International Journal of Humanities and Social Science Research
ISSN: 2455-2070; Impact Factor: RJIF 5.22
Received: 01-01-2020; Accepted: 02-02-2020; Published: 01-03-2020
www.socialsciencejournal.in
Volume 6; Issue 2; 2020; Page No. 01-05

Repercussions of e-frauds on e-commerce-an analytical study

Sudhamani NS[1], Vidya VC[2], Saraswathi KV[3]
[1] HOD of Commerce, Seshadripuram Independent PU College, Magadi Road, Bengaluru, Karnataka, India
[2] HOD in Computer Science, Seshadripuram Independent PU College, Magadi Road, Bengaluru, Karnataka, India
[3] HOD in Mathematics, Seshadripuram PU College, Yalahanka Branch, Bengaluru, Karnataka, India

Abstract
The revolution of e-commerce has led the e-payment systems to be very popular with the on-line buyers. The magnitude of the on-line transactions is rapidly increasing by every day. The security concerns have been on the rise with the increase of the volume of on-line businesses transactions. The smart-phones, user-friendly apps, easy user-interface has made electronic business to Worms, Trojans, viruses, phishing, pharming, spoofing, man-in the middle, denial of service attack, transaction poisoning and spamming are the most common threats.

Keywords: fraud, E-payments, E-commerce

Introduction

In recent years, various mobile services have been introduced for in-store payment. While most in-store mobile payment services demonstrate desirable usability, they raise many security issues [1]. Payment cards are often targets of fraud schemes, which victimize the issuing financial institution and individual cardholders [2]. Payment cards have evolved considerably over the decades. But a plethora of competing standards, and their patchy take-up around the globe, have left cards vulnerable to creative fraudsters [3]. Due to the growing volume of electronic payments, the monetary strain of credit-card fraud is turning into a substantial challenge for financial institutions and service providers, thus forcing them to continuously improve their fraud detection systems [4].

In real world we have two distinct types of payment systems

1. **Internet –Based payment system There are four models of Internet-Based payment system**
1. e-Cash
2. Credit Card
3. Debit Card
4. Smart Car

2. **Electronic Transaction-Based payment system**
1. Secure Electronic Transaction
2. Cyber Cash
3. Net Bill
4. First Virtual Holdings

Risks in Electronic Payment Systems

There are three major risks in the operation of the payment system

1. Fraud or mistake.
2. Privacy issues.
3. Credit Risk.

1. Fraud or Mistake

All electronic payment systems need some ability to keep automatic records. Once information has been captured electronically, it is easy and inexpensive to maintain. The need for record keeping for purpose of risk management like fraud or any sort of mistakes.

2. Privacy Issues

His electronic payment system must ensure and maintain privacy. The privacy of customers should be protected as much as possible. Privacy must be maintained against unauthorized access. For any type of transaction trusted third-parties will be needed for all tenacity and good faith.

3. Managing Credit Risk

Credit or systematic risk is a major concern in net settlement systems because a bank's failure to settle its net position could lead to a chain reaction of bank failures.

[1] Yu, Xingjie, Su Mon Kywe, and Yingjiu Li. "Chapter 6 - Security Issues of In-Store Mobile Payment." In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*, edited by David Lee Kuo Chuen and Robert Deng, 115–44. Academic Press, 2018.
[2] Rockwell, L.R. "Payment Cards." In *Encyclopedia of Forensic Sciences (Second Edition)*, edited by Jay A. Siegel, Pekka J. Saukko, and Max M. Houck, 432–38. Waltham: Academic Press, 2013.
[3] Gold, Steve. "The Evolution of Payment Card Fraud." *Computer Fraud & Security* 2014, no. 3 (March 1, 2014): 12–17.
[4] Jurgovsky, Johannes, Michael Granitzer, Konstantin Ziegler, Sylvie Calabretto, Pierre-Edouard Portier, Liyun He-Guelton, and Olivier Caelen. "Sequence Classification for Credit-Card Fraud Detection." *Expert Systems with Applications* 100 (June 15, 2018): 234–45.

Table 1

Computer virus	Computer program that causes serious damage to computer systems or files
Phishing	when the perpetrator set up deceitful websites that appears official and causing the victim to give out personal information to the criminals
Vishing	Personal details stolen via phone
Botnet	this occurs when a hacker transmits instructions to other computers for the purpose of controlling them
Spoofing its	its use of email to swindle an individual into providing personal information that is later used for unlawful purposes
E- theft	The perpetrator hacks into a financial institution e.g. a bank and diverts funds to accounts accessible to the criminal. To prevent e-theft, most major banks severely limit what clients can do online
Cyber terrorism	Cyber terrorism occurs when terrorists cause virtual destruction in online computer systems
Espionage	occurs when perpetrators hack into online systems or individual PCs to obtain confidential information for the purpose of selling it to other parties (criminals)
Malware	This is constituted by a category of viruses such as spyware, Trojan horse, worms with its original intent to break the host system
Spam	Refers to unsolicited email; spam is illegal if it violates the Can-Spam Act of 2003, such as by not giving recipients an optoutmethod. Source: (Andam, 2003;

***Source*:** (Andam, 2003; Carol Mendelsohn, 2015 May 13)

Review of Literature

Gómez *et al*. (2018) [5] Millions of euros are lost every year due to fraudulent card transactions. The design and implementation of efficient fraud detection methods is mandatory to minimize such losses. In this paper, we present a neural network based system for fraud detection in banking systems. We use a real world dataset, and describe an end-to-end solution from the practitioner's perspective, by focusing on the following crucial aspects: unbalancedness, data processing and cost metric evaluation. Our analysis shows that the proposed solution achieves comparable performance values with state-of-the-art proprietary and costly solutions.

Yang *et al*. (2015) [6]

The uncertainties of transaction handling and consumer perception toward risk have been identified as some of the major problems causing consumers' hesitance toward taking advantage of online payments. With the ever-growing implementation of trusting mechanisms for online payments, consumer confidence has greatly increased. The researchers explore the elements of perceived risk and trust – the two most vital factors influencing consumer behavior of online payment – in the relatively mature stage of China's online payment environment. It also analyzes and classifies perceived risks of different nature into two categories: systematic perceived risk and transactional perceived risk according to their different roles in affecting consumer trust. The results show that in the current stage of China's online payment, consumers have built up trust first as an antecedent of their perceived risks. Moreover, perceived total risk is negatively related to trust while perceived risks can be classified into two types: system dependent risk which is positively related to trust and transactional risk which is negatively related to trust.

Quah and Sriganesh (2008) [7]

Online banking and e-commerce have been experiencing rapid growth over the past few years and show tremendous promise of growth even in the future. This has made it easier for fraudsters to indulge in new and abstruse ways of committing credit card fraud over the Internet. This paper focuses on real-time fraud detection and presents a new and innovative approach in understanding spending patterns to decipher potential fraud cases. It makes use of self-organization map to decipher, filter and analyze customer behavior for detection of fraud.

Bogdan-Alexandru Urs (2015) [8]

Nowadays e-Payment systems have become increasingly popular due to the widespread use of the internet based shopping and banking. The number of private and corporate transactions that are done electronically is growing rapidly. Malicious applications targeting online banking transactions have also increased dramatically in past few years. Worms, Trojans, viruses, phishing, pharming, spoofing, man-in the middle, denial of service attack, transaction poisoning and spamming are the most common threats. All this malicious activity has lead to unauthorized access, theft and fraud. Information security is an essential requirement for any efficient and effective e-Payment system. In Romania, specific legislation has been created in order to protect the e-Payment system and fight cyber-crime.

Statement of the Problem

With the internet-based payment mechanisms becoming very popular with the people in buying and selling of goods and services. The security concerns have been the epicenter of the on-line transactions. The present study accounts for the various problems encountered in the e-payment modes in the businesses.

Objectives of the Study

1. To review the existing literature on the e-payment frauds;
2. To understand the various risks involved in the electronic payment systems; and
3. To find out the precautions to be taken in e-payment modes

Scope of the Study

[5] Gómez, Jon Ander, Juan Arévalo, Roberto Paredes, and Jordi Nin. "End-to-End Neural Network Architecture for Fraud Scoring in Card Payments." *Machine Learning and Applications in Artificial Intelligence* 105 (April 1, 2018): 175–81.

[6] Yang, Qing, Chuan Pang, Liu Liu, David C. Yen, and J. Michael Tarn. "Exploring Consumer Perceived Risk and Trust for Online Payments: An Empirical Study in China's Younger Generation." *Computers in Human Behavior* 50 (September 1, 2015): 9–24.

[7] Quah, Jon T.S., and M. Sriganesh. "Real-Time Credit Card Fraud Detection Using Computational Intelligence." *Expert Systems with Applications* 35, no. 4 (November 1, 2008): 1721–32.

[8] Bogdan-Alexandru Urs, 2015. "Security Issues and Solutions in E-Payment Systems," Fiat Iustitia, Faculty of Law,"Dimitrie Cantemir" Christian University Bucharest, vol. 9(1), pages 172-179, June.

The present study is restricted to the individual consumers drawn from various walks of life who are well conversant with the e-commerce and are active in on-line trading. The study involved the convenience sampling in drawing the samples in the city of Bengaluru.

Limitations of the Study

- The data provided by the respondents may not be fool-proof
- All the limitations of the tools used are applicable to this study
- There could be flaws in the samples chosen for the research

Methodology

Types of Research

The current research work adopted descriptive survey, analytical, cause and effect method of research.

Sampling –Universe

- All the individual consumers active in on-line trading in Bangalore.

Sample size

Research has taken up and surveyed 60 respondents in the city of Bangalore by using convenient sampling.

Primary data

The primary data for the purpose of the current research work have been collected with the help of well-structured schedules and personal interviewing.

Secondary data

For the purpose of the study, secondary data are gathered from books, articles, reports, magazines, journals, and newspapers on the topic and internet information.

Analysis and Interpretation of Data

Table 1: Classification Based On the Consumer Category

Social Groups	Responses (n=60)	
	Number	Percent (%)
Student	10	16.67
Working	24	40.00
Housewife	13	21.67
Self-Employed	13	21.67
Total	60	100.00

***Source*:** Primary Data

Analysis

The respondents from the student category account for 16.67% of the total composition. 40% of the respondents belong to the working class. Self-employed are 13 in the total.

Table 2: Age-Wise Distribution of Respondents

Age in Years	Responses (n=60)	
	Number	Percent (%)
Below 25 years	10	16.67
25-50 years	14	23.33
50-75 years	35	58.33
Above 75 years	01	1.67
Total	60	100

***Source*:** Primary Data

Analysis

58.33% of the respondents belong to the age-group of 25-50 years. Only 1.67% of the respondents are above the age of 75 years.

Table 3: Income-Wise Distribution of the Respondents

Monthly Income in Rupees	Responses (n=60)	
	Number	Percent (%)
Below 10,000	20	34.72
10,000-20,000	30	50
20,000-45,000	07	11.67
Above 45,000	03	4.87
Total	60	100

***Source*:** Primary Data

Analysis

50% of the respondents have an average monthly income in the range of Rs.10, 000-Rs.20, 000. Below Rs. 10, 000 is accounting for 34.72% of the total composition of respondents.

Table 4: Experience- Wise Distribution of Respondents

Experience in Years using E-Payment modes	Responses(n=60)	
	Number	Percent (%)
0-5	09	15.0
5-10	36	60.0
10 Years and Above	15	25.0
Total	60	100

***Source*:** Primary Data

Analysis

60% of the respondents have an experience of 5-10 years. 25% of the respondents have 10 years and above experience.

Table 5: Tenure of Usage of E-Payment Modes

Statement	Scale	Number	(%)
Tenure of usage of E-Payment modes	More than 10 years	06	10.00
	From last 10 years	17	28.33
	Last 5 years	19	31.67
	Last 2 years	18	30.00
Total		60	100

***Source*:** Primary Data

Analysis

10% of the respondents are benefited from E-Payment for more than 10 years. 15 % of the respondents are benefited from last 10 years. More than $3/10^{th}$ of the respondents are using the E-Payment modes from last 5 years.

Table 6: E-Payment in Increasing the Frauds

Statement	Scale	Number	(%)
E-Payment increases the Frauds in the Business transactions	Very True	30	50.0
	Mostly True	10	16.67
	True	5	8.33
	True to some extent	5	8.33
	Not At All	10	16.67
Total		60	100

***Source*:** Primary Data

Analysis

50% of the respondents strongly feel that the E-Payment increases the Frauds in the Business transactions. 16.67% of the respondents express the statement to be mostly true.

8.33% of the respondents express the statement to be true.

Hypothesis Testing

H_o: There is no relationship between E-Payment modes on one hand and the frauds on the other

H_a: There is a relationship between E-Payment modes on one hand and the frauds on the other

E-Payment Modes Increases the Frauds in the Business Transactions

Table 7: Computation of Hypothesis Testing

Elements	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
O	30	10	5	5	10	60
E	12	12	12	12	12	60
(O-E)	18	-2	-7	-7	-2	
$(O-E)^2$	324	4	49	49	4	
$(O-E)^2/E$	27	0.33	4.08	4.08	0.33	35.83

Alpha=0.05 Degree of freedom= 5-1=4 Chi square=35.83 Table value of F (0.05) at 95% level of significance = 9.94

Conclusion

Hypothesis is rejected but the alternate hypothesis is accepted.

Findings

- The respondents from the student category account for 16.67% of the total composition. 40% of the respondents belong to the working class. Self-employed are 13 in the total.
- 58.33% of the respondents belong to the age-group of 25-50 years. Only 1.67% of the respondents are above the age of 75 years.
- 50% of the respondents have an average monthly income in the range of Rs.10, 000-Rs.20, 000. Below Rs. 10, 000 is accounting for 34.72% of the total composition of respondents.
- 60% of the respondents have an experience of 5-10 years. 25% of the respondents have 10 years and above experience.
- 10% of the respondents are benefited from E-Payment for more than 10 years. 15 % of the respondents are benefited from last 10 years. More than $3/10^{th}$ of the respondents are using the E-Payment modes from last 5 years.
- 50% of the respondents strongly feel that the E-Payment increases the Frauds in the Business transactions. 16.67% of the respondents express the statement to be mostly true. 8.33% of the respondents express the statement to be true.

Checklist of E-Transactions

An ideal requirements wish-list for online payments in e-commerce might look something like the following:

1. **Confidentiality** – The payment scheme should offer optional levels of confidentiality – allowing details of the transaction to only be made known to those parties to whom the customer or merchant so wishes.
2. **Integrity** – The scheme should maintain the integrity of the transaction – making tampering or changes to the details of the transaction practically infeasible.
3. **Authentication** – The scheme should provide methods for the authentication of communicating parties and/or the authentication of messages that are relied upon for payment authorization – making fraudulent activity difficult.
4. **Non-Repudiation** – The scheme should provide non-repudiation services – protecting both the merchant and customer against false claims.
5. **Availability** – The scheme should be highly available – allowing customers and merchants to participate in payment transactions when required.
6. **Implementation** – The scheme should provide clear benefits to merchants and customers justifying any costs associated with the scheme's implementation. The implementation details should attempt to abstract complexity and provide interfaces with merchant systems that represent good practices in software development in general.
7. **Interoperability** – The scheme should be interoperable – providing the widest possible access to merchants and customers.
8. **Ease of Use** – The scheme should be easy to understand and use for the customer.
9. **Scheme Protection** – The scheme rules and policies should continue to provide consumer protection from unscrupulous or fraudulent merchants. The scheme rules, policies and regulations should also continue to protect the payer when a claim of fraudulent activity is made. The onus should be on the scheme owners to disprove the validity of the claim, and not rely solely on the mechanisms of the scheme to automatically dispute such claims.

Conclusion

There is a need for a transparent and effective consumer protection in respect of E-Commerce. The businesses, marketing, advertising, trading and commerce need to be in good faith when consumers go about the e-trading. The risks in the services and the transactions should be addressed and lead to e-loyalty. Fraud victims must be given an opportunity to be heard and addressed with due-diligence. The financial institutions and the service providers have to provide robust fraud detection systems.

References

1. Yu, Xingjie, Su Mon Kywe, and Yingjiu Li. "Chapter 6 - Security Issues of In-Store Mobile Payment." In Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2, edited by David Lee Kuo Chuen and Robert Deng, 115–44. Academic Press, 2018.
2. Rockwell LR. "Payment Cards." In Encyclopedia of Forensic Sciences (Second Edition), edited by Jay A. Siegel, Pekka J. Saukko, Max M Houck, 432–38. Waltham: Academic Press, 2013.
3. Gold, Steve. "The Evolution of Payment Card Fraud." Computer Fraud & Security. 2014; (3):12-17.
4. Jurgovsky, Johannes, Michael Granitzer, Konstantin Ziegler, Sylvie Calabretto, Pierre-Edouard Portier, Liyun He-Guelton, and Olivier Caelen. "Sequence Classification for Credit-Card Fraud Detection." Expert Systems with Applications, 2018; 100:234-45.
5. Gómez Jon Ander, Juan Arévalo, Roberto Paredes, Jordi Nin. "End-to-End Neural Network Architecture for Fraud Scoring in Card Payments." Machine Learning and Applications in Artificial Intelligence, 2018; 105:175-81.

6. Yang Qing, Chuan Pang, Liu Liu, David C Yen, J Michael Tarn. “Exploring Consumer Perceived Risk and Trust for Online Payments: An Empirical Study in China’s Younger Generation.” Computers in Human Behavior, 2015; 50:9-24.
7. Quah Jon TS, Sriganesh M. “Real-Time Credit Card Fraud Detection Using Computational Intelligence.” Expert Systems with Applications. 2008; 35(4):1721-32.
8. Bogdan-Alexandru Urs. "Security Issues and Solutions in E-Payment Systems," Fiat Iustitia, Faculty of Law,"Dimitrie Cantemir" Christian University Bucharest. 2015; 9(1):172-179.