*Asia Pacific Journal of Marketing & Management Review*____ ISSN 2319-2836
Vol.2 (3), March (2013)
Online available at indianresearchjournals.com

FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES

LINA FERNANDES

LECTURER
DEPARTMENT OF BUSINESS AND ACCOUNTING
MUSCAT COLLEGE
SULTANATE OF OMAN.

ABSTRACT

The rapid growth of internet over the past several years has increased the use for Electronic business (e-business). E-business is done online without face to face interaction. Several Electronic payments (e-payments) systems have been developed and are increasing used in e-business. This has given birth to electronic frauds (e-frauds) and it has become a major problem in the electronic payment system. As internet increases business opportunities, there are new fraudulent and sophisticated techniques being developed by fraudster. For the merchant managing frauds has been major and growing cost. This paper provides an overview on e-payment frauds. It presents statistics on actual payment frauds and revenue loss due to frauds. Several measures for fraud detection and prevention are discussed. The scope of this research is to minimize the fraud in e-payment transaction and also the revenue loss by taking the detective and preventive measures.

KEYWORDS: E-frauds, e-business, security, measures, prevention, detection.

INTRODUCTION

With the development of the Internet in the 1990s and subsequent evolution of electronic commerce (e-commerce) have given rise to a dynamic business environment where transactions take place without face to face interaction. The International Telecommunication Union reported that internet is quickly becoming the first stop for people for making decision about buying services and products over internet and that the number of internet users has reached 2.3 billion in 2011. The increase in the volume of transactions has given rise to numerous electronic payment (e-payments) systems. Recent studies (Manning 1998, Wortington 2000) agree that electronic payment transactions have been in use for quite some years, like automatic teller machines (ATM), credit and debit cards, direct deposit and direct payment. Innopay Online payment report (2011) found that there is massive growth in the market for digital goods and this has given rise to numerous payment systems making the process of payment over the Internet easier for consumers. E-payment ensures smooth, secure and efficient transactions in e-business.

However, the development of e-payment methods have expanded and with it the fakery has inevitably kept pace. As a result, the consumers face a number of risks to personal information and have second thoughts of giving their credit account information over internet (Centeno

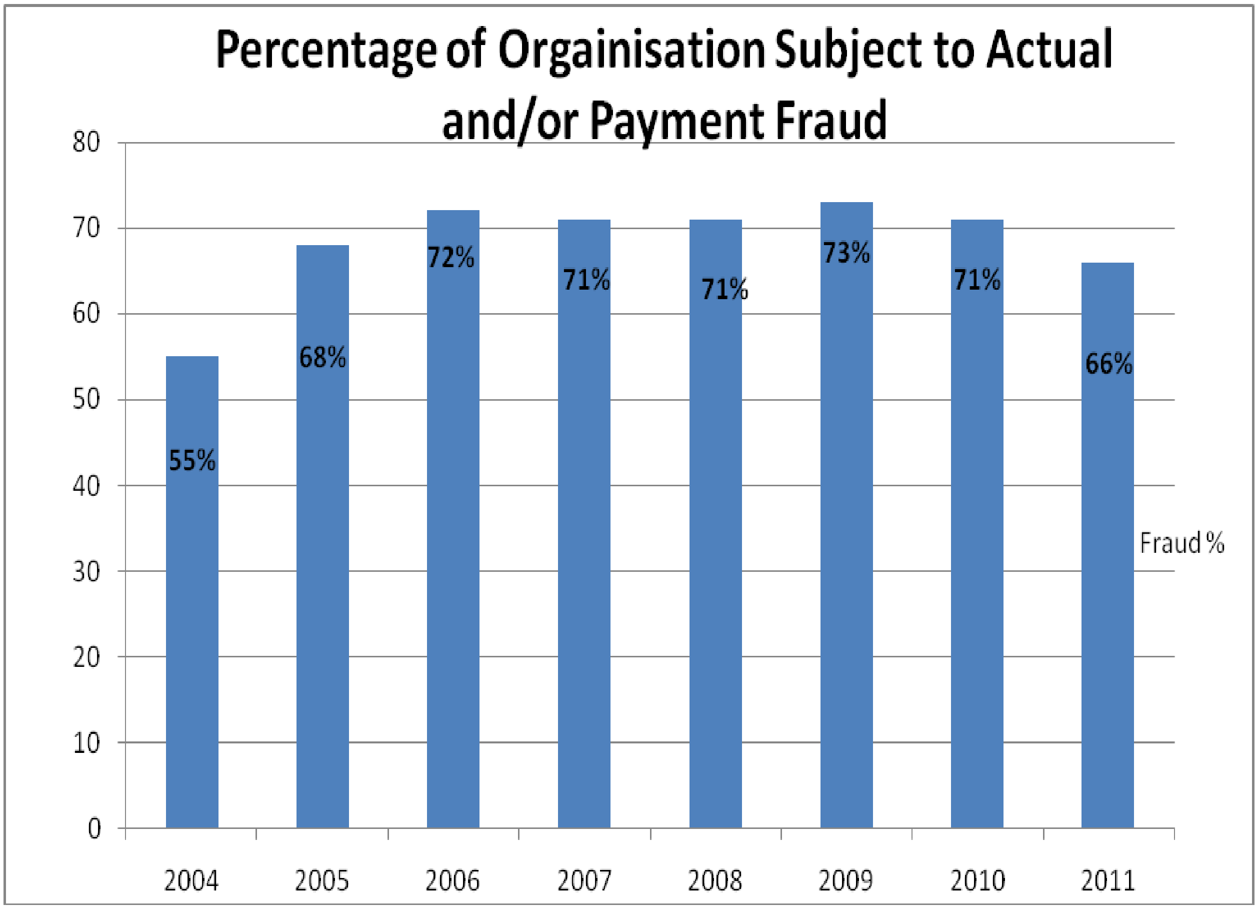
(2002). A recent study found that more than 7 million consumer complaints have been received during the period from 2007 to 2011and a total of 990,242 of these complaints were related to frauds The Consumer Sentinel Network (2012) (CSN). Consumers have reported paying over $1.5 billion in those fraud complaints. According to CyberSource (2012) found that merchants have reported losing an average of 1.0% of the total online revenue to fraud. It is also reported that the fraud rate of international order is 2% more than domestic orders. For the merchants managing e-frauds remain to be major and growing cost.

Fraud in e-payment transaction is a global problem. We find fraudsters maneuver in all countries and industries. The purpose of this research is to study frauds in e-payments transactions, in order to point out some prospective threats and countermeasure required to reduce frauds. This paper discusses e-fraud (electronic fraud) and the different types of frauds in e-payment transactions. It further addresses various possible measures for prevention and detection of frauds in order to minimize frauds and make internet a safer, sound and trusted environment to consumers and merchants.

OVERVIEW OF E-PAYMENT FRAUDS

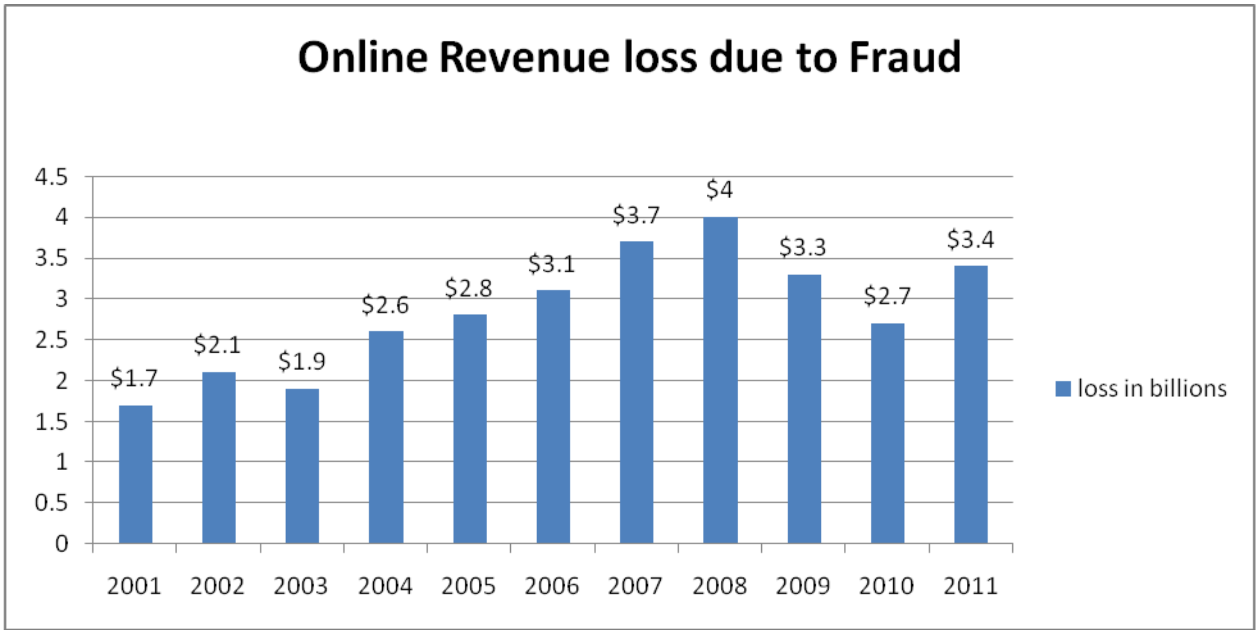
Graycar & Smith (2002) has defined fraud as a “act or instance of deception, an artifice by which the right or interest of another is injured, a dishonest trick or stratagem.” Bergmen (2005) define E-Fraud as “ a deception deliberately practiced to secure unfair or unlawful gain where some part of the communication between the victim and the fraudster is via a computer network and/or some action of the victim and/or the fraudster is performed on the computer network .” The USA Department of Justice (DOJ) defines e-fraud as “ a fraud scheme that uses one or more components of the Internet – such as chat rooms, e-mails, message boards, or web sites – to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institution or to other connected with the scheme”

With more and more people using internet in recent times e-fraud is becoming common because internet allows fraudsters appears anonymous. Internet has been a suitable method for committing fraud because the Internet allows hiding real identification of people who deal with it and thus the fraudsters remain anonymous. As internet increases business opportunities the criminal develop more sophisticated and effective ways to scam online. Commission of European Committee (2008) report summarized the fraud problem by saying “Fraud against means of payment (payment fraud) remains a threat to the success of the internal market for payments. Payment fraud affects the consumer confidence in non-cash means of payment and ultimately the real economy.”



Source: AFP survey (2012)

Organizations find that the frauds in the e-payment transaction are increasing year after year. Association for Financial Professionals AFP (2012) has reported percentage of organizations subject to attempted and/or actual payments fraud has shown an increase from 2004 to 2009, while from 2010 and 2011 showed a decline in attempted and actual payment fraud. The report also showed that it the larger organization are targets of payment frauds than smaller ones. 81% of the organizations with annual revenue over $1 billion were victims of payments fraud in 2011 compared to 55% organization with less than $1billion revenue. It is also observed in 2011 that it is the larger organizations that have experienced decrease in fraud while the smaller organizations continue to experience increase in the fraud activity.



Source: CyberSource

According to the CyberSource (2012) the loss of online revenue to fraud in 2011 showed a decrease and the merchants reported 33% decrease in the orders lost to fraud which was due to effective fraud measures. In north America the total revenue loss was approximately $3.4 billion which is around $700 million increase over 2010. This was for due to increase in the rejection rate since 2009. The merchants reported that 2.8% of the orders were rejected due to suspicion of payment fraud. It is also found that international orders are riskier than domestic orders. It is reported by the merchants that the international order fraud rate is three times more than domestic.

TYPES OF E-FRAUDS

In order to assess the risks of and combat payment fraud there should be an understanding of its many facets. E-payment frauds have a multiplicity of types and there is no exact number or fixed list of these types. Frauds are classified as online fraud and offline frauds. Online frauds occur when fraudster possess legitimate company to obtain sensitive personal information and illegally conduct transactions in the existing accounts. Phishing and spoofing are examples of online frauds. Online frauds occur when fraudster steals personal information such as credit number, bank account number or other identification and uses it repeatedly to open new account or pledges transaction in the real individual/company’s name. Offline fraud includes credit card fraud, phone solicitations, print fraud, check scams and mail fraud. Department of Justice (DOJ) U.S has divided frauds(computer fraud) into three categories: 1) crimes in which computer hardware, peripherals, and software are the target of a crime; where in the fraudster obtains objects illegally: 2) crimes in which the computer is the immediate subject of a crime, that is the attacks is on a computer or a system, destruction or disrupting of which is the damage caused; and 3) crimes in which computers and related systems are the means or "instrument" by which ordinary crimes are committed, such as theft of identities, data, or money or the distribution of child pornography. There are different types of e-fraud and all of these attack in a slightly different way. Fraud can occur in a number of ways as listed below.

Account Hacking: Hacking includes gaining illegal entry into a person computer (PC) system. Fraudster use compromised customer credentials to hijack the origination system and use it in the lawful account holder's name. Corporation are also targeted and also seen on a rise. Attacks are aimed

Identity theft: Identity theft/fraud refer to crime in which fraudster illegally obtains and uses another person personal information in some way that involves deception or fraud to gain something of value. Identity theft/fraud is the most serious crime for the person whose information is stolen as well as the financial institution.

Phishing : Phishing is a well-known technique for obtaining confidential information from an user by posing as a trusted authoring. Phishing is an attempt by fraudster to 'fish' for your baking details through emails with attachment or hyperlinks. The e-mail appears to be send from legitimate organization to trick people in order to reveal sensitive information. On clicking the attachment or the hyperlink the computer system get infected with malware. During the next online transaction the malware will activate and steal private and personal financial information, including credit card numbers, PIN number which is used by fraudster to steal money from the account. Malware or 'Malicious Software' is software which includes computer viruses, worms, Trojan Horses, spyware and other malicious software.

Spoofing or Website cloning: This is an act of creating a hoax web site or to say duplication of a website for criminal use. The fraudsters use legitimate companies name, logos, graphics and even code. This usually take form of know chat room or trade sites where in people would innocently giving out personal information to criminals or make a fake purchase of a product the does not exist.

Internet Gambling (Virtual casinos): The Internet has made certain types of gambling possible. A person in India or china from his home can participate in internet poker game in Caribbean over the Internet. CERT-LEXSI (2006) as cited by McAfee (2009) ther are around 15000 active online gambling sites in 2006 out of which 1766 operate on license. Although there are operating online casinos in an honest manner, the potential for fraud connected with casinos and bookmarking operations is far greater. Online gambling establishment appear and disappear with regularity, collecting from losers and not paying winners without any fear of being appended and prosecuted.

ACH Frauds : Automated Clearing House (ACH) Fraud is basically information fraud. With the increase in ACH transactions for corporate payments obviously there is increase in the ACH frauds. The fraudsters access the account information and route number illegitimately to steal funds directly from accounts. Government payment, payroll and other online payment face these frauds. In the year 2011, 17% of the organizations that are victims of fraud, suffered financial loss (AFP 2012)

Check frauds: Check frauds continue to be a threat to financial security. Electronic check frauds can be easily committed; the fraudster needs scanner, printer and desktop phishing software. The most common forms of check fraud include altering check, forging endorsement, counterfeiting checks and creating remote checks. According to the AFP Report (2011) 14% of the victims of the organization suffered financial loss due to check fraud.

Lottery frauds: One will receive scam emails informing of winning a substantial amount of money in a lottery draw. When the receiver reply's, the sender then asks for bank account details and other personal information so they can transfer the money. These emails are fake and may ask to pay a handling feel that will lead to loss of money and your personal information which may be used in other fraud.

Nigerian advance fee fraud (419 fraud)" This e-fraud is the most popular and lucrative fraud, which is named after the section of Nigerian law that covers it "419". The hoax often arrive with bulk mailing or family member email of asking the recipients to enter into business and getting money transferred with huge commission in return. Once the contact is established the fraudsters request money in advance which need opening of an account in the bank or paying some fee which leads to troubles and expenses.

MEASURES FOR FRAUD PREVENTION AND DETECTION

With the increase in e-commerce sales the merchants face challenges to reduce frauds in e-payment transactions. E-frauds start with diversion of personal information. A poorly protected computer , a trash or recycling bin, an email message or chat on internet exposes to fraud. For the merchants the majority of fraud loss is due to consumer's claim of fraudulent account used and/or subsequent information from additional orders placed by fraudster. Fraud has become the persistent threat to merchants in e-payment transactions in e-business. It is impossible to totally eliminate the chance of fraud but timely measures taken can reduce the frauds. The merchant and the financial Institution take the necessary measures in combating fraud effectively. Fraud prevention involves taking measures to stop fraud from occurring and while fraud prevention fails then the merchant takes steps to detect the frauds quickly and stop it as soon as possible. Fraud prevention and detection involves planning, detecting and avoiding risk. Frauds can be controlled by monitoring the internet threats, understanding the customer and implementing security measures. Different techniques are required as there are different types of fraud in e-payment transactions.

Fraud Detection Tools

Fraud detection tools are those that are used to assess the probability of frauds in payment transactions. Cyber source 2012 shows that 56% of merchants surveyed utilize an automated screening system. Every merchant doing e-business should be aware that frauds cannot be totally eliminated but can be controlled with protective measures. Some of these measures are to counter internal threats and some are to stop external threats. Some are relatively inexpensive while others are expensive involving huge amount of money. The anti-fraud tool are required to detect frauds accurately and in time, automate processes when required, adapt to changing patterns of fraud and behavior of customers. Some of the Anti-fraud tools are include

Universal Payment Identification Code (UPIC):A UPIC is a unique account identifier that issued by financial Institution is developed by Electronic Payment Network (EPN) . This will allow merchants doing e-business to receive e-payment without disclosing confidential banking information.

ACH Block (Automated Clearing House): This can place a 'block' preventing ACH activity when the merchant account is unauthorized for ACH transaction. The merchant can receive alert from the bank to ACH transactions that don't meet predefined conditions and then take decision whether to accept or decline the transaction. This enables the merchant to stop e-fraud before it happens.

Fraud Detection Software/tools: The organization doing e-business should install fraud detection software/tools that can detect fraud and to reduce fraud rates. The software will give fraud results and the merchant will be able to take decision whether to accept, reject or review the transaction. There are different categories of fraud detection tools which are grouped into validation service, proprietary data, purchase device tracing and multi-merchant data. Some of the tool are AVS – Address Verification Service, CVC – Card Verification Code and Risk Management Modules or Fraud Screens. According to CyberSource (2012), 56% of the merchants' survey made use of these tools.

IP Address Locator: It provides the merchant the data on user's exact location and displays its origin on a map, giving approximately the city and state. It also calculates the distance between the billing address of online buyer and actual location of persons entering the orders. This is not a fool proof that visitor is using a proxy; however the merchants can apply authentication measures for transaction wherein there is a great difference in distance and take decision on which transaction to review and which to allow. There should a check to if any users are using anonymous proxy servers to hide their IP address, which can be done by obtaining a list of anonymous proxy server.

Minimizing Charge backs

Merchant are concerned exclusively in minimizing charge backs. E-payment fraud has an impact on the profits in different ways like revenue loss, cost on staffing for manual review and administration of fraud claims. Merchant can take total risk management pipeline view of operation and can gain efficiencies. The risk management pipeline view involve the following activities Automated screening, Manual review, Order dispositioning and Fraud claim management

Automated Screening: Merchants that handle large online orders should employ automated order evaluation system or anti-fraud detection tools. These tools would enable the merchant to determine if an incoming order represents fraud risk. Merchants deploy more than tool for automated screening process. The automated order screening would process produces three results 1) order accepted without review 2) Orders flagged for further review and 3) automated order rejection.

Manual review: Order that are flagged and are not accepted in the automated order screening stage will enter a manual review stage. During this stage additional information is required to be collected to decide if the order should be accepted or rejected. This is a very critical area as it is the larger portion of fraud management operation and can be expensive when merchants divert more staff time to order review or increase staff levels. The merchants should improve on automated screening accuracy and reduce reliance on expensive manual review process.

Order dispositioning: This stage ultimately results in to accept or reject the order. Orders which appear suspicious should be rejected. This is a very sensitive stage as care should be taken not to reject good customers' orders as lost customers and negative word of mouth can adversely impact future revenues. It is important to bear in mind that poor screening, over cautiousness and lack of expertise would lead to high rejection rates

Fraud claim Management: Orders that are fraudulent would be presented to merchants in two ways as direct request for credit (they make fraudulent use of account) or as a charge back. The action to be taken by the organization is to make a direct contact to the customer to address fraud claims as this would avoid charge back fees by merchant bank. If the customer directly contacts the merchant then either the merchant should handle the dispute directly with customer or advise to initiate chargeback process. Organization have to balance the cost of implementing controls with potential or perceived risk of loss.

Security in e-payment process

Secured e-payment transaction system is critical to e-business. Without a secured payment trasaction system, e-commerce will be a castle build in the sand. There are two commonly used secure e-payments Secured Socket Layer (SSL) and Secured Electronic Transaction (SET).

SSL is a secured connection for cyber shoppers to send payment information to e-tailor's web. The objective of SSL is to ensure confidentiality, by encrypting the data that moves the client and server computers when exchanging information. It also provide authentication by use of RSA algorithm. SSL provides a secured connections for payment for merchants and customers.

SET is a messaging protocol designed by VISA a nd MasterCard for securing credit card transaction over open network. The main feature of SET protocol is that all sensitive information sent to all parties (customer, merchant and Bank) are encrypted, all three parties are required to authenticate with certificates from SET certificate authority and the merchant never sees the customer card number in plain text. SET ensure that payment process is private, convenient and secured. It allows customer do internet transaction at ease as it is easy and simple; and also without any fear.

Awareness and Education

Awareness of security risks by merchants and consumers plays an important role in reducing fraud in e-payments Merchants awareness and education is also important. They should be aware of the types of frauds, statistic and best practices. Consumer awareness and education is important in order to reduce Identity theft or payment data theft. This would help the user in adopting active and cautious attitude when doing transaction using internet. It could teach them to be aware of possible risks, avoid e-scams, and minimize giving information to merchants when buying online. This would increase consumers' responsibility in keeping personal data secured in physical and virtual world

Protection from Internal Threats: Organizations should take measures to minimize internal tampering with the computer system. The Management should take precautionary measures which include monitoring the use of computers and network by employees. The physical access to computer should be limited by use of passwords, magnetic card reader and biometrics to verify the identity of the user. Management should stress the importance of keeping the password confidential to employees. There should be responsibility for custody, safeguarding and limiting access to computers.

Fraud prevention not only saves money but also cost money. In Fraud prevention organizations have to be highly cautious as false rejection of non-fraudulent transaction will cost the company. At times, in spite of using technology tools in detection of fraud, fraud prevention involves manual procession of the transaction. Different techniques may be needed for different kind of fraud. The organization should formulate successful strategy for detecting and preventing fraud and thereby eliminating fraud losses.

Conclusion:

With the development of e-payment options, the number of online shoppers and merchants has beeb gradually rising. This has provided fast, reasonably safe and relatively low cost operations for e-business. As the financial and other data is become digitized, the opportunities for e-payment frauds also continues to rise. Furthermore, new fraudulent and sophisticated techniques are being developed by the fraudster. The merchants and the consumers have to be cautious and take preventive measure to minimise the fraud in e-payment transactions.

This paper first has provided an overview of payment frauds in e-business which began with the definition of fraud and e-fraud. It then provided the statistics of actual payment frauds and online revenue loss due to frauds. It further described the different types of frauds in e-payment. Finally concluded with discussion on prevention and detection measures for payment frauds in e-business which included the tools of detecting of frauds, reducing charge back, securing of e-payment system and need of awareness and education. The study shows fraud detection techniques attempted to maximize accuracy rate and minimize frauds at a low cost level. An ongoing research is necessary to reduce risk and protect merchants, consumers and financial institutions.

References

Association for Financial Professionals(AFP) 2011, 2012, *Payments Fraud and Control Survey Report* by J.P. Morgan, San Diego, USA. Viewed on 02, December 2012,

www.AFPonline.org

Bergman B. (2005), ISRN: LITH-IDA-EX-05/029-SE, *"E-fraud – State of art and countermeasures"* viewed on 5, December 2012,

http://www.ep.liu.se/exjobb/ida/2005/dd-d/029/

Centeno C. (2002), *"Building Security and Consumer Trust in Internet Payments",* Background paper No. 7, Electronic Payment System Observatory (ePSO)

CERT-LEXSI, *"Cybercriminality of online gambling,"* (2006) viewed on 14 November 2012, http://www.lexsi.com/telecharger/gambling_cybercrime_2006.pdf

Commission of European Committee (2008) Report, *"Fraud on non-cash means of payment in EU, Brussels",* viewed on 10 November 2012,

http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf

Consumer Sentinel Network Data Book for January-December 2011, *Federal Trade Commission*, viewed on 16 November 2012,

http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf

CyberSource (2012), :*Online fraud report 2012",* by Mindwave Research, viewed on 18 November 2012,

www.cybersource/product_and_sevices/fraud_management/

DOJ (2001),Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue Almost $8 Million in Cisco Stock to Themselves‟, United States Department of Justice (DOJ), viewed on 22 November 2012

http://definitions.uslegal.com/c/computer-crime/

Graycar, A & Smith, R (2002), *"Identifying and Responding to Electronic Fraud Risks",* Australian Institute of Criminology, viewed 28 November 2012,

http://www.aic.gov.au/media_library/conferences/other/graycar_adam/2002-11-registrars.pdf

Innoypay (2010) *"Online payment r 2010"* report on the current state of affairs in the global landscape of Internet payments by Wijnand Jongen, viewed on 12 November 2012,

http://www.innopay.com/publications,

Wortington, T. (2000); *"Internet Payments for Government Agencies Commonwealth of Australia",* viewed on 4 December 2012,

http://about.Business.gov.au/ipp/ipga/html

Manning, R. (1998); "Electronic Commerce on the Internet" in Olumide, S. A and Falaki, S. O (2001): Electronic Commerce – Promises, Treats, Trust and payment Systems. Conference Proceedings, Computer Association of Nigeria (COAN)

McAfee Report (2012) *" Financial Fraud and Internet Banking: Threats and countermeasures",*

By François Paget, viewed on 8 December 2012,

http://www.mcafee.com/in/resources/reports/rp-financial-fraud-int-banking.pdf