Original Article

International Journal of Forensic Science
Volume 3 Number 2, July–December 2020

"Digital Transactional Fraud in Electronic Era": Current Trend and Unmasking Techniques

Shikha Upadhyay

How to cite this article:
Shikha Upadhyay. "Digital Transactional Fraud in Electronic Era": Current Trend and Unmasking Techniques. International Journal of Forensic Science. 2020;3(2):105–108.

Abstract

The digital revolution and the reasonable, high-speed Internet have together transformed the payments market. Nowadays, the new-age consumer is spending more time on "virtual platforms" and they prefer "digital conversations" means cashless and seamless payments. Frauds related to digital payment have seen a rising trend and there is an urgent need to revamp the secure techniques, transactional scams involving crores of rupees being unearthed in recent decades. The new-age hacker is using more sophisticated, innovative ways to obtain valuable customer information and login credentials to hack into accounts. Customer awareness of online security risks is often poor and they are easily duped into divulging confidential data to criminal groups that can then be used to authenticate fraudulent transactions. To deal with the fraud, we need to adopt various measures to make the digital payments landscape more secure. The current study analyses the current trend of transactional frauds and It also elucidates the impacts that are being faced due to the frauds. Further the study endeavours to throw light on the different types of unmasking techniques.

Keywords: Digital payment; Payment security; Electronic fraud; Online transaction; Fraud detection technique.

Introduction

Information and communication technology (ICT) rapid growth of internet over the past several years has increased the use for e-commerce market where transactions take place without face to face interaction. Internet has been a suitable method for committing fraud because the Internet permits hiding real identification of people who deal with it and thus the fraudsters remain anonymous. Payment fraud is any type of false or illegal transaction completed by a cyber criminal. The perpetrator deprives the victim of funds, personal property, interest or sensitive information via the Internet. In an ecommerce surrounding, payments made in an electronic form, and are therefore called Electronic Payment. Electronic payment is a division of an e-commerce transaction to include e-payment for buying and selling of goods or services accessible through the internet.[5] Several Caseless payments (e-payments) systems have been developed and are increasing used in business. This has given birth to electronic frauds (e-frauds) and it has become a major problem in the caseless payment system.[1] The digital revolution is given opportunity to the users for the various types of electronic services like e-banking, e-transaction, e-shopping, e-payment, etc.[5] An e-commerce cash system delivers proficiency for online transaction. E-commerce frauds can be possible as offline and online in both ways in the online trend of shopping.[3],[9] When fraudster possess legitimate company to obtain sensitive personal information and illegally conduct transactions in the current accounts then it is known as Online frauds. Online Frauds includes phishing and spoofing and hacking. Offline frauds

Author's Affiliation: Lecturer, Department of Forensic Science, Jain (Deemed-to-be University), Bangalore 560069, India.

Corresponding Author: Shikha Upadhyay, Lecturer, Department of Forensic Science, Jain (Deemed-to-be University), Bangalore 560069, India.

E-mail: shikhasivi@gmail.com

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 original individual/company's name. Credit card fraud, phone solicitations, print fraud, check scams and mail fraud are examples of offline frauds.[1,2]

Fraud problems usually comes by different medium, such us - if the original database is hacked from bank or e-commerce database by fraudster in which having all the information related to customer card is stored then in the absence of the credit/debit card fraud can be possible. Fraudster do not want to purchase anything from the shopping cart but still he/she giving the wrong information and make payment transaction as a cash on delivery to harm to the merchant. If credit/debit card information stolen or lost then by using the credit card number and card verification code (CVV) number fraudster can be make payment easily without knowing to the actual user.[3] Based on Big commerce report payment fraudsare divided into three ways: Unauthorized transactions, Lost or stolen merchandise, False requests for a refund, return or bounced checks.[10]

Methodology

Based on our main objective the data collected from different resources for study of current trend of transactional frauds and unmasking technique. The study depend on the descriptive analytical method through the following data sources as follows - Secondary data sources: published research articles available on scientific resource sites like PubMed, Science hub, and Research Gate etc., Books, regulations and instructions issued by the relevant academic and professional bodies in paper and electronic form. The present study is based entirely on secondary data.

Result and Discussion

With digital revolution in technology, the fraudster criminals change their method as well. There are different types of e-fraud and different classifications of the fraud can be presented based on the different viewpoints of the researcher.[4] Some common fraud included:

1. Overview of Types of fraud

Phishing: Phishing is an attempt by fraudster to "fish" for your confidential information such as banking details through emails with attachment or hyperlinks. It usually involves seemingly official notifications or messages, such as official e-mails. Mostly, the email seeks customer to make available sensitive information such as name, password, account number etc. It is a form of social engineering.[1,6,7,8]

Hacking: Hacking includes gaining illegal entry into a person computer (PC) system. Fraudster use compromised customer credentials to hi-jack the origination system and use it in the lawful account holder's name. Corporation sector is mostly targeted by hackers.[1]

Malware: It is the term for malicious software code. Especially negative written computer programs now exist that enable intruders to fool customers into believing that security is protecting customers during online banking transactions. Malware hi-jack the customer's browser and transfer funds without the knowledge of the customers. It performs especially account information theft and fake website substitution.[8]

Trojan Horse: It is an application in which the program installed itself into a user's computer via an email, where the program will automatically direct the user of the system to a website which is exactly similar to a Bank website, which built a sophisticated command and-control (C and C) system thatcompletely automates the attacks. After attacking it steal your sensitive information such as bank details.[8] It is also a type of malware.

Pharming: This technique specially used in hijacking the Domain Name System (DNS) means web address of service provider. This occurs when a hacker redirects website traffic from a legitimate website to the hacker's fraudulent website without customers knowledge by exploiting vulnerabilities in the Domain Name System.[6,8]

Internet Gambling: Internet gambling is a new trend in internet. A person in US or India from siting his home can participate in internet poker game in over the Internet. Many organizations have been reported there are lots of illegally active gambling sites that appear and disappear with regularity, collecting money and details from losers and not paying to winners without any fear.[1]

In Table 1 all types of fraud in specific manner briefly listed by author on the basis of various sources.

2. Methods used indetection of fraud

There are different methods for prevention and detection of frauds in order to minimize internet

Table 1: Author compilation of different types of fraud on the basis of secondary sources.

S.No.		FRAUD	Reference No.
I.	Investment related internet scams	Online auction and retail schemes, Online Survey frauds	(6)
II.	Business Fraud	Purchase frauds, Online automotive fraud, Counterfeit cashier's check scam, PayPal Fraud, Call tag scam, Money transfer fraud	(6)
III.	Target youth frauds	Internet ticket fraud, Nigerian letter 419 fraud	(1,6,7)
IV.	Miscellaneous internet frauds	Phishing, Pharming, Malware, Spoofing or Website cloning, Trojan Horse, Identity theft, Account Hacking, Automated Clearing House (ACH) Frauds, Internet Gambling (Virtual casinos).	(1,6,7,8)
V	Credit card fraud	Bankruptcy fraud, Theft fraud/counterfeit fraud, Application fraud, Behavioural fraud, Telecommunication Fraud, Computer Intrusion, Card Not Present (CNP), Account Take Over (ATO)	(3,7)

frauds and make internet an innocuous, and trusted place for consumers and merchants. In today's technological world it is impossible to completely eliminate the chance of fraud but by timely correct measures taken by people can reduce the frauds. It can be controlled by monitoring internet threat activity and timely implementing security measures.[1]

Internet frauds had thevarious behaviour characteristics like: Large number of different accounts accessed by a single fraudster; Transactions involving small values in many accounts; More payment transactions than normal in a single account; Higher number of password failures before the occurrence of frauds.[11]

Some of different techniques are discussed in various papers for different internet fraud transactions. Some of important unmasking techniques are given in Table 2.

3. Prevention techniques

As we know it's impossible to completely remove any fraud but with some preventive methods, we

Table 2: Author summarizes the online fraud detection techniquesfrom various secondary sources.

S.No.	Name of Methods/ Tools	How it works -	Methods used for-	Reference No.
1.	Hidden Markov Model (HMM)	It is a finite set of states having a probability distribution that administrates the transition states of card holder. Amount of incoming transaction is compared to the predefined threshold value to define transaction is legitimate or Fraudulent of each card holder.	Credit card fraud detection	(3,12)
2.	A Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning (DST and BL)	Both combines three approaches rule based filter, Dempster-Shafer adder and Bayesian learner. It detects based on combination of current as well as past behaviour together have recorded a profile for every card holder.	Credit card fraud detection	(3)
3.	Blast-Ssaha Hybridization	It is a two-stage sequence alignment. It has two analyzer as name is profile analyzer and Deviation analyzer. Profile analyzer match the sequence with the card holder database. Deviation analyzer compare the incoming unusual data with the past fraud history database.If the transaction knows to suspicious then system will raise alarm and giving alert message.	Credit card fraud detection	(3)
4.	Universal Payment Identification Code (UPIC)	It 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 revealing confidential banking information.	Online payment	(1)
5.	Fraud Detection Software/tools	Merchants doing e-business should install fraud detection software/ tools that can detect fraud and to reduce fraud rates.	Online payment	(1)
6.	IP Address Locator	It provides the merchant the data on user's exact location and displays its origin on a map. 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.	Electronic Payment	(1)
7.	Neural Networks (NN)	Neural Networks (NN) are an Artificial Intelligence (AI) techniques or methods that represent models of biological learning systems. It can be used to distinguish legal from fraudulent transactions, detect Internet fraud on an e-commerce site, predict which transaction may be a fraudulent transaction, etc.	Internet fraud, Credit Card fraud	(13)

can curb payment fraud. Here are a few measures that we can take such as -be aware of the latest trends in online fraud, have a verified payment processor, use antivirus software that will run constant checks, regularly change login and token credentials, set-up strict policies for accessing crucial and sensitive information, emails and transactions with confidential information need to be encrypted etc (sources: iovation).

4. Impact of Frauds

In recent years, cases of banking fraud reported in India risen drastically. The delays in the legal procedures for reporting, and different loopholes in the system have been considered the major reasons of frauds.[14] FIS' fifth annual PACE report showed that over 96% of Indian customers got affected by online payment frauds. E- transactional fraud has an impact on the financial sector far beyond immediate loss of income, since the effects of lower income due to loss of reputation and trust manifest themselves in the short, medium, and long term starting from when the fraud incident occurs (sources: ICAR, Clab 2016, Action Fraud UK, Forbes).

Conclusion

In this paper, different types of fraud, fraud detection techniques and impact are briefly discussed. From the above analysis it can be concluded that digital transactions definitely are on the rise but we have different detection tools also that are available for detecting online fraud. E-fraud prevention such as awareness of security risks by merchants and consumers also plays an important role in reducing fraud in e-payments. Every person should take precautionary measures, be aware about types fraud, detection tools and methods. It's very important for internet users to be careful that not everything on e-commerce platforms can be trusted easily.

References

1. L Fernandes, (2013), Fraud in electronic payment transactions: threats and counter measures, Asia Pacific Journal of Marketing and Management Review, ISSN 2319–2836 Vol.2 (3).
2. 2019 Experian Identity and Fraud Report, Asia-Pacific Edition.
3. J Rana, Priya and Baria, Jwalant (2015). A Survey on Fraud Detection Techniques in Ecommerce. International Journal of Computer Applications. 113. 5–7. 10.5120/19892–1898.
4. M jans, N Lybaert, K Vanhoof, A framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: the IFR2 Framework, The Internal journal of Digital Accounting Research, Vol.9. 2009, pp.1–29, ISSN: 1577–8517.
5. Agrawal, M, and Bansal, A. Factors Influencing Consumer's Intention to Use E-payment System: An Empirical Study,ISSN: 2349–7165.
6. Bansal, U. Online Business Frauds: A Case Study of an Online Fraud Survey Company.
7. Delamaire, L, Abdou, H, and Pointon, J. (2009). Credit card fraud and detection techniques: a review. Banks and Bank systems, 4(2), 57–68.
8. Emefiele, C, Obim, E N, and Nkamare, S E (2018). Impact of Electronic Banking on Detection of Fraud in Nigerian Banking. International Journal of Research in Finance and Marketing (IJRFM), 8(9).
9. Unmask Digital fraud Today, Accenture report, 2018.
10. Nejad, S H T, Nikbakht, M, and Afrakhteh, M H (2017). An Overview of the Bank Fraud and Its Detection Techniques through Data Mining. International Journal of Mobile Network Communications and Telematics (IJMNCT) Vol, 7.
11. Kovach, S, and Ruggiero, W V (2011). Online banking fraud detection based on local and global behavior. In Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France (pp. 166–171).
12. Mhamane, S, and Lobo, L M (2012). Use of Hidden Markov Model as Internet Banking Fraud Detection. International Journal of Computer Applications, 45, 5–10.
13. Al-Khatib, A (2012). Electronic payment fraud detection techniques. World of Computer Science and Information Technology Journal (WCSIT), 2(4), 137–141.
14. Ainsley G, Andre J B, Brahma E B, Rodney D (2019). Impact of Frauds on the Indian Banking Sector International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278–3075, Volume–8 Issue–7S2.