.

---

58 The American Chemistry Council (ACCC), the National Association of Chemical Distributors (NACD), the American Textile Manufacturers Institute (ATMI) and the American Forest and Paper Association (AFPA).
Understanding the Real Problems

Although some efforts have been made, particularly by Bank Indonesia, to gather, manage and disseminate payments fraud data from the victim side (e.g. from consumers’ complaints) by, for example, creating obligations for financial institutions to report any fraud incidents to the central bank, more should be done to improve the reliability of the information generated from such a mechanism. This includes creating clear guidelines on how to record, calculate and report fraud incidents to the central bank. Such guidelines must address matters such as data items and definition, scope and coverage, data reporting and timing, data processing and release (see the above discussions).

To support these procedures, the establishment of a special database such as that of the FTC’s Identity Theft Data Clearinghouse is worthy of consideration, at least in the future, Expanding data sources to include more than just victims (e.g. offender data) should also add to the reliability of the information. Parties from the Indonesian criminal justice system (e.g. Indonesian police and prosecutors) who handle the investigation of offenders might effectively collaborate with, for example, parties from the payment system (e.g. Bank Indonesia and the commercial banks) which handle the complaints from victims to synchronise their data from both sides (victim and offender) to construct a more complete picture on the actual fraud problems that need to be solved. Just as in the US, the UK and Australia, where various institutions use the fraud data from the FTC, the APACS and the APCA to support their crime prevention, investigation and prosecution efforts, institutions in Indonesia may also gain benefit from using reliable fraud data, at least from the victim side, as a basis for their decision-making processes. However, due to the sensitive nature of the data, the mechanism of fraud data collection, management and distribution must be arranged in a way that balances promoting transparency and maintaining confidentiality.
Fraud Prevention Policy

Bank Indonesia Regulation Number 11/11/PBI/2009 Concerning the Operation of Card-Based Payment Instrument Activities mandates participants in credit card networks (e.g. issuers, acquirers and associations) to promote safety in their systems (Bank Indonesia, 2009b, pp. 6-21). Among the matters governed by the regulation is the use of chip technology on credit cards, which is understandably important, considering the fact that counterfeit card fraud is one of the most common types of credit card fraud in Indonesia, because the country was previously still relying on magnetic stripe technology.

However, because counterfeit card fraud is not the only types of credit card fraud and that offenders will tend to shift their offences to other vulnerable areas (e.g. other targets or by using other methods, such as what occurred in the UK), this study believes that Bank Indonesia needs to seriously consider advancing its regulations to cover more areas, so that the benefits of the implementation of the chip technology will not be offset by the increase of losses from other fraud schemes (e.g. card-not-present and application fraud). Despite the high investment required, mandating financial institutions to comply with the online security standards of the Payment Card Industry Security Standard Council (PCI SSC), at least in the future, may help to reduce offenders’ crime opportunities by limiting the options for displacements. Alternatively, Bank Indonesia may require the industry to use and develop online fraud measures such as Verified by Visa, MasterCard SecureCode, address verification services (AVS) and card verification numbers (CVNs), to name a few.

To anticipate the possibility that offenders will also shift their offences to application fraud, Bank Indonesia may also take advantage of the future Single Identification Number (SIN) system in Indonesia, which should limit offenders’ ability to obtain multiple and/or false identity documents for credit card applications. Therefore, this

---

59 Accompanied by the Circular Letter No. 11/10/DASP concerning Card-Based Payment Instrument Operation that provides explanatory information.
study suggests that when the SIN system is up and running, Bank Indonesia (or any other relevant institution) should consider formulating a specific regulation on the credit card application process to ensure that the applicants are really who they say they are. In Australia, for example, such a procedure is part of the 100-point identification system, which requires any individual who wishes to open an account to provide multiple independent sources of identification (Smith, 1998, p. 4). Such procedures will make the Indonesian payments system a particularly hostile environment for credit card fraud application offenders. Finally, to support fraud data collection, management and distribution, Bank Indonesia, in its regulations, may provide clear technical explanations about how to comply with the fraud reporting requirements.

**Fraud Awareness**

Despite a range of initiatives, such as training events and seminars on credit card fraud and other current issues, more should be done to enhance society’s awareness on the issues of credit card fraud and credit card fraud prevention in Indonesia. Due to the rapidly evolving nature of technology-enabled crime, more intensive and extensive education on credit card fraud prevention is needed in Indonesia to educate society. For example, due to the recent chip conversion (1 January 2010) in the country, some members of society may still need to be educated on the strengths and weaknesses of the new system, because, for example, although the chip technology can tackle counterfeit card fraud, it provides less (if not no) protection against card-not-present fraud such as online credit card fraud (Prabowo, 2010). Therefore, consumers need to be made aware of the other security options, such as 3D secure technology (e.g. Verified by Visa and MasterCard SecureCode) when making transactions online. As practised in the benchmark countries, a range of means of education, such as seminars, training events, workshops, educational websites with online materials, advertisements, brochures and pamphlets, to name a few, can be employed to educate the society. An aware society will ‘unwillingly’ provide less crime opportunity for credit card fraud offenders.
Technology-Based Protection

In terms of technology-based protection, smartcard technology is the recent trendsetter in Indonesia. As of 1 January 2010, all credit cards in Indonesia have been equipped with chips (Bank Indonesia, 2009c, pp. 35-36). However, as suggested by the above recommendation on the area of fraud prevention policy employing a particular technology to reduce crime opportunity in a particular area may contribute to offenders shifting their offences to other, more vulnerable areas. To prevent this, the Indonesian credit card industry should also work on strengthening its defence against other credit card fraud schemes, such as card-not-present and application fraud. For card-not-present fraud, referring to the experience of the US and the UK as depicted by CyberSource’s annual studies\textsuperscript{60}, various online security measures such as address verification services (AVS), card verification numbers (CVNs), IP geolocation information, Verified by Visa and MasterCard SecureCode have been employed to tackle online credit card fraud. In the US, the PCI Data Security Standard for online transaction security has gained favourable reception. For example, approximately 95 per cent of large Visa merchants already comply with the standard (Visa U.S.A., 2009). For application fraud, as mentioned above, in relation to the future establishment of the Single Identification Number (SIN) in Indonesia, the Indonesian credit card industry might establish and develop systems or applications that can be used in conjunction with the SIN system to verify applicants’ identity to protect itself from identity-related fraud. In principle, in terms of technology, what the credit card industry must do to protect its customers is to plug as many loopholes as possible to minimise (if not eliminate) credit card offenders’ opportunities to commit their offences in Indonesia.

Identity Management

As stipulated by the Law No. 23/2006 Concerning the Population Administration System, by 2011, the Single Identification Number (SIN) system is scheduled for operation in Indonesia (Wardany, 2009). Although the complete application of the system is yet to be seen, basically, should this system be already up and running,

\textsuperscript{60} For examples, see CyberSource (2008, p. 6) and CyberSource UK (2008, p. 11).
identity management in Indonesia will be more centralised than before. This will bring benefits, among which is the difficulty for credit card fraud offenders to obtain multiple and/or false documents for fraudulent purposes. However, based on the experience of the UK’s National Identity Scheme, being too excessive in implementing centralized identity management within a country will result in more problems than benefits for the society (Prabowo, 2010). Among the major drawbacks of an excessively centralized identity management system is the fact damages from data breaches will be more severe compared to those of a less centralized system. Furthermore, society may perceive the system as a form of surveillance and is a threat to their privacy which in turn will result in the resistance to the system itself. It is of outmost importance that the Indonesian government considers establishing a sound mechanism (e.g. by policy or technology) to control the use of the SINs by institutions to avoid unnecessary use that may increase the risk of identity theft. Above all, Indonesian government should carefully assess how far the centralization will go so as to avoid having too many problems in the future.

**Legal Deterrence**

The first Indonesian cyberlaw, the Law No. 11/2008 on Electronic Information and Electronic Transactions, has strengthened the area of legal deterrence in Indonesia, particularly that related to credit card fraud in the form of higher sanctions for offenders. In other words, the law now supports Indonesian law enforcers in investigating credit card fraud offences as well as prosecuting offenders. Therefore, the next important step is to enhance the knowledge and skills of law enforcers to be able to enforce the law effectively. To achieve this, proactive efforts to educate law enforcers should be undertaken, including reviewing the curricula of the law enforcement education institutions as well as conducting training and seminars for law enforcers. Cooperation with industry practitioners may also support such efforts. For example, industry experts may share their fraud data to be used to educate the law enforcers. The existence of both effective law on technology-related crimes and effective law enforcers with extensive knowledge and skills in the investigation and
prosecution of such crimes will discourage offenders from committing their offences in Indonesia.

**Strengthening the Pillars**

As discussed above, among the future plans to promote the safety and efficiency in the Indonesian payments system is the establishment of a credit card industry self-regulatory organisation (SRO). As a payments system SRO, ASPI is expected to support the Indonesian payments system by, among other things, deciding on the most effective and efficient ways to achieve the objectives set by the government. Nevertheless, the operation of ASPI particularly for the credit card industry in Indonesia must be carefully planned, including the targeted objectives to be achieved as well as means (e.g. regulations and policies) to achieve them. To ensure the achievement of the objectives, mechanisms to ensure the compliance of members must also exist, which may include explicit sanctions as well as sound monitoring processes. Additionally, the Indonesian government must always monitor the progress of the self-regulation system so as to decide properly the time when intervention is needed and how far the intervention should go.

To further strengthen the four ‘pillars’ of payments fraud prevention in Indonesia, referring to the experience of the US and the UK, where payments fraud level is relatively high compared to Australia, the establishment of a special task force to coordinate the available resources in circumventing fraud problems is worthy of consideration. For example, the President’s Identity Theft Task Force was established in May 2006 to coordinate federal agencies in the US in combating identity theft and was charged with creating a strategic plan for such a purpose (Finklea, 2009, p. 5). Similarly, in the UK, the National Fraud Strategic Authority (NFSA) was established in October 2008 as an executive agency of the Attorney General’s Office to protect the economy from fraud through the creation of a more hostile environment for offenders (National Fraud Strategic Authority, 2008). Establishing a special task force for tackling a serious crime is not a new matter in Indonesia, because previously, the country had already established the Corruption Eradication
Commission of Indonesia (KPK) for combating corruption, and the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) for circumventing money laundering.

CONCLUSION

Over the years, Indonesia has allocated resources to counter the growing problem of credit card fraud. This includes the six key areas of payments fraud prevention: understanding the real problems, fraud prevention policy, fraud awareness, technology-based protection, identity management and legal deterrence. Due to the growing threat of credit card fraud, particularly that caused by offenders shifting offences to Indonesia from other countries that have already strengthened their defences, recent efforts to protect consumers from fraud have been intensified, particularly in the six key areas: understanding the real problems, fraud prevention policy, fraud awareness, technology-based protection, identity management and legal deterrence (Prabowo, 2010).

Major prevention measures in these areas include: publication of fraud data by Bank Indonesia, formulation of fraud risk management policy by Bank Indonesia, seminars and training events about credit card fraud and prevention, implementation of the chip technology, development of the Single Identification Number (SIN) and the enactment of Law No. 11/2008 on Electronic Information and Electronic Transactions. Additionally, as part of the efforts to strengthen in particular the fourth pillar (government and industry) of the payments fraud prevention, a credit card industry SRO is planned to be established in the near future. All these efforts will at least reduce crime opportunity for credit card fraud offenders such as by increasing consumer awareness and thus improving their resistance to fraud attacks. Additionally, technology-based protection such as smartcard makes it more difficult for offenders in committing offences such as counterfeit card fraud. Consumers’ higher resistance means that they will be less suitable as fraud targets. Additionally, measures such as smartcard technology will make stolen credit cards valueless as it will be very difficult to use them for fraudulent purposes due to the encryption
technology within. Similarly, with more robust identity management system, application fraud becomes very difficult to commit.

Each measure has its strengths as well as weaknesses in protecting Indonesia from credit card fraud in particular, and payments fraud in general. Generally, future improvements for credit card fraud prevention in Indonesia include: improving the reliability of fraud data collection and dissemination, designing better fraud prevention policy which can establish a standard of sound credit card fraud prevention practice, implementing additional technology which can increase the difficulty of offenders in committing their offences online and offline, developing a balanced identity management system and improving the skills of law enforcement personnel to uphold the new law on information and communication technology. Continuous improvements must always be kept in motion to cope with the rapidly changing environment that may include the introduction of new prevention measures or improvements on existing ones.

Nevertheless, in implementing the above initiatives, considerations need to be made on the costs and benefits thereof. The Single Identification Number (SIN), for example, when applied excessively will result in more disadvantages than benefits to the society (Prabowo, 2010). The same applies to other measures such as the smartcard technology which requires substantial investments by banks and financial institutions to make it up and running. In principle, the desired end results from credit card fraud prevention practices in the payments system is that the benefits thereof must exceed the costs (Prabowo, 2010). This is also related to the efficiency in using the available resources to achieve the objective of crime prevention practices. This also signifies the need for reliable fraud data collection, management and distribution which represents efforts to understand what the actual problems are and how resources can be properly allocated to address them.
Bibliography


42


Channel Magazine. (2008(b)). *Teknologi Chip Mulai Ekspansif (Chip Technology is Getting Expansive)*. *Channel Magazine*, 22 (May - June), pp. 5-6.

Chip and PIN. (2005, October 10). *After 14 February 2006 Chip and PIN Cardholders Must Use Their PIN to be Sure They Can Pay*. Retrieved
October 12, 2009, from Chip and PIN:
http://www.chipandpin.co.uk/reflib/chipandpin_10oct05.pdf


Koran Jakarta. (2010, January 2). *Pengguna Kartu Kredit Bakal Meningkat (Number of Credit Card User will Increase)*. Retrieved February 6, 2010, from Bataviase: http://bataviase.co.id/node/33996


Conference on Information Technology and Communication for Indonesia) (pp. 9-14). Bandung: Bandung Institute of Technology.


Republika. (2011, July 25). *Komputer Telat Datang, Penerapan E-KTP Terancam Molor (Computer Delivery Arrives Late, E-KTP Implementation May be Delayed)*. Retrieved August 2, 2011, from Republika:


http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf


Warta Kota.co.id. (2010, December 29). *Tanpa Chip, Kartu Kredit Ditolak 1 Januari 2010 (As of 1 January 2010, Credit Cards without Chip will be Rejected)*. Retrieved February 5, 2010, from Warta Kota.co.id:  
http://www.wartakota.co.id/read/mal/18989

http://www.sinarharapan.co.id/berita/0601/14/eko06.html


Yanuarti, A. (2008, April 17). *Wajib Ada, Kok Malah Dicerca (Must Exist and yet is Despised)*. Retrieved February 4, 2010, from Gatra.com:  

Yeo, V. (2006, May 24). *Smart Cards Lower Credit Card Fraud in Msia*. Retrieved February 8, 2010, from ZDNet Asia:  
http://www.zdnetasia.com/news/security/0,39044215,39361483,00.htm