NATIONWIDE CREDIT CARD FRAUD PREVENTION

Hendi Yogi Prabowo*

Recent global payment fraud statistics indicate the seriousness of the credit card fraud problem. In the United Kingdom, in 2009 alone, losses from plastic (debit and credit) card fraud according to the report by the Financial Fraud Action UK (FFA) were $US696 million (Financial Fraud Action UK, 2010). In the same year, the Australian Payments Clearing Association (APCA) recorded losses of $US144 million from credit and charge card fraud perpetrated on Australian issued cards (Australian Payments Clearing Association, 2010). Both countries have been experiencing an upward trend in the losses from the offences over the past few years. Payment fraud statistics from the two countries suggest that card-not-present fraud (e.g. online credit card fraud) is the most common type of credit card fraud followed by skimming/counterfeit card fraud. This is different from a decade ago when skimming/counterfeit card fraud was statistically the most prevalent modus operandi. The emergence and growth of e-commerce has been a driving factor behind such a change. The implementation of the Chip and PIN technology in many countries, for example, has caused geographical displacement (e.g. from one country to another) and tactical displacement (e.g. from skimming/counterfeit card fraud to online credit card fraud) of credit card fraud.

Many credit card fraud offenders are now better organized than before, resulting in higher losses from their offences. They even have their own supply and demand in the underground economy for stolen credit card information (Wilson, 2008, p. 5). Some of the proceeds from this economy are used to finance other crimes including terrorism[1]. This requires fraud preventers to also become more organized. Countries such as the United States and the United Kingdom have been improving their fraud prevention strategies by enhancing their coordination. The establishment of the President's Identity Theft Task Force in the United States and the National Fraud Authority in the United Kingdom are evidence of their seriousness in addressing fraud problems. Author's study suggests that the key areas of

[1] The first Bali bombings (2002) are a good example of the use of credit card fraud for terrorist funding. According to Lormel (2008, p. 14), in relation to the bombings, more than any other case study, the case of Imam Samudra highlights the critical importance of credit card information security. While in prison in 2004, Imam Samudra wrote a jailhouse manifesto, in which one chapter describes hacking (Lormel, 2008, p. 14). The chapter does not focus on specific techniques, but instead provides information on how to find techniques on the internet as well as how to connect with people in chat rooms to hone credit card fraud skills (Lormel, 2008, p. 14).

resource allocation in credit card fraud prevention within a payments system are: understanding of the real problems; fraud prevention policy; fraud awareness; technology-based protection, identity management; and legal deterrence. These areas are mainly supported by four pillars: user; institution; network; and government and industry. This is dubbed by the author as the Four Pillared-House of Payments Fraud Prevention Practice.

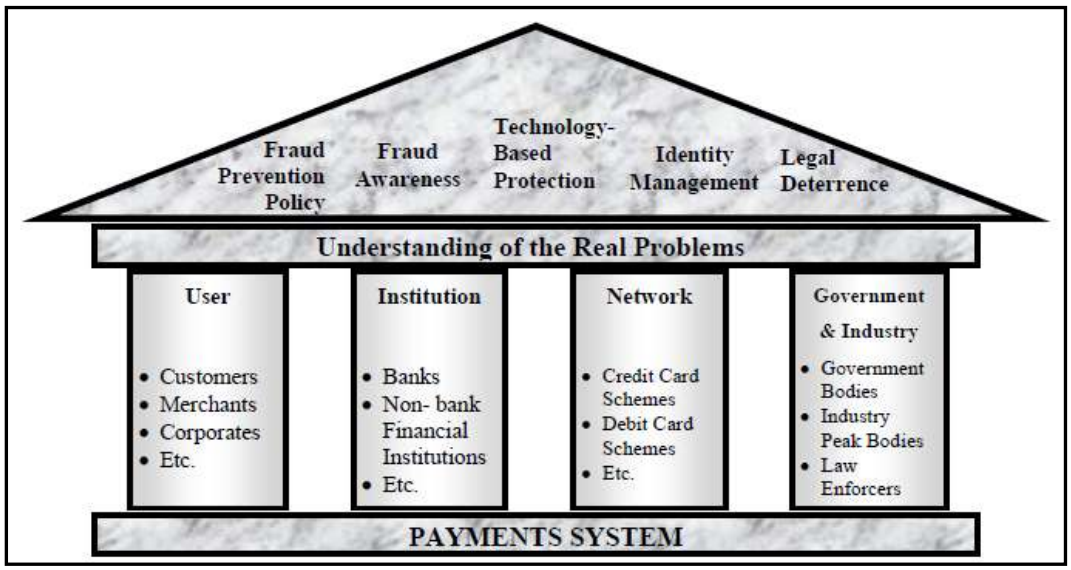

Figure 1 The Four-Pillared House of Payments Fraud Prevention Practice

As shown by Figure 1, the structure of the prevention practices is supported by four 'pillars', which represent the four groups of key participants in the payments system (users, institutions, networks and government and industry) who work together to promote the safety of the payments industry. In Australia, the framework of payments fraud prevention practices with these four groups is known as the 'four layers of fraud prevention', with the fourth layer the most challenging to manage and coordinate, because it encompass the interests of many different parties. Other than the central banks (for example, the US Federal Reserve, the Bank of England and the Reserve Bank of Australia), whose responsibilities include promoting the safety and efficiency in the payments systems, other institutions such as the US Federal Trade Commission (FTC), the Financial Fraud Action UK (FFA) and the Australian Payments Clearing Association (APCA) along with other payments system institutions, play important roles in payments fraud prevention practices.

Each pillar is important to the entire structure in achieving its purpose. For example, cardholders can make their best efforts to keep their confidential information such as PINs

protected, and credit card-issuing banks and financial institutions can design and implement effective and efficient fraud prevention measures to minimize fraud risk. Card networks such as Visa and MasterCard can issue rules of operation that provide incentives for implementing better fraud prevention measures, such as chip and PIN technology for offline transactions, and PCI DSS compliance for online transactions. Finally, the collaboration among government and industry peak bodies in preventing credit card fraud in the form of, for example, the issuance of laws and regulations specifically designed for tackling fraud will further strengthen the 'house'. This fourth pillar includes the role of law enforcement agencies in upholding anti-fraud laws and regulations to establish sufficient deterrence effect.

On top of the four pillars are the six broad groups of initiatives which form the essentials in the payments fraud prevention practices in a country: understanding of the real problems, fraud prevention policy, fraud awareness, technology-based protection, identity management and legal deterrence. *Understanding of the real problems* is the basis for decision-making processes for the remaining five groups of initiatives, because good prevention practices are based on the actual problems, and thus building sufficient understanding on the problems should be achieved before resorting to further actions (Gilling, 1996, p. 11). Important elements in the process of understanding the real problems include fraud data collection, management and distribution, such as those of the FTC, the FFA and the APCA. Payments system institutions are in a strategic position to shed some light on recent issues (such as recent trends in credit card fraud and credit card fraud prevention practices), particularly in the form of the collection of victim-side data through self-reporting mechanisms[2]. For example, the FTC, the FFA and the APCA regularly publish fraud statistics based on the reports of victims. Combined with the information on offenders from the criminal justice system, such victim data and information can be used to draw a more complete picture of payments fraud for further actions regarding prevention, investigation and prosecution.

As mentioned before, based on the understanding of the actual problems, further actions to tackle payments fraud must be taken properly. In terms of *fraud prevention policy*, banks and other financial institutions, card schemes, government bodies and industry bodies can establish specific rules dedicated to fraud prevention activities. For example, in the US, the

[2] In the United Kingdom, for example, according to the Home Office (2007, p. 31), the Association for Payment Clearing Services APACS (now succeeded by, among others, the FFA) is considered as a better fraud figures source than the police. The Home Office (2007, p. 30) contends that the statistics from the police are a poor indication of the real level and trends in fraud.

Red Flags rule was issued in 2007 by the Federal Trade Commission (FTC), the federal bank regulatory agencies and the National Credit Union Administration (NCUA), creating an obligation for creditors and financial institutions to implement identity theft prevention programs pursuant to the Fair and Accurate Credit Transactions (FACT) Act 2003 (P.L. 108–159) (Finklea, 2009). As potential victims, consumers should be kept aware of the recent issues in payments fraud and the available prevention measures thereof. Fraud data and information from the fraud data and information collection process can also be used for educational purposes to increase consumers' *fraud awareness*. In the UK, for example, during the period of transition from magnetic stripe to chip and PIN technology, several consumer education initiatives were undertaken to ensure that consumers were aware of the new security features introduced. The Chip and PIN technology itself represents *technology-based protection* against fraud to minimize crime opportunities.

Despite the currently available options of technology for use in preventing fraud in the payments system, not all can be implemented by the industry, because considerations must be made regarding the costs and benefits of each option. For example, the level of acceptance of chip and PIN technology in the UK is higher than in the US; whereas the PCI DSS for online protection, which is well received in the US, is being adopted in the UK at a slower pace. This may have been caused — at least partly — by the previous significant investment in the UK in chip and PIN technology, which made industry members reluctant to make additional investment in the PCI standards.

Identity management, is related to the combination of technical systems, rules and procedures that define the ownership, utilization and safeguarding of personal identity information (National Science and Technology Council, 2008, pp. ES-1). In other words, the existence of personal identity information is a major reason this group of prevention practices exists. Identity management is essential not just for prevention of payments fraud, but also for the entire course of investigation and prosecution into it. Identity management can be used to reduce the opportunity for fraud offenders to use forged or stolen identity document to commit fraud (for example, fraudulent credit card application). In the US, for example, efforts have been made to minimize the use of the social security number (SSN) by public and private sectors to reduce the risks of such information being unlawfully obtained by offenders (President's Identity Theft Task Force, 2007). In Australia, to open an account, an applicant must satisfy the requirements of the 100-point check by providing multiple sources

of identification, and this can reduce the opportunity for fraudulent applications to occur (Smith, 1998).

Although the focus of this article is on the fraud prevention practices in the payments system, author also acknowledges the fact that despite all the resources spent on prevention measures, payments fraud can still occur. To address this shortfall, cooperation with members of the criminal justice system should be strengthened to provide sufficient legal deterrence to discourage potential offenders to commit fraud. Among such cooperation is the sharing of information on fraud cases reported by victims, based on which, and combined with information on offenders, should form a more complete picture of the actual fraud problem in a country. For example, the FTC, the FFA and the APCA are sources of fraud data and information based on victims' reports, and continues to supply such information to members of the criminal justice systems in their countries.

Members of criminal justice systems can increase legal deterrence by improving their skills and knowledge about the investigation of fraud cases and prosecution of the fraud offenders, supported by the improvement of the legal systems by, among other things, the enactment of laws for the prosecution of payments fraud offenders. In the US, for example, to cope with growing threats from identity theft, the US Congress passed two statutes that criminalize identity theft: the Identity Theft and Assumption Deterrence Act (18 USC. §1028(a)(7)) on 30 October 1998, and the Identity Theft Penalty Enhancement Act (Aggravated Identity Theft) (18 USC. §1028A) on 15 July 2004 (Richey, 2007).

Although each is different, the six areas of payments fraud prevention practices often overlap and support one another. For example, the UK credit card network's (for example, Visa and MasterCard) policies for fraud prevention contributed to the adoption of chip and PIN technology in the country by network members (for example, banks and merchants), as well as several fraud awareness campaigns to inform consumers about recent issues in fraud and fraud prevention practices. To optimize the role of the four pillars in the six categories of fraud prevention practices, coordination is of the essence in ensuring that objectives are achieved. In the US, for example, the President's Identity Theft Task Force issued a strategic plan in April 2007, *Combating Identity Theft: A Strategic Plan* (President's Identity Theft Task Force, 2007), to tackle growing threats of identity theft in the US. Later, the UK National Fraud Authority released its first national strategy on 19 March 2009 to mitigate threats of

fraud in the country (National Fraud Strategic Authority, 2009). Both strategies basically represent the efforts to coordinate the available resources to combat crimes in the respective countries to achieve the intended objectives effectively and efficiently. The Four-Pillared House of Payments Fraud Prevention Practice only sets a minimum standard for payments fraud prevention practices. This means that, in reality, more parties and efforts can be added to the 'house' to improve the achievability of the objectives.

Combating fraud is a continual journey that can be seen as similar in many ways to the game of chess, where 'players' (for example, fraud preventers and fraud offenders) generally seek to optimize their benefits, and their decision-making processes are related to each other. For example, fraud preventers' acts are often based, at least in part, on the previous actions of fraud offenders and vice versa. In the end, the player with the better strategy will emerge victorious. In preparing or refining a strategy, a player needs to understand the resources that they have at their disposal, as well as the best way to use them to achieve the desired objectives. Gaining sufficient understanding of the 'enemy' is also an important element in achieving the best results with the least amount of resources. In combating fraud, every country has its own set of resources (for example, financial resources), but the desired results are in many ways similar (for example, reducing fraud losses). The most important thing is not how many resources a country has but whether they are used effectively and efficiently. As the focus of this article, fraud prevention is just as important (some would say more important) as other areas (for example, investigation and prosecution) in combating fraud. Preparation against possible future threat should be of the same level of importance with combating existing fraud threats. As the great master of strategy, Sun Tzu, once said (Giles, 1910):

> Now the general who wins a battle makes many calculations in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculations at all!
>
> Fighting with a large army under your command is nowise different from fighting with a small one: it is merely a question of instituting signs and signals…
>
> …to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

BIBLIOGRAPHY

Australian Payments Clearing Association. (2010). *Fraud Perpetrated on Australian Issued Payment Instruments 1 January 2009 - 31 December 2009.* Retrieved November 5, 2010, from Australian Payments Clearing Association: http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Payment_Fraud_Statistics_20099_PrintFriendly.pdf/$File/Payment_Fraud_Statistics_20099_PrintFriendly.pdf

Financial Fraud Action UK. (2010). *Fraud the Facts 2010.* Retrieved December 27, 2010, from Financial Fraud Action UK: http://www.financialfraudaction.org.uk/download.asp?file=749

Finklea, K. M. (2009, May 27). Identity Theft: Trends and Issues. *Prepared for Members and Committees of Congress* . Congressional Reserach Service.

Giles, L. (1910). *Sun Tzu on the Art of War.* Retrieved December 31, 2007, from Artofwarsuntzu.com: http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf

Gilling, D. (1996). Problems with the Problem-Oriented Approach. (R. Homel, Ed.) *The Politics and Practice of Situational Crime Prevention: Crime Prevention Studies , 5*, pp. 9-23.

Home Office. (2007, May 15). *Mobile Phone Theft, Plastic Card and Identity Fraud: Findings from the 2005/06 British Crime Survey.* (J. Flatley, Ed.) Retrieved November 10, 2010, from Home Office: http://rds.homeoffice.gov.uk/rds/pdfs10/hosb0810.pdf

Lormel, D. M. (2008, September). *Terrorism and Credit Card Information Theft: Connecting the Dots.* Retrieved November 2, 2008, from IPSA International: http://www.ipsaintl.com/news-and-events/articles/pdf/lormel-terrorism-and-credit-cards.pdf

National Fraud Strategic Authority. (2009, March 19). *The National Fraud Strategy - New Rules to Crackdown on Fraud Will Provide Real Help Now to Consumers and Businesses: News Release.* Retrieved September 27, 2009, from The Attorney General's Office: http://www.attorneygeneral.gov.uk/attachments/090317%20NFS%20news%20release%20FINAL%20electronic.pdf

National Science and Technology Council. (2008, September). *Identity Management Task Force Report 2008.* Retrieved September 5, 2009, from National Science and Technology Council: http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf

President's Identity Theft Task Force. (2007, April). *Combating Identity Theft: A Strategic Plan.* Retrieved July 18, 2009, from Idtheft.gov: http://www.idtheft.gov/reports/StrategicPlan.pdf

Richey, M. (2007). Computer Crimes Identity Theft. *Paper presented at the Multi-Track Federal Criminal Defense Seminar*, (pp. 1-7). Baltimore.

Smith, R. G. (1998, December). *Best Practice in Fraud Prevention.* Retrieved October 1, 2007, from Australian Institute of Criminology: http://www.aic.gov.au/publications/tandi/ti100.pdf

Wilson, S. (2008). Cardless Criminals: Card-Not-Present Fraud is Spiraling Out of Control, with Very Few Options for Stopping It. *Onlne Banking Review , April/May*, p. 5.

---

* Hendi Yogi Prabowo holds a Master of Forensic Accounting degree from the University of Wollongong Australia. In 2010 he completed his PhD majoring in Forensic Accounting at the Centre for Transnational Crime Prevention of the University of Wollongong Australia. He is currently a lecturer at the Islamic University of Indonesia.