1-1-2006

An insight into advance fee fraud on the Internet

Joshua Chang
University of Wollongong, jchang@uow.edu.au

An insight into advance fee fraud on the Internet

Abstract

Advance fee fraud on the Internet currently rakes in hundreds of millions of dollars golbally per year. Aslo known as the "419" fraud, this scheme originated from Nigeria in the 1970s and was marketed via traditional means such as mail and facsimile transmissions.

Keywords

insight, into, advance, fee, fraud, Internet

Publication Details

Chang, J. (2006). An insight into advance fee fraud on the Internet. 3rd International Conference on Contemporary Business: Conference Proceedings (pp. 1-10). Bathurst, Australia: Charles Sturt University.

An Insight into Advance Fee Fraud on the Internet

Joshua Chang
University of Wollongong, Australia

Abstract

Advance fee fraud on the Internet currently rakes in hundreds of millions of dollars globally per year. Also known as the '419' fraud, this scheme originated from Nigeria in the 1970s and was marketed via traditional means such as mail and facsimile transmissions. The advent of the Internet and proliferation of its use from the 1990s makes it an attractive medium for marketing the fraud. Fraudsters are able to obtain an effective worldwide reach, employing key principles of persuasion in the proposal of the fraud. This paper provides an insight into advance fee fraud on the Internet, incorporating theory on the economics of information and persuasion.

Key words: Internet marketing, advance fee fraud, 419 fraud, persuasion

I. Introduction

The U.S. Department of Justice defines Internet fraud as, "any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Websites - to present fraudulent solicitation to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme." (U.S. Department of Justice 2000). Advance fee fraud on the Internet is one such example. The U.S. Secret Service reported that advance fee fraud on the Internet currently rakes in hundreds of millions of dollars globally per year and describes it as a "growing epidemic". It originated in the 1970s from Nigeria (Thompson 2003) and was marketed via traditional means such as mail and facsimile transmissions. Advance fee fraud is also known as the Nigerian scam or the '419' fraud, based on the section of the Nigerian penal code addressing fraud schemes (Rosen 2004). The Nigerian origins of the fraud have damaged the credibility of business with Nigeria and Africa (Viosca et al 2004).

The advent of the Internet and proliferation of its use from the 1990s makes it an attractive medium for marketing the fraud as not only can fraudsters obtain an effective worldwide reach, but can do so anonymously or incognito. Viosca et al (2004) state that new technology and the explosive growth of the Internet provides new outlets for fraud. Advance fee fraud is a confidence trick in which victims are persuaded to advance relatively small sums of money in the hope of realising a much larger gain. A typical version of the fraud is an email, most often from Nigeria, seeking an investor to help in transfer large sums of money (usually in tens of millions in US Dollars) out of the country, promising the investor a share. The fraudster then makes a request for a sum of money that is required in facilitating the transaction, such as a bribe to bank officials or to pay certain fees such as processing or customs fees. These scams can be highly elaborate and can appear to be very convincing, netting an estimated US$1 million daily from victims in the United States (Wagner 2004).

Originally, the fraudsters contacted mainly corporations due to their limited reach. The subsequent advent of the Internet opened up a far wider reach for the fraudsters, enabling

them to target potential individual victims via emails, discussion boards, and instant messaging systems (e.g. ICQ, Yahoo messenger, MSN messenger). Email is the primary mechanism by which a fraudulent contact takes place over the Internet (National White Collar Crime Center and the Federal Bureau of Investigation 2003).

This paper aims to provide an insight into advance fee fraud on the Internet, incorporating theory on the economics of information (Evans and Wurster 1999) and persuasion (Petty and Cacioppo 1986, Cialdini 1998, Cialdini and Goldstein 2002).

II. How advance fee fraud operates

Advance fee fraud operates by persuading victims to advance relatively small sums of money in the hope of realising a much larger gain. Fraudsters claim to be Nigerian officials, royalty, businesspeople, or their relatives trying to transfer money out of the country, offering to divide the proceeds with the victim for their help in facilitating the transfer. If a victim responds to the initial offer, the victim may receive numerous documents with official looking stamps, seals and logos testifying to the authenticity of the proposal. The victim is then typically asked to provide blank company letterheads, bank account details, as well as some advance fees to cover various taxes, transfer costs, attorney fees, or bribes. The victim may even be encouraged to travel to Nigeria or a border country to complete the transaction. Sometimes, the fraudsters will produce trunks of dyed or stamped money to verify their claims that the money exists, claiming that the money is dyed for security reasons. They then claim to require special chemicals to remove the dye so that the money becomes usable (this part is known as 'black money scam'). Inevitably, other issues arise, requiring more of the victim's money and delaying the "transfer" of funds. In the end, there are no profits to share, and the fraudster will have vanished with the money. This is a summary of how classical advance fee fraud operates.

There is little or no respite for victims of such fraud due to the limited official influence into Nigeria for investigations to take place. According to a report by McDermott (1998), a Nigerian consulate officer in New York said Nigerian officials are unhappy that Nigeria

is sometimes blamed for what some U.S. citizens may be doing. He suggested that the only real way to stop the fraud is for U.S. businesses and individuals to "stop being greedy," and not go along with the schemes. Without diplomatic support, it is difficult for victims to investigate the fraud on their own, and 17 people have been killed since 1992 in Nigeria trying to recover their lost funds (Thompson 2003).

An example of a typical advance fee fraud proposal is as follows (U.S. Department of State 1997):

> *"Having consulted with my colleagues, and based on information gathered from the Nigerian Chamber of Commerce, I am pleased to propose a confidential business transaction to our mutual benefit. I and my colleagues have in our possession instruments to transfer the sum of $35,500,000.00 into a foreign company's account in our favor. This amount emanated as a result from an over-invoiced contract, executed, commissioned, and paid for about two years ago by a foreign contractor. We are therefore seeking your assistance in transferring this money to your account as it can only be remitted to a foreign account, and as civil servants, we are forbidden to operate foreign accounts. The total sum will be shared as follows:*
>
> *30% for the account owner (you)*
>
> *60% for us*
>
> *10% to settle any incidental expenses*
>
> *"We shall commence the transfer of funds immediately, as soon as you send the following documents/information through the above fax number.*
>
> *1. Four copies of your company's letter head and invoice papers signed and stamped*
>
> *2. Your banker's name, address and fax numbers*
>
> *3. The account number and name of would be beneficiary.*
>
> *"Bear in mind that this is absolutely a private and personal deal, nonofficial; and should be treated with all measure of secrecy and confidentiality."*

Relevant to explaining why the fraud originates from Nigeria, it is interesting to see that according to the anti-fraud website 419eater.com, the justification from fraudsters is assumed as follows:

1. Nigeria was a happy and peaceful country until the West came along.
2. Western companies, such as Halliburton and Shell, bribed their way into the country and proceeded to strip Nigeria of its assets leaving the inhabitants poverty stricken and struggling to survive.
3. Therefore the West is responsible and now it is payback time.

Below are some guidelines that can help guard against classical advance fee fraud for individuals:

1. Resist the temptation to communicate with any party that purports to offer a sum of money (e.g. offers to transfer stocks, money, treasure, lottery wins, etc.) until they are proven to be legitimate.
2. Do not assume an individual's or organisation's identity to be true in calls, letters, emails or faxes received. Most fraudsters assume a false identity and do so highly convincingly.
3. When in doubt of the legitimacy of any transaction, do not provide personal details, bank information, or send money. Seek advice from law enforcement authorities if a hint of fraud is detected.

A popular version of advance fee fraud is known as the 'refund' variation (Wagner 2004), and it targets sellers on the Internet. The buyer offers to buy items advertised online, mostly high value items such as electronics, and pays by mailing a counterfeit cashier's cheque drawn from a US financial institution. This type of fraud works because cashier's cheques are regarded as an equivalent of cash. Financial institutions are required to make funds available the next business day (up to the first US$5,000, after the banking day of receiving a local cashier's check). The next-day availability requirement may confuse depositors into thinking cashier's cheques will clear in a short amount of time. Based on that misunderstanding, sellers feel comfortable refunding apparent overpayments. In reality, cashier's checks can take several days or longer to clear, depending on whether or not they're local (Wagner 2004).

A few ways in which a seller can be defrauded are:

a) The seller sends the goods after depositing the cashier's cheque but before it is cleared.

b) The buyer makes a significant overpayment on the price of the goods, offering a plausible explanation, and asks for a refund for the difference. The seller sends a refund for the overpayment after depositing the cashier's check but before it is cleared.

c) The deal is mutually cancelled after the buyer pays the seller. The seller refunds the amount of the transaction after depositing the cashier's check but before it is cleared.

To guard against this variety of fraud, sellers should not make refunds or send goods until the cheque or cashier's order has been cleared by the bank and the money is safely in the available balance.

The concept of this variation of advance fee fraud works with not only with cashier's cheques, but with any type of payment where there exists a lapse of time between deposit and clearance, or where the funds paid can be rescinded at a later date (e.g. credit cards and third party payment systems such as Paypal or Bidpay). In the case of credit cards, credit card companies can rescind payments from merchants that unknowingly process stolen credit cards, as the risk and responsibility for proving the authenticity of the credit card transaction lies completely with the merchant. This is a problem as such fraudulent credit card payments are immediately processed and the goods subsequently dispatched, only to have the unauthorised transaction discovered by the genuine credit card holder at a later date, and the funds rescinded by the credit card company.

III. The role of 'richness and reach' of information

According to the consumer organisation Internet Fraud Watch (www.fraud.org), the number of consumer complaints it receives about Internet fraud schemes has risen dramatically in the two years between early 1997 and late 1998, from 1,152 in 1997 to more than 7,500 in 1998, implying a proliferation in the number of online fraud. This proliferation of fraud is an externality of the communicative advantages provided from the advent of Internet.

Traditionally, from the 1970s (Thompson 2003), the fraud was marketed mainly via mail and facsimile transmissions. Such methods are expensive and slow compared to emails, online discussion boards, and instant messaging systems (e.g. ICQ, Yahoo messenger, MSN messenger etc.). Email allows the fraud to be communicated to an exponentially larger number of potential victims than the traditional methods with the help of email lists, which can be targeted, and relatively easy and inexpensive to obtain.

An important reason for the proliferation of fraud on the Internet is its advantages in richness and reach of information. Evans and Wurster (1999 p.23) state: "To the extent that information is embedded in physical modes of delivery, a basic law governs its economics; there is a universal trade-off between richness and reach." The theory of richness and reach (Evans and Wurster 1999) states that the Internet weakens or eliminates this trade-off, enabling the advantages of both richness and reach of information. This weakening or elimination of the 'richness/reach' trade-off enables fraudsters to reach a large number of potential victims and exchange a high level of literary, pictorial, audio, and interactive information (e.g. photos, phone calls, and video conferencing).

IV. The role of persuasion

The Elaboration Likelihood Model (ELM) distinguishes between two routes to persuasion: the central route and the peripheral route (Petty and Cacioppo 1986). The central route to persuasion refers to processes that involve a high level of cognition and therefore are likely to predominate under conditions that promote high elaboration. An example would be the attempt to gain favourable consumer attitudes using cogent arguments or detailed literary information provided, for instance, in a luxury car advertisement. The peripheral route to persuasion, on the other hand, refers to processes that involve little cognition and therefore predominate under conditions that promote low elaboration. An example would be the attempt to gain favourable consumer attitudes using attractiveness, credibility or prestige, bypassing deeper cognitive processes.

As every scheme to defraud necessarily involves the offering of goods or services in ways that misrepresent their objective qualities and features, the principals in the scheme can never afford to use a direct route to persuasion, and therefore invariably fall back on methods using peripheral routes to persuasion (Rusch 1999). According to Cialdini (1998), there are six basic principles relying on peripheral routes to persuasion that are highly likely to persuade or influence others, being liking, reciprocation, consistency, scarcity, social validation, and authority. Of these factors, authority, scarcity, and reciprocation appear to be most relevant in persuading victims of the classical advance fee fraud as outlined below.

Fraudsters usually claim to be relatives of government officials or royalty to assert a position of authority. According to Cialdini (1998), in the right situation, people are very likely to be highly responsive to assertions of authority, even when the person who purports to be in a position of authority is not physically present. To illustrate the influence of authority, researchers (Lefkowitz, Blake, and Mouton 1955, quoted in Cialdini and Goldstein 2002) had a 31-year-old man illegally cross the street on a number of different occasions, while they surreptitiously observed the number of pedestrians who followed him across each time. Three times more people followed the jaywalking man into traffic and across the street when he wore formal business attire than when he was dressed in a more casual work outfit.

The fraud is positioned such that it appears to be a rare and one-off opportunity that highlights its scarcity. Cialdini (1998) states that people are highly responsive to indications that a particular item they may want is in short supply or available for only a limited period. Research by Dr Jack Brehm of Stanford University (as reviewed in Cialdini 1998) indicates that people come to desire that item even more when they perceive that their freedom to obtain it is or may be limited in some way. The belief that others may be competing for the short supply of the desired item may enhance the person's desire even more. In an example by Cialdini and Goldstein (2002), wholesale beef buyers more than doubled their orders when they were informed that a shortage of Australian beef was likely due to weather conditions overseas. When those purchasers

were told that the information came from an exclusive source at the Australian National Weather Service, however, they increased their orders by an astounding 600 percent.

The fraud involves reciprocation of a favour, promising a generous cut for helping to transfer a large amount of money out of the country. According to Cialdini (1998), a well-recognised rule of social interaction requires that if someone gives us (or promises to give us) something, we feel a strong inclination to reciprocate by providing something in return. According to Dennis Regan (1971, reviewed in Cialdini and Goldstein 2002), individuals who received a small, unsolicited favour from a stranger ("Joe") in the form of a can of Coca Cola purchased twice as many raffle tickets from Joe as those who received no favor at all. This occurred even though the favour and the request took place one-half hour apart, and that Joe made neither implicit nor explicit reference to the original favour when he made his pitch about the raffle tickets.

V. Conclusions

The growth of advance fee fraud is an externality parasitic to the communicative advantages provided by the advent of the Internet. According to theory in the economics of information (Evans and Wurster 1999), it allows fraudsters to reach a large number of potential victims with a high level of information. Fraudsters persuade their victims using the peripheral route of persuasion according to the Elaboration Likelihood Model (Petty and Cacioppo 1986), employing key principles of persuasion (Cialdini 1998), namely authority, scarcity, and reciprocation to ensnare victims. This insight into advance fee fraud on the Internet can be of importance to Internet users in understanding the nature of the fraud, and how it can be identified and avoided. A useful direction for further research is to conceptualise how Internet users identify and manage fraud on the Internet.

List of References

Cialdini, R. (1998) *Influence: The Psychology of Persuasion*, William-Morrow, New York

Cialdini, R. and Goldstein, N. (2002) 'The science and practice of persuasion' *Cornell Hotel and Restaurant Administration Quarterly*, 43 (2), pp 40-51

Evans, P. and Wurster, T. (1999) *Blown to Bits: How the Economics of Information Transforms Strategy*, Harvard Business School Press, Boston.

Internet Fraud Watch (www.fraud.org)

Lefkowitz, M., Blake, R. and Mouton, J. (1955) 'Status Factors in Pedestrian Violation of Traffic Signals', *Journal of Abnormal Social Psychology*, 51m pp 704-706

McDermott, J. (1998) 'US Postal Service is cracking down on Nigerian scams', *Wall Street Journal* (Eastern edition). New York, N.Y.: Nov 11, p 1

National White Collar Crime Center and the Federal Bureau of Investigation. (2002) *IFCC 2001 Internet Fraud Report*, (found at: www.ic3.gov/media/annualreport/2001_IFCCReport.pdf)

Petty, R. and Cacioppo, J. (1986) *Communication and persuasion: Central and peripheral routes to attitude change*. New York: Springer-Verlag.

Regan, D. (1971) 'Effects of a Favor and Liking on Compliance', *Journal of Experimental Social Psychology*, Vol 7, pp 627-639.

Rosen, J. (2004) 'Avoiding the Nigerian Scam', *Publishers Weekly*, 251 (28), p 14

Rusch, J. (1999) 'The "Social Engineering" of Internet Fraud', Proceedings from the ISOC conference, San Jose, California

Thompson, N. (2003) 'You've got fraud!' *Foreign Policy*, Washington: May/Jun, p 93

Wagner, V. (2004) 'Nigerian scam has new twist', *Credit Union Magazine*, Madison, 70 (9), pp 70-72

United States Department of Justice. (2000). *Internet Fraud* (found at: http://www.usdoj.gov/criminal/fraud/text/Internet.htm)

United States Department of State Report (1997) *Nigerian Advance Fee Fraud* (found at: http://www.state.gov/www/regions/africa/naffpub.pdf)

United States Federal Trade Commission (www.ftc.gov)

Viosca, C., Bergiel, B., and Balsmeier, P. (2004) 'Effects of the Electronic Nigerian Money Fraud on the Brand Equity of Nigeria and Africa', *Management Research News*, 27 (6), pp 11-21

419 Eater (www.410eater.com)