World Applied Sciences Journal 29 (6): 774-778, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.06.13930

Fraud in Non-Cash Transactions: Methods, Tendencies and Threats

Oleg Victorovich Sobko

Financial Police Academy, Koshi vil.,
Akmola region, Republic of Kazakhstan

Abstract: This paper discusses the various methods of non-cash payments, the frauds perpetrated relative to their use. After a brief discussion of the methods, used by swindlers, the paper thus discusses the key circumstances conducive to fraud, risks, scale of detriment and the obstacles to providing safe financial transactions. The paper then describes the most effective measures being adopted by the industry as well as by governments to stop or at least diminish their incidences. Issues discussed include predictable tendencies and threats to economic security.

Key words: Larceny · Fraud · Non-cash transaction fraud · Computer fraud · Cheque fraud · Click fraud · Circumstances conducive to fraud

INTRODUCTION

Non-cash transactions or settlements conducted without the use actual cash is increasing globally. Figure 1 shows that this has become a prevailing phenomenon on all parts of the globe not only in North America and Europe, but even among mature Asia-Pacific countries, Brazil, Russia, India and China (BRIC), Central Europe, Middle East and Africa, Latin America and the rest of Asia. With the rise of this method of payment, however, is a parallel increase in non-cash transaction frauds, which is causing concerns among governments because of their eventual negative impact on the economy.

For accounting purposes, there are three kinds of transactions: cash transactions; credit transactions and non-cash transactions. The distinguishing factor between the three is the presence or absence of cash/money in the transaction. Among the three types, it is only the non-cash transaction that never involves cash since cash transactions always involve cash and credit transactions may involve cash after the date of transaction [1]. Methods of non-cash transactions include: cheques, whether commercial cheques, US Treasury cheques or postal money orders and; electronic payments, such as Automated Clearing House (ACH), debit cards and credit cards [2]. Also on the rise are e-Payments and m-Payments, which are brief terms for payments made for e-commerce transactions and transactions using mobile devices, respectively [3].

Cheques are primary paper-based instruments in settlement transactions, but according to the World Payment Reports 2011, their use is considerably declining in certain markets and has even become obsolete in some. In the global sphere, its use has reportedly decline from 22% in 2005 to 16% in 2009 out of all non-cash transactions.

The move away from its use, whether intentionally or not, is driven by the rise of the digital age. Some governments, like the UK and the US, are intentionally discouraging its use and measures have been adopted towards this end. In the UK, the UK Payments Council is encouraging the development of innovation that would satisfactorily substitute the use of cheques. In the US, the improvement of cheque processing is the focus, such as the ability to process them electronically through cheque-imaging [3].

Electronic payments in the US, on the other hand, are rising, especially in the use of debit and credit cards, which shot up from 64.7 billion in 2006 to 84.5 in 2009. Statistics show that transactions using debit cards have increased from 25 billion in 2006 to 37.9 billion in 2009,

Corresponding Author: Sobko, Financial Police Academy, Koshi vil.,
Tselinograd district, 010000, Akmola region, Republic of Kazakhstan.

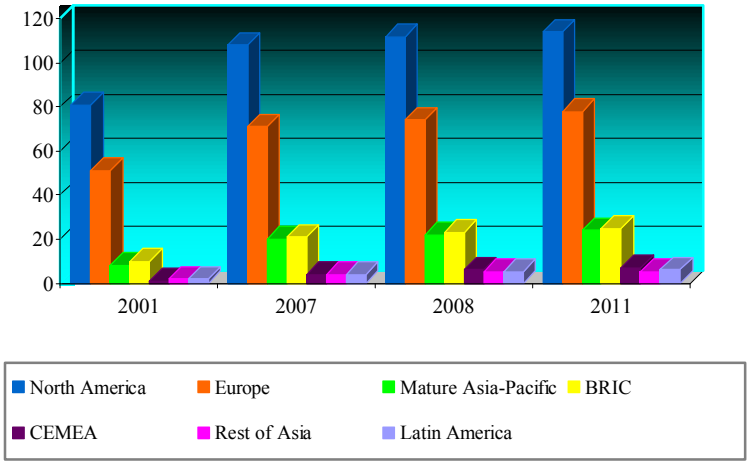

Fig. 1: Number of Non-Cash Transactions by Region (in billions)

while credit cards declined a little [2]. Credit cards are issued by banks, financial institutions, like Mastercard or Visa and can be used to purchase items or pay for services in various stores the payment of which are made by the issuing bank or institutions to the store. The customer in return pays the issuing institution later, but the cards can be used only in stores in which the issuing institution has partnership with. Store credit cards are similar to credit cards except that they are issued by a particular store and can be used only in that store [4].

The increase in non-cash settlements and transactions also gave rise to a parallel increase in non-cash fraud. Non-cash fraud are varied, but they can be classified as traditional and the newer methods. Traditional methods are schemes that have been long used by fraudsters such as stealing physical cards or forging cheques while newer methods make use of technological knowhow. The bigger fraud being presently perpetuated involves transactions using credit or debit cards, which uses sophisticated technology in accessing data and information. Credit card frauds include point-of-sale (or POS) fraud, card-not-present fraud (CNP hereafter), e-commerce fraud, ATM fraud and identity theft [5]. POS occurs when payment is made at the time of the transaction usually in a face-to-face situation and involves stolen, lost or counterfeit cards [6]. CNP is so-called because the merchant has no opportunity to inspect the credit or debit card since transactions are done online or over the internet or phone. In this type of fraud, a fraudster uses the debit or credit information and data of another to enter into a transaction without the authorization of the real card owner [5]. E-commerce fraud is similar to CNP fraud in that the merchant does not have the opportunity to examine the card physically, but it is narrower in the sense that it involves only transactions done over the internet.

In all kinds of fraud involving electronic transactions, credit or debit, identity theft is involved because without accessing data and information of a cardholder the fraud cannot be perpetrated. Some of the methods used in stealing data and information of cardholders include skimming, phishing and carding. In skimming, personal and account information stored in a card is accessed when it is being processed by using an electronic device called a skimmer, which fraudsters attach over or near genuine card slots. Skimmers are used in restaurants to capture credit card information through accomplices in the restaurant staff, at unattended ATM machines or gas stations and may even be perpetuated by store clerks themselves by scanning cards twice, once with the real scanner and the other with a skimmer [7]. Phishing has the same goal as skimming, but is conducted through emails where a recipient is directed to enter a site, usually bogus, that is being monitored by the fraudsters. Carding, on the other hand, is the validation of stolen credit card numbers by making small non-distracting purchases with online merchants with real-time transaction processing. When the transaction is successful, the information is later sold to or exchanged with other fraudsters who will make bigger purchases [8].

In light of the increasing use of non-cash transactions worldwide, especially in the US and Europe, there are concerns that fraud relative to this type of transactions will also rise. This is compounded by a projected increase in ecommerce. Goldman Sachs predicts that ecommerce sales will reach $963 billion by 2013. This observation is supported by Emarketer, a

digital and media researcher and analyst in the US, which forecasts a $224.2 billion online shopping sales in 2012 or a 15.4% increase from the previous year as well as by projections in Latin America, Africa, Middle East, Australia and Asia-Pacific. The parallel rise in non-cash fraudulent activities is being seen in North America, where losses from ecommerce fraud topped at $4 billion in 2009 from $1.7 billion in 2001 [9].

Global card fraud has likewise risen. It grew to 12.8% in 2009 compared to the 2008 figures, which amounts to a total global loss of [a]4.9 billion. This is attributed to the growing sophistication of fraudsters allowing them wider access to merchant databases and processors data centers [3]. In the US, Canada and Australia, the misuse of credit cards or existing bank accounts is the biggest form of identity crime. In the UK, misuse of payment cards account for its highest loss at £504.8 million. In Australia CNP fraud is the most common at 48% while the UK CNP fraud has increased by 350% since 2000 [10]. As of 2006, the US had the highest loss rate at $3.718 billion as a result of card fraud as compared to Australia, France, Spain and the UK. Of the total loss, 59% was attributed to card issues and 41% to POS, internet and mail order [5].

On top of this, the merchant is likely to ruin his reputation and business goodwill, which is very important in the conduct of business [11]. It is commonly believed that only merchants and credit issuers that bear the brunt of these activities, but this is not true.

The victims whose personal data and information are stolen are vulnerable to other crimes that may cause them worse injury are also casualties of fraud. Although cardholders are not liable for unauthorized use of their cards [12], the experience can give them emotional and psychological trauma in addition to the anxiety caused by the personal data and information that have been stolen from them [13]. In addition, the consumers suffer as a whole because losses are eventually passed on to them in terms of higher interest rates and fees [12]. More importantly, the economy of a country may be affected as well. Customers confidence in commerce and business may wear off because of fear of being defrauded resulting in less transactions. The revenues lost and investments in fraud-detection technology, services and expertise will result into a weakened economy [9].

According to statistics, fraud loss rates differ from country to country. Dempsey (2010) attributes this variation in rates to several factors, which might as well be the same factors that can be said to conducive to the perpetration of fraud. The logic is that a country's fraud loss rate is higher because more fraud activities are being perpetrated there than in other countries because of the existence of more window of opportunities. Dempsey cites mix of payment cards in use, transaction authorization processes, types of payment made in cards, evolving security standards and the kind of card technology in use [14]. In the US, for example, debit card transactions using signature is of higher volume, i.e. 23.4 billion as opposed to 14.5 billion transactions, respectively in 2009, than those using PIN [2], which is the opposite in Australia, which uses 90% PIN. The rate of fraud involved in debit cards using PIN is lower than those using signatures, which may account for the high fraud rate in debit cards in the US. Moreover, CNP transactions are inherently riskier than other types because merchants are deprived the opportunity to look at the cards personally, which may be the reason why countries such as Spain have relatively lower card fraud than the US or the UK. The technology use in producing the cards also contributes to the facility in perpetrating fraud. As discussed elsewhere in this paper, the chip-and-PIN technology in the EU, as opposed to the magnetic stripes in the US, have considerably lowered the card fraud in the former [5].

In preventing the perpetration of fraud in connection with non-cash transactions, there are two measures with which authorities rely on: technology and; legislations.

In Europe, the technology of chip-and-PIN is being resorted to for the general protection of non-cash transactions. The chip-and-PIN technology entails the use of chips in credit and debit cards rather magnetic stripes and the addition of personal identification number or PIN. This system generates dynamic data that is exclusive only to a single transaction and authentication rather than the static data produced by magnetic stripes during verification stages. The chip-and-PIN system is primarily employed by the Europay, Mastercard, Visa or EMV, [3]. the collective card scheme being composed of Europay, Mastercard and Visa. American Express, JCB and Discover are, however, also adopting the system. [14]. Presently, 95% of European ATMS are already EMV-compliant and countries such as Japan, Korea and other developed and developing countries are taking the cue. The chip-and-PIN technology is most effective in face-to-face transactions (POP), ATM withdrawals and cases of lost and stolen cards. Its positive effect is being illustrated by the 77% decline in counterfeit card losses in the UK since its adoption in 2004 and in the entire European continent, which is now seeing a remarkable decrease in fraud losses [3]. Unlike Europe, the US has not adopted the EMV system, but rather uses other sophisticated technology to detect fraud in non-cash transactions.

Technologies related to "enhancing of data security standards, supplementing approval system of contactless payment cards, developing methods to encrypt payment data and disguising card numbers are being relied upon to combat fraud in non-cash settlements." [14]. To achieve the best desired goal, card companies led by Visa and MasterCard in the US have bonded together in 2004 to create the Payment Card Industry (PCI hereafter) Security Standards Council to administer industry standards. Some of the innovations being studied and implemented are contactless payment cards, encryption and tokenization [14]. Contactless payment cards and devices use the radio frequency technology instead of being swiped. They have secure microprocessors and memory, can perform cryptographic processing and other multiple functions [15]. End-to-end encryption, that is, from the time data is captured in the application layer to the point when it is at rest in databases and up to the moment when it is in transit from one application/system to another, is also seriously considered. On the other hand, tokenization works like chips in casinos where chips are used and accepted as money within the location, but are worthless outside them. In tokenization, data in cards are protected the moment they are captured by sending them to a secure vault where they are encrypted. Only a select number of applications are allowed access to actual card numbers in the vault and all the other applications are simply given tokens or substituted values randomly generated that can be passed from one system to another without the risk of harm [9].

The government is important in combating fraud because it can set the tone by issuing policies as well as adopt legislative measures to combat fraud. In the US, the agency President's Theft Task Force was created in 2006. It subsequently issued Combating Identity Theft: A Strategic Plan in 2007, which outlines the several key measures in overcoming identity theft. On the other hand, the UK National Fraud Authority published its own strategic plan in 2009 likewise to combat fraud within the country [16]. The EU also came up with its 2004-2007 Action Plan to Prevent Fraud on Non-Cash Means of Payment, which made the following priorities: the organization of pan-European training and conferences for law enforcement authorities, magistrates and prosecutors to apprise them of various methods of fraud involved in non-cash transactions and their impact on the financial system; the clarification and harmonization of data rules and transmission within the EU; the reorganization of the Fraud Prevention Expert Group to take into account the expansion of the EU with the addition of several states; the improvement of security in payment and; the new technologies that may be availed of to further protect the public from fraud [17]. The EU has likewise issued E-Money Directive (2009/110/EC), which obliges states to require their financial institutions to safeguard e-money payments for a number of days [18].

Non-cash transactions are rising and are projected to eventually substitute cash transactions in the future. The losses associated with the fraud occasioned in their use are staggering, especially in the US and the UK. The industry is up in its arms trying to figure out how to put a stop to these frauds. Governments are likewise worried because of the possible negative impact these frauds will create on their respective economies. These entities are resorting to new technology, stricter processing as well as policies and legislations to ensure that non-cash transactions can weather all these types of frauds that are being perpetuated by fraudsters and syndicates out to cash in on their technological know-how to steal and access personal information and data of cardholders.

According to the tendencies of growing non-cash transactions in developing countries, the measures that have been adopted by the developed markets, the experience of detecting and prosecuting non-cash fraud, should be taken for prevention of huge damage and massive losses on a formation level of financial system, based on non-cash transactions. Legislative and policy measures have to be coordinated and complementary, but the basis of the solution is an adequate and timely assessment of risks, threats and tendencies.

REFERENCES

1. Rajasekaran, V., 2012. Accounting for Managers. New Delhi: Pearson Education for India, pp: 47.
2. US Census Bureau, Statistical Abstract of the United States Table 1184. Non-Cash Payments by Method of Payment and ATM Cash Withdrawals: 2006 and 2009 (Banking, Finance & Insurance, 2012. Date Views 04.09.2013 www.census.gov/ compendia/ statab/ 2012/ tables/12s1184.pdf.
3. Capgemini, RSB & EFMA World Payments Report 2011 (2012). Date Views 21.08.2013 www.capgemini.com/ resource-file-access/ resource/ pdf/ World_Payments_Report_2011.pdf
4. The Growing Global Threat of Economic and Cybercrime; the results of the research, conducted by The National Fraud Center Inc.. Date Views 15.09.2013 www.utica.edu/ academic/ institutes/ ecii/ publications/ media/global_threat_crime.pdf.

5. Dempsey, J., 2010. Introduction to Private Security. Cengage Learning, pp: 321.
6. Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan, conducted by the EU Comission of the European Communities. Brussels, 2008. Date Views 15.08.2013 ec.europa.eu/ internal_market/ payments/ docs/ fraud/ implementation_report_en.pdf.
7. Albrecht, S., C. Albrecht, C. Albrecht and M. Zimbelman, 2011. Fraud Examination. Cengage Learning, pp: 364-365.
8. Card Not Present Fraud, A Simple Primer. White Paper conducted by Accertify Inc. Date Views 20.09.2013 www.proddownloads.vertmarkets.com/ download/b977cf33/b977cf33-6d64-493b-8a13-20ad45114917/original/accertifycnpfraudprimer.pdf.
9. E-Commerce Ffraud Protecting Data, Transactions and Consumers.White paper, conducted by RSA. Date Views 12.07.2013 www.yieldopedia.com/ paneladmin/ reports/ 3eb 19aa 3eb 35ca 18e 74a 4710838ffc 9b.pdf
10. Clough, J., 2010. Principles of Cybercrime. Cambridge University Press, pp: 186.
11. Bhatla, T., V. Prabhu and A.A. Dua, 2003. Understanding Credit Card Frauds. Cards Business Review, 2003–01. Date Views 05.10.2013 www.popcenter.org/ problems/ credit_card_fraud/ PDFs/ Bhatla.pdf.
12. Understanding Credit Cards, Credit Reports and Fraud. Date Views 10.12.2013 www.lectlaw.com/ files/ ban16.htm.
13. Gottschalk, P., 2010. Investigation and Prevention of Financial Crime: Knowledge Management. Gower Publishing Limited, pp: 14.
14. Sullivan, R., 2010. The Changing Nature of US Card Payment Fraud: Industry and Public Policy Options. Economic Review, 2(114). Date Views 22.08.2013 www.kansascityfed.org/PUBLICAT/ECONREV/PDF/10q2Sullivan.pdf.
15. Contactless Payment Security.Conducted by the Smart Card Alliance. Date Views 07.08.2013 www.smartcardalliance.org/ pages/ publications-contactless-payment-security-qa.
16. Hendi Yogi Probowo. Nationwide Credit Card Fraud Prevention. Date Views 18.07.2013 www.popcenter.org/ problems/ credit_card_fraud/ PDFs/ Prabowo%20card%20fraud.pdf.
17. A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment, conducted by Commission of the European Communities. Date Views 05.07.2013 europa.eu/ legislation_summaries/ fight_against_fraud/fight_against_counterfeiting/l 33306_en.htm.
18. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Date Views 04.08.2013 eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF