AFRREV IJAH
An International Journal of Arts and Humanities
Bahir Dar, Ethiopia
Vol. 1 (1), February, 2012:30-39
ISSN: 2225-8590

Ways of Curbing Frauds Associated with Electronic Payment

Adigwe, P. K.
Department of Banking & Finance
Nnamdi Azikiwe University, Awka

Abstract

Payment fraud is pervasive: Most business organization have experienced actual payment fraud in the past decades. Today, many business and government agencies make payments electronically rather than physically. People today, break so many security measures in banks to take other people's money and other valuables in banks. This paper tries to identity types of frauds in e-payment and posits appropriate measures to control them. The paper recommends that once payment is made on behalf of an agency, the agency must be notified instantly and fast ordering system with live update, technology used to curb frauds associated with electronic payment.

Introduction

Fraud is an issue with psychological, economic and legal ramifications for both the public and private sectors spanning geographic regions (Tagaris, 2008). Electronic payment (e-payment) is an online service that allows user to make payment using internet mode of –payment (mark, 2008).

Hundreds of electronic payment systems have been developed to provide secure internet transactions.

The year 2008 was a year of economic turmoil and financial crises characterized by housing collapse, mounting foreclosures, and pervasive liquidity constraints as well as deteriorating financial conditions especially in the second half of the year coupled with the emergence of new payments types, the growth of electronic payments types and the growth of electronic payment, also opened up new opportunities for payment fraud.

Morgan (2009) viewed that since 2005, the Association for Financial Professional (AFP) has examined the nature and frequency of fraudulent attacks on business-to-business payments as well as the industry fraud-risk tools that organizations use to control payment frauds. The results of the 2009 AFP payment fraud and control survey show that payments fraud is rampant. A majority of organization experienced attempted or actual payments fraud in 2008. These results also underscore the importance of fraud control measures to mitigate risk and reduce exposure to losses from emerging assaults to payment. Association for Financial Professional (2008) held the view that safeguarding their organizations against payment fraud continues to be a major concern of treasury and finance professionals. Repeated reports of cheque scams, data breaches and losses from online commerce reinforce the need to strengthen defences against attempted fraud. In January 2008, the AFP conducted a survey to spotlight the type and frequency of payment fraud experienced by organization in 2007. The survey was a follow-up to similar AFP surveys in each of the previous three years to measure the prevalence of payment fraud and the weapons that organizations deploy to fight against it.

Furthermore, the association in 2008 did a survey to seek and reveal the gaps in payment systems defenses that resulted in financial liability for some organizations and the fraud control measures that other organizations use to prevent financial losses to payments fraud. Responses to the survey when identify best practices that protect organizations against fraud in cheque, Automated Clearing House (ACH) and card payments for both internal and external sources. The survey was also designed to focus attention on the security measures that organization are adopting to protect online payments and cash management data.

The key findings of the study in 2009 regarding payment fraud and control revealed that seventy-one percent (71%) of organization experienced attempted or actual payment fraud in 2008.

Large organizations were more likely to have experienced payments fraud than were smaller ones. Eighty percent of organizations with annual revenue of over $ 1 billion were victims of payment fraud in 2008 compared with 63 percent of organizations with annual revenue under $ 1 billion. It was also reported that fraud has increased in 2008 compared to 2007. Furthermore, thirty-eight percent of organizations experienced increased fraud activity during the second half or 2008 as economic conditions worsened in the United States. Nine out of every ten organizations (91 percent) that experienced attempted or actual payment fraud in 2008 were victims of cheque fraud. The percentage of organization affected by payment fraud via other payment methods were Automated Clearing House (ACH) debit (28 percent), consumer credit/debit cards (18 percent), corporate / commercial card (14 percent) and wire transfers (six percent)

Frauds in Electronic Payment

Mark (2004) stated that online payment fraud is big business, costing UK (United Kingdom) e-commerce retailers an estimated ∑ 535million per year, becoming increasingly Savvy, strategically targeting sensitive consumer data in their efforts to pose as legitimate customers to unwary online merchants. There are so many frauds in electronic payments. They are purchase 5 comes, Money transfer Fraud, Internet Marketing and Retail fraud, internet Ticket fraud, Phishing, Identity fraud, Fraud Involving Paper-Based Payment Systems, Cheque Fraud, Automated.

Clearing House (ACH) Fraud, Business-To-Business and Payments Fraud and Consumer Electronic payments Fraud (Forestor, Morrison, 1994).

i. **Purchase 5 Coms:** This is done when a buyer in another country approaches many merchant though cheating on them but directly asking them to pay using credit card. The merchant thinks that a buyer will actually pay using credit card. Once goods or articles are in his custody, he would just change his website, and money for those goods would never been accounted for again.

ii. **Money Transfer Fraud:** According to Hsu (1975) is the most common types of electronic payments. An individually asks another person to pay certain amount into his banks, with the account number given, what some banks do are to transfer the money into the wrong account. Once such happen, the people involve will delete any trace of such transaction and the owner suffers the lost. In most cases it is rampant when somebody wants to transfer money to foreign company or bank.

iii. **Internet and Retail Fraud:** Spinello (2000) stated that internet marketing and retail fraud is a fast growing area of internet fraud perpetrated by dishonesty. Internet marketing and retail website, the customer is tricked by a legitimate looking website and effective marketing into giving their credit card information.

iv. **Internet Ticket Fraud:** Cline (2007) stated that a variation of internet market fraud is to offer tickets to buy after events, such as concert shows, the tickets turned out to be fake or are simply never delivered.

v. **Phishing:** Spinello (2000) described phishing as the act of attempting to fraudulently acquire sensitive information such as personal and credit card details by masquerading as a trust worthy person.

vi. **Fraud involving electronic fund transfer:** It is possible for private encryption keys to be stolen or used without authorization. Submitting false identification to obtain the public private key can do this. If the private key is holding on a smart card, the access control obtains the key (Osuagwu, 2008) this would enable unauthorized people to order goods and services on line.

vii. **Identity Fraud**: Langford (1991) stated that users can disguise their identities, whilst online consumers of government services will need to be confident that they are dealing with the legitimate government agency not knowing they are simply fraudsters. The user needs to be sure the provider is genuine and providers need to be sure that legitimate users are making use of services.

viii. **Fraud involving paper based payment systems:** A fraudster can open a bank account with false identity and issues cheques in excess of the credit balance in the account to obtain online goods or services. If the business or government agency that provides the service does not wait for authentication checks to be carried out, it exposes itself to fraud risk.

ix. **Cheque Fraud:** Association for Financial Professionals (2008) stated that cheques continue to be the preferred target for criminals committing payment fraud. Moving from cheques to electronic payment could be a fraud-fighting tool. Almost all organizations (94 percent) that experienced attempted or actual payment fraud were victims of cheque fraud in 2007. This percentage is relatively unchanged from that reported for 2006.

x. **Automated clearing house (ACH) Fraud:** ACH frauds are always caused by not using ACH debit blocks or Automated Clearing House. ACH debit filters. It can also be caused by not using Automated Clearing House (ACH) positive pay, and failure to adopt effective internal procedures and bank fraud control services were the most frequently cited reasons for he such loss (Association for Financial Professionals, 2008).

xi. **On line payment Fraud: Hackers attacks, data breaches network:** Customers pay wrongly with fake account number, after which the fraudsters close the fake account (Association for Financial Professional 2009).

xii. **Business-to-business card payment fraud:** Seventy-eight percent (78 percent) of organizations that experienced fraud via the use of an organization own corporate/commercial card indicated that an external party perpetrated the fraud. Seventy percent of such organizations reported that an unknown external party committed the fraud. Using business-to-business card payments, so many organizations have suffered fraud. Just one out of six organization tested, just accepted corporate/commercial cards from its business-to-business partners suffered a financial loss resulting from fraud using such cards.

xiii. **Consumer Electronic payments Fraud:** The Association for Financial Professionals, (2008) stated that ten percent of organizations that accepted electronic payment from consumers indicated that they were victims of attempted or actual consumer Automated Clearing House (ACH) and / or card payments fraud. In 2007, Consumer electronic payment fraud targeted the three forms of payments, which are credit cards, Automated Clearing house (ACH) and signature debit cards.

Control Measures in Electronic Fraud

Just as one protects one's business with locks on doors and burglar alarms; it is vital to make sure that all payments made though computers are protected against the latest threats (Angus, Alan, 2009). The measures are so many. They include Firewalls, Cryptography or Encryption, Pass-words, Anti-virus or Anti-malware, Blometric Authentication, Multifactor, Authentication, Maintain and Information Security Policy, Online Payment Fraud Control, business-To-Business card payment Control, Check Fraud Control and Automated Clearing House (ACH) Fraud Control.

- Osuagwu (2008) saw firewall, as one of the key defense lines for the electronic payment is use. Firewall is a security system intended to protect an organization's network against external threats, such as hackers, coming from another network such as the internet (Osuagwu, 2007) A firewall prevents computers from external attacks in the network and vice versa. All communications is routed through a proxy server outside of the organizations network. Proxy server intercepts all messages entering and leaving the network (Wolfe, 2003). The proxy server decides whether it is safe to let a particular message of files pass through to the organization's network. It is also a firewall component that manages internet traffic to and from a Local Area Network (LAN) and can provide other features such as documents caching and access control. Firewall uses several techniques like packet filter, application gateway, and circuit level gateway and proxy server.

- Cryptography as a control measure is used in application present in technologically advanced societies. Cryptography is used to secure the ATM cards, computer password and electronic commerce. In cryptography, encryption is the process of transforming information (referred to as plain text) using an algorithm (called ciper) to make it unreadable to everyone except those possessing special knowledge, usually referred to as key. The result of the process, is encrypted information. Encryption is also used to protect data in transit for example, data being transferred via networks (e.g. the internet, e-commerce), mobile telephones, wireless microphones, wireless intercom system, blue tooth devices and bank automatic teller machines. One of the earliest public key encryption applications was called Pretty Good Privacy (PGP), according to

Paul Rubens. It was written in 1991 by Phil Zimmermann and was bought by network associates in 1997 and is now called PGP corporation. (Osuagwu, 2007).

- Anti-Virus : The term “Virus” is used to describe self-replicating computer programs that propagate themselves between file on a computer and even between computer (Cornwall,
- 1985). Anti-virus capabilities are a feature of some network and host-based firewalls. The best way to protect your organization against viruses is to use a good-quality commercial anti-virus package. We have some anti-virus kits in the market like Avas, AVG, so many versions, Norton and others (Langford, 1995).
- Biometric: Authentication is a brand new technology used to indicate whether people are actually who they say they are using traits unique to them (Osuagwu, 2008). These traits include finger print patterns, the arrangement of tissue in the eye’s iris and the timbre of a person’s voice. There are three factors used to authenticate an individual; something a person knows that is commonly a password or PIN access is granted. Something a person has, most commonly a physical device, referred to as a token. Tokens include self-contained devices that must be physically a small screen where an OTP is displayed, which the user must enter into an interface to be authenticated by the backend server. Something a person is, most commonly a physical character such as fingerprint, voice pattern, hand geometry or pattern of veins in the user’s eye. This type of authentication is referred to as biometric and often requires the installation of specific hardware on the system to be accessed (Osuagwu, 2007).
- Cheque fraud control best practices. Association for Financial Professionals (2009) stated that tight internal controls and positive pay services ensured that organization did not suffer a financials loss from cheque fraud in 2007. Over three quarters of organization reported that positive pay or reverse positive pay was responsible for preventing financial loss from cheque fraud. Payee positive pay prevented cheque fraud loss at 40 percent of organizations. These services combined with internal controls to stop the financial drain of cheque fraud. More than two out of five organizations indicated

that daily reconciliation and internal controls such as separation of duties prevented financial loss.

	All Organization	Revenues Over $ 1	Revenues Under $ 1 billion
Positive pay	77%	76%	77%
Daily reconciliation	45%	46%	42%
Internal Controls	43%	46%	36%
Payee positive pay	40%	49%	245
"Post no cheque"	21%	29%	12%
Timely cheque return	16%	14%	22%
Other	9%	8%	9%

Percentage of organization not subjected to financial loss from cheque fraud in 2008.

- Automated Clearing House Fraud (ACH) control best practices: Despite having been victims of attempted Automated Clearing house (ACH) fraud, organization do not suffer financially because they are protected by their bank's anti-fraud services and by implementing tight internal controls. Three-quarters of organizations (76 percent) indicate that ACH debit blocks prevented financial loss from Automated Clearing House (ACH) fraud and 6 percent credit Automated Clearing House (ACH) debit fitters with their defense. Large organization with annual revenues over $ 1 billion and ACH debit filters with preventing financial loss than the smaller organizations (Association for Financial Professionals, 2008).

- Business- To-business Control (B2B): With continued growth in the use of corporate cards, especially purchasing cards for B2B

  Payments organizations have implemented a range of control against fraudulent use of teir payments organization have been put in place at various stages of card administration at program set up, as an' on-going procedure and as part of the management oversight function. As an on going procedure, most organizations that use corporate cards require original receipts for purchases and / or print-outs of web confirmations of purchase. When setting up the program, organization' must define card spending limits by employees or by employee level also assign a permanent administer to train cardholders and monitor usage (Association for Financial Professionals, (2008).

Importance of electronic payment

Technologies like internet may be changing, the way government interacts citizens and businesses, but that's only part of the puzzle. What happens behind the web site is fundamental; in the way government business is being conducted. Electronic fund transfer is made easy by the use of electronic payment. Real time processing system allows one and one's clients easy, secure and instants access to the payment system. Organization would save on administrative cost. It reduces queuing at physical counters. It improves economy by direct transfer of funds. It secures payment by direct transfer of funds. It secures payment processing to world-class authentication and it improves free operational, as well as technical support.

Conclusion

Assaults against the payment system by criminal intent on committing fraud continued at full force in 2007. The prevalence of payments fraud and the varied methods by which it is carried out requires the constant attention of treasury and finance professionals responsible for safe guarding their organizations assets. Organization should be on guard against internal payment fraud, as well as fraud from external sources.

Effective defence payment fraud requires a range of fraud fighting tolls. Best practice organizations employ a two –pronged approach continues to promote the awareness fraud issues and encourage the use of best practices by treasury and finance to improve the prevalence, methods and prevention of payments fraud through regular surveys on the issue.

Recommendation

The battle against payments fraud would require innovative technical tolls and high alert to guard against the new technical capabilities and practices of criminals. Also, the use of instant payment notification, use of multiple payment options and fast ordering system, with live update technology would help to reduce fraud associated with electronic payment.

References

Angus, W. & Alan, Y. (2009). *Network infrastructure security. New York: Springerc*

Association for Financial Professionals (2008). Payment fraud and control survey. Report of survey results

Association for Financial Professional (2009). Payment fraud and control survey. Report of survey results

Cornwall, H. (1985). *The hackers handbook century communication.* London McGraw Hill Inc.

Doug, T. (2006). *Creating and maintaining proper system for electronic record keeping*. New York:

Forestor, T. Morrison, P. (1994): Computer ethics cautionary tales and ethical dilemmas in computing. London: MIT Press.

Hsu, L.S. (1975). *The Political Philosophy of confuciamsm. London: Curzon Press.c*

Jacob, U. (2004). Measure and condition of success in public sector knowledge network. Cambridge: M.I.T Press.

Langford, D. (1995) Practical computer ethics. London: McGraw Hill Inc.

Langford, D. (1999) Business computer ethics London: Addison –Wiley Press.

Mark, H. (2008). Critical issues and practical cheapener of IT tolls for policy analysis and program evaluation. Cambridge: M.I.T Press Morgan, J. (2009). Payment Fraud and control survey (www. AFP online org.)

Osuagwu, O.E. (2008): *Insight into the new frontiers of computer forensics and cyber criminality*. Owerri: OIPH Press.

Osuagwu, (2007) Blocking credit card theft though Biometric authentication system. Proceeding of the international conference of the Nigeria Computer Society.

Wolfe (2003): Computer and security, EI Severe science, Ltd PP 26 – 28 (www.sciencediretical).

Spinellor, R. (2000). Cyber morality and law in cyberspace. London: Jones and Bartlett Publishers.