



**An investigation of the causes and consequences  
of card-not-present fraud, its impact and  
solution.**

**Kingsley Chibuzor Aguoru**

**A thesis submitted in partial fulfilment of the requirements of the**

**University of East London for the degree of**

**Doctor of Information Security**

**September 2015**

---

## **Abstract**

The boom of electronic commerce technologies in recent years has drastically increased the demand for an effective electronic method to pay or be paid. The currently predominant method is online card payment, in which the cardholder is not present at the point of sale. However this method is accompanied by huge vulnerabilities and also serves as a low-risk avenue for fraudsters to steal card details with the intent to defraud online merchants. These merchants are those who mostly bear the overall risk and consequences because they cannot provide a document signed by the legitimate cardholder. Several attempts and proposals have been introduced to solve this problem. However, many have failed to be adopted, while those that have been adopted have not been able to adequately solve the problem. The card payment industry is fully aware of the problem and its consequences, but it has abdicated responsibility for fraud in this type of transaction, and declines to guarantee the “card-not-present” fraud solutions that have been proposed during the past ten years. Instead, the industry has chosen only to accept responsibility for fraud arising from the “card present” environment, which is of low risk because it uses chip-and-pin technology. As a result, many merchants have withdrawn from online business for fear of losses, while consumers are sometimes turning back to alternative payment and traditional “bricks-and-mortar”-style shopping, for fear of identity theft.

In light of these problems and challenges, this research adopted a practice approach to investigate the causes and consequences of card-not-present fraud, the associated infiltration techniques, and the impact on the development of e-commerce, in order to unveil and establish an understanding of the background and characteristics of card-not-present fraud, its causes, its penetration techniques and aftermath.

This research examined the result of the investigation, and proposes a feasible solution known as 3W-ADA Sentry System, built out of the framework of analytic geometry to counter threats of card-not-present fraud and related identity theft by introducing a non-electronic and low-cost dynamic tokenization process for card-not-present authentication. This proposal could eventually help to restore the security of online card payment authentication, restore the trust of participants, and improve the development of electronic commerce. However, due to limitations inherent in this research, it provides instead

recommendations concerning the additional work that would be required to turn the 3W-ADA Sentry into an Association or Scheme to promote its global adoption and its compatibility with the infrastructures and systems of relevant organisations.

## Declaration

I hereby certify that this thesis constitutes my own work, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the thesis describes original work that has not previously been presented for the award of any other degree of any institution.



Signed: \_\_\_\_\_

Kingsley Chibuzor Aguoru

## **Acknowledgement**

Firstly, I thank almighty GOD for his mercies, and wisdom, and for giving me the ability to embark upon, and successfully conclude, this project.

I would also like to express my deep appreciation to my supervisor - Prof. Hamid Jahankhani, Dr. Sin Wee Lee and Dr Al-Nemrat Ameer - for their firm support, enthusiasm and persistent supervision throughout the research period. Without their valuable expertise, tolerance and guidance, this thesis would not have been possible.

I also convey my gratitude to the Board and Management of Paymenex Limited and Paymenex Regional Administrators worldwide for their unflinching financial support for the overall cost of this research degree program, and for their feedback in evaluating the solution produced by this research.

My appreciation and love also extends to the entire Aguru family for their love, inspiration, care and positive encouragement throughout my research period.

Glory be to God Almighty, Amen!

## **Publications**

INVESTIGATION OF THE CAUSES AND CONSEQUENCES OF CARD-NOT-PRESENT FRAUD, ITS IMPACT AND SOLUTION

7th annual event of the Advances in Computing and Technology Conference (AC&T) 2012.

# Table of Contents

<b>ABSTRACT</b>	<b>II</b>
<b>DECLARATION</b>	<b>IV</b>
<b>ACKNOWLEDGEMENT</b>	<b>V</b>
<b>PUBLICATIONS</b>	<b>VI</b>
<b>TABLE OF CONTENTS</b>	<b>VII</b>
<b>LIST OF FIGURES</b>	<b>XVII</b>
<b>LIST OF TABLES</b>	<b>XX</b>
<b>GLOSSARY TABLE</b>	<b>XXII</b>
<b>1. PART 1 - INTRODUCTION</b>	<b>1</b>
<b>1.1 Introduction</b>	<b>1</b>
<b>1.2 Problem statement</b>	<b>2</b>
1.2.1 About the sponsor	2
1.2.2 Background to the problem	3
<b>1.3 Research question, purpose and scope</b>	<b>4</b>
1.3.1 Research question	5
1.3.2 The research purpose	5
1.3.3 The research scope	5
<b>1.4 The research motivation</b>	<b>6</b>

1.4.1	Primary motivations -----	6
1.4.2	Secondary motivation -----	8
<b>1.5</b>	<b>Related work and research -----</b>	<b>8</b>
1.5.1	Findings of related research -----	8
1.5.2	Solutions from related research -----	9
<b>1.6</b>	<b>Contribution to knowledge -----</b>	<b>11</b>
1.6.1	Presentation of a philosophy of identity theft and card-not-present fraud ----	11
1.6.2	Development of an academic framework for future research -----	11
1.6.3	Introduction of a non-electronic and low-cost CNP fraud solution -----	12
1.6.3.1	Variation between existing solutions and the proposed new solution ---	13
1.6.3.2	Static vs. dynamic authentication data -----	15
1.6.3.3	Security of card and personal information in a CNP environment -----	15
1.6.3.4	Benefits of replacing existing solutions with 3W-ADA Sentry -----	16
<b>1.7</b>	<b>The research approach and context -----</b>	<b>18</b>
1.7.1	Investigation -----	18
1.7.2	Evaluation -----	18
1.7.3	Solution -----	18
<b>1.8</b>	<b>Research Structure -----</b>	<b>21</b>
<b>2.</b>	<b>PART 2 – BACKGROUND AND LITERATURE REVIEW -----</b>	<b>23</b>
<b>2.1</b>	<b>Introduction -----</b>	<b>23</b>



<b>2.2 Information</b>	<b>25</b>
2.2.1 Value of information	25
2.2.2 Information Security and Assurance	26
2.2.3 Trust	28
2.2.4 Research insight of Information and Trust in electronic commerce	29
<b>2.3 Background to Electronic Commerce (E-Commerce)</b>	<b>30</b>
2.3.1 The trend of electronic commerce	30
2.3.2 Types of electronic commerce	31
2.3.3 Key essentials of electronic commerce	32
2.3.3.1 Business Model and Workflow Management System	33
2.3.3.2 Shopping Cart and Content Management System	33
<b>2.4 The B2C e-commerce transaction flowchart</b>	<b>34</b>
<b>2.5 Electronic commerce: pros and cons to businesses</b>	<b>38</b>
<b>2.6 The electronic commerce pros and cons to consumers</b>	<b>39</b>
<b>2.7 Electronic Commerce payment systems</b>	<b>39</b>
2.7.1 Electronic payment card system	41
2.7.1.1 Types of payment card	42
<b>2.8 Card-not-present fraud in e-commerce transaction</b>	<b>44</b>
2.8.1 Card-not-present fraud losses in Australia	46
2.8.2 Card-not-present Fraud losses in Canada	49
2.8.3 Card-not-present fraud losses in United States	50

<b>2.9 Card-not-present fraud losses in United Kingdom</b>	<b>50</b>
2.9.1 Card-not-present fraud level controversy	54
2.9.2 Undisclosed factors behind the drop in card-not-present fraud losses	55
2.9.2.1 Aggressive measures of handling card-not-present transactions	56
2.9.2.2 Introduction of Alternative Payments	56
<b>2.10 Causes of card-not-present fraud</b>	<b>59</b>
2.10.1 Identity Theft	60
2.10.1.1 Methods of identity theft and infiltration techniques	65
2.10.2 Growth of Internet Users	74
2.10.3 Exploitation of Trust among parties	75
2.10.4 Flaws in card-not-present systems and solutions	76
2.10.4.1 The CVV and the AVS	76
2.10.4.2 Secure Electronic Transactions (SET)	78
2.10.4.3 Secure Socket Layer (SSL)	81
2.10.4.4 3D Secure	81
2.10.4.5 Telephone Fraud Screening	83
2.10.4.6 Neural Network Credit card fraud detection	84
<b>2.11 Impact of card-not-present fraud on e-commerce development</b>	<b>85</b>
<b>3. PART 3 – 3W-ADA SENTRY SYSTEM</b>	<b>89</b>
<b>3.1 Introduction to dynamic authentication</b>	<b>89</b>

3.1.1	Random number generator (RNG)-----	90
3.1.2	Hardware dynamic authentication method (True Number Generator)-----	90
3.1.3	Software dynamic authentication method (Pseudo Random Number Generator)	91
<b>3.2</b>	<b>An Overview of the 3W-ADA Sentry System -----</b>	<b>94</b>
3.2.1	An overview of coordinate or analytic geometry -----	95
3.2.2	Concept of Coordinate geometry plane in 3W ADA Sentry -----	96
3.2.3	Random Number generator for the 3W-ADA Sentry PAC-----	96
3.2.4	How the 3W-ADA Sentry System Works-----	97
3.2.5	The 3W-ADA Sentry system Models-----	101
3.2.6	SWOT Analysis of the 3W-ADA Sentry system-----	106
3.2.6.1	Strengths - 3W-ADA Sentry system -----	106
3.2.6.2	Weaknesses - the 3W-ADA Sentry system -----	106
3.2.6.3	Opportunities - the 3W-ADA Sentry system -----	107
3.2.6.4	Threats - The 3W-ADA Sentry system-----	107
3.2.7	Justification of 3W-ADA Sentry -----	108
3.2.7.1	Research Findings -----	108
<b>3.3</b>	<b>3W-ADA Sentry Software Requirements Specification (SRS) -----</b>	<b>110</b>
3.3.1	Introduction-----	110
3.3.1.1	Purpose-----	110
3.3.1.2	Project Scope-----	110

3.3.1.3	Definitions, Acronyms and Abbreviations-----	112
3.3.1.4	References -----	112
3.3.2	Overview-----	112
3.3.3	Overall Description-----	113
3.3.3.1	Product Perspective-----	113
3.3.3.2	Product Functions-----	114
3.3.3.3	User Characteristics -----	116
3.3.3.4	General Constraints-----	117
3.3.3.5	User Documentations -----	117
3.3.3.6	Assumptions and Dependencies -----	117
3.3.3.7	Deliverables -----	118
3.3.4	Functional Requirements -----	118
3.3.4.1	3W-ADA Sentry System functional requirements-----	118
	Setup Payment Network and Setting-----	123
	Setup SMS Gateway-----	123
	Setup Email Gateway -----	123
	Authentication Settings and Configurations -----	123
	User Profile Management -----	123
	Card Enrollment-----	123
	Enrolled Card Directory -----	123
	Authentication History-----	123

Merchant application programming interface -----	123
Payment Network application programming interface -----	123
3.3.4.2 Use Cases -----	124
3.3.4.3 Non-Functional Requirements -----	125
3.3.4.4 Interface Requirements -----	128
<b>3.4 3W-ADA Sentry System Design -----</b>	<b>130</b>
3.4.1 Introduction -----	130
3.4.1.1 Purpose and Scope -----	130
3.4.1.2 Audience -----	130
3.4.1.3 Project design executive summary -----	130
3.4.1.4 3W-ADA Sentry system design overview -----	131
3.4.1.5 3W-ADA Sentry System design constraints -----	132
3.4.1.6 Point of Contact -----	132
3.4.1.7 Project References -----	133
3.4.1.8 Project Document Overview -----	133
3.4.2 3W-ADA Sentry system architecture and design -----	133
3.4.2.1 Design of 3W-ADA Sentry system on Paymenex TransNET -----	136
3.4.3 3W-ADA Sentry System database design -----	137
3.4.3.1 Database dictionary -----	139
3.4.4 Detailed Software design -----	139
3.4.4.1 3W-ADA Sentry Paymenex module software design -----	139

3.4.4.2	3W-ADA Sentry merchant module software design -----	142
3.4.4.3	Merchant authentication parameter -----	142
3.4.4.4	Requesting transaction session ID-----	143
3.4.4.5	Parameter string-----	144
3.4.4.6	Response from Paymenex TransNET-----	145
3.4.4.7	Database design -----	148
<b>3.5</b>	<b>3W-ADA Sentry User Acceptance Test (UAT) -----</b>	<b>149</b>
3.5.1	Introduction-----	149
3.5.2	Purpose -----	149
3.5.3	Role and Responsibilities-----	149
3.5.4	Testers and Participants-----	150
3.5.5	Testing Schedules-----	152
3.5.6	Test Requirements -----	153
3.5.6.1	Types of Testing -----	153
3.5.7	Test Environments-----	154
3.5.8	Test Perspectives-----	154
3.5.9	3W-ADA Sentry Test Cases -----	154
3.5.9.1	3W-ADA Sentry Paymenex TransNET Module Test Cases -----	154
3.5.9.2	3W ADA Sentry Merchant interface Test Case -----	157
3.5.10	Test Assumptions -----	159
3.5.11	Test Risks -----	159

3.5.12	Acceptance and Acknowledgments	159
<b>4.</b>	<b>PART 4 – 3W-ADA VERIFICATION AND VALIDATION</b>	<b>161</b>
<b>4.1</b>	<b>Introduction</b>	<b>161</b>
4.1.1	Purpose	161
<b>4.2</b>	<b>3W-ADA Sentry System Verification</b>	<b>161</b>
4.2.1	System Feasibility	161
4.2.2	System development cycle	162
4.2.3	System Development Checklist	163
4.2.4	System Acceptance Criteria	164
<b>4.3</b>	<b>3W-ADA Sentry System Validation</b>	<b>166</b>
4.3.1	Acceptance Validation	166
4.3.2	Operational Validation	167
4.3.3	Performance Validation	167
<b>5.</b>	<b>PART 5 – CONCLUSION</b>	<b>168</b>
<b>5.1</b>	<b>Thesis Summary</b>	<b>168</b>
<b>5.2</b>	<b>Limitations</b>	<b>169</b>
<b>5.3</b>	<b>Contribution summary of this thesis</b>	<b>169</b>
5.3.1	Philosophy of identity theft and card-not-present fraud	170
5.3.2	A framework work for academic scrutiny and future research	170
5.3.3	Introduction of a non-electronic and low-cost CNP Fraud solution	171

<b>5.4 Conclusion</b>	<b>171</b>
<b>5.5 Future research direction</b>	<b>172</b>
5.5.1 Trend and causes of card-not-present fraud	173
5.5.2 Concealing Sensitive information	173
5.5.3 More research on dynamic authentication method	173
5.5.4 Additional Research Recommendation	173
<b>6. BIBLIOGRAPHY</b>	<b>175</b>
<b>7. APPENDICES</b>	<b>188</b>
<b>7.1 Appendix A: TransNET module PseudoCode and Database</b>	<b>188</b>
7.1.1 PAC Card Production Pseudocode	188
7.1.2 Link PAC Card to Account Pseudocode	188
7.1.3 Database Dictionary	189
<b>7.2 Appendix B: AES Encryption/Decryption in PHP Language</b>	<b>191</b>
<b>7.3 Appendix C: Log of System UAT Recommended Changes</b>	<b>197</b>
<b>7.4 Appendix D: 3W-ADA Sentry Acceptance Matrix</b>	<b>198</b>
<b>7.5 Appendix E: Case Study of Vodafone Ghana</b>	<b>199</b>



## List of Figures

Figure 1: Relationship and strength of authentication factors .....	13
Figure 2: Identity theft technique .....	17
Figure 3: The research plan flowchart .....	19
Figure 4: McCumber Information Assurance Model (Maconachy, et al., 2001).....	27
Figure 5: Modified McCumber Information Assurance Model (Maconachy, et al., 2001) .....	27
Figure 6: The Ecommerce transaction flowchart (Aguoru, 2007) .....	36
Figure 7: Format of a Credit or Debit Card (APACS, 2005) .....	43
Figure 8: Format of a Diners Club and American Express Card (APACS, 2005).....	44
Figure 9: Australia Plastic Card Fraud by Type 2009 (Smith, n.d.) .....	47
Figure 10: Australian Scheme Credit, Debit and Charge Card Fraud 2012 (Australian Payments Clearing Association, 2013) .....	48
Figure 11: Fraud per every \$1,000 transacted on Australian payment card (Australian Payments Clearing Association, 2013) .....	49
Figure 12: Credit Card Fraud losses in Canada 2011-12 (Canadian Anti-Fraud Centre, 2013) .....	50
Figure 13: Percentage of Card fraud losses split by types (APACS, 2010).....	51
Figure 14: Percentage of Card fraud losses split by types (APACS, 2012).....	51
Figure 15: Card-not-present fraud losses on UK-issued cards 2002-2012 .....	53
Figure 16: Card-not-present fraud losses on UK –issued cards 2004 - 2014.....	53
Figure 18: Flaws in remote Identification with static numbers .....	64

Figure 19: Email or web-link Phishing flowchart.....	67
Figure 20: Email screenshot Received in 2008 by Kingsley Aguru .....	68
Figure 21: Web-Link Redirection Page .....	68
Figure 22: A flowchart of a Trojan attack by Email .....	70
Figure 23: UK Household internet access 2006 to 2010 (Ofcom, 2011).....	75
Figure 24: CVV and AVS Validation Flowchart (Aguoru, 2007).....	77
Figure 25: SET Ordering and processing flowchart .....	80
Figure 26: Example 1 of 3D Secure enrolment.....	82
Figure 27: Example of 3D Secure enrolment.....	82
Figure 28: Coordinate geometry on a plane .....	95
Figure 29: PAC Request and Response Architecture .....	97
Figure 30: 3W-ADA Sentry dynamic authentication.....	99
Figure 31: 3W-ADA Sentry coordinate plane .....	100
Figure 32: 3W-ADA Sentry integrated Model.....	101
Figure 33: 3W-ADA standalone Model.....	102
Figure 34: 3W-ADA Card-not-present Transaction flowchart.....	103
Figure 35: Sample PAC card (Plane).....	106
Figure 36: 3W ADA Sentry system Use Case .....	124
Figure 37: Merchant interface Use Case.....	125
Figure 38: Integrated 3W-ADA Sentry environment in Paymenex TransNET.....	132
Figure 39: Paymenex TransNET 3W ADA Sentry System Architecture .....	134

Figure 40: TransNET and Merchant’s Systems communication flowchart..... 135

Figure 41: 3W ADA Sentry dataflow ..... 135

Figure 42: 3W-ADA Sentry Sequence diagram..... 136

Figure 43: 3W-ADA Sentry Statechart diagram ..... 137

Figure 44: 3W-ADA Paymenex TransNET Entity Relationship Diagram ..... 138

Figure 45: PAC Card Production and Management Wireframe design..... 140

Figure 46: PAC Card Link wireframe design ..... 141

Figure 47: Merchant interface – step one wireframe ..... 144

Figure 48: Merchant interface – step two wireframe ..... 147

Figure 49: Waterfall Development process with iteration (Aguoru, 2007) ..... 162

## List of Tables

Table 1: Authentication factors assessment chart .....	14
Table 2: The research approach framework.....	20
Table 3: The research method logic .....	21
Table 4: Subset of Information Assurance Model .....	28
Table 5: Legend of e-commerce transaction flowchart.....	38
Table 6: Characteristics of electronic payment systems .....	41
Table 7: Australia Card-not-present fraud 2006 – 2009 (Smith, n.d.).....	47
Table 8: Card-not-present fraud losses on UK-issued cards – 1995 - 2014 (APACS, 2005); (Financial Fraud Action UK, 2014). .....	52
Table 9: Alternative Payment Providers .....	59
Table 10: Bases classification of identity theft methods.....	66
Table 11: UK household internet access 2006 to 2010 (Office for National Statistics, 2010) .....	74
Table 12: Characteristics comparison table of dynamic schemes.....	92
Table 13: Security and functionality comparison table of dynamic schemes.....	93
Table 14: 3W Sentry transaction flowchart .....	105
Table 15: 3W-ADA Sentry system data requirement relationship .....	115
Table 16: 3W ADA Sentry System Model Components .....	123
Table 17: Project design document overview .....	133
Table 18: Merchant 3W Sentry authentication parameter and description.....	143

Table 19: Merchant Interface step one parameter and description .....	144
Table 20: Merchant interface step one response XML .....	146
Table 21: UAT role and responsibilities .....	150
Table 22: Testers and Participants .....	152
Table 23: Testing Schedule.....	153
Table 24: Test Case - Paymenex card enrolment.....	155
Table 25: Test Case – Disable PAC feature on a card .....	156
Table 26: Test Case – Re-enable PAC feature on a card .....	157
Table 27: Test Case – 3W Sentry Merchant interface .....	158
Table 28: 3W-ADA Sentry System checklist roles .....	164
Table 29: 3W-ADA Sentry User Acceptance Criteria.....	166

## Glossary Table

<b>Acronyms</b>	<b>Description</b>
2FA	Two-Factor Authentication
<b>3W ADA Sentry</b>	Who-Where-When Account Dynamic Authentication Sentry.
<b>AES</b>	Advance Encryption Standard (AES)
<b>AI</b>	Information Assurance
<b>APACS</b>	Association for Payment Clearing Services
<b>API</b>	Application Programming Interface
<b>ATM</b>	Automated Teller Machine
<b>AVS</b>	Address Verification Services
<b>CBC</b>	Cipher Block Chaining
<b>CNP</b>	Card-not-present
<b>CNP</b>	Card-not-present
<b>CSS</b>	Cascading Style Sheet
<b>CVV</b>	Card Verification Value
<b>CVV</b>	Card Verification Values
<b>DBMS</b>	Database Management System
<b>EDI</b>	Electronic Data Interchange
<b>ERD</b>	Entity Relationship Diagram
<b>GPS</b>	Global Positioning System

<b>GPS</b>	Global Positioning System
<b>HTML</b>	Hypertext Markup Language
<b>ICT</b>	Information Communication Technology
<b>IP</b>	Internet Protocol
<b>LAMP</b>	Linux, Apache, MySQL, PHP
<b>NVP</b>	Name Value Pair
<b>PCI</b>	Payment Card Industry
<b>PAC</b>	Personal Authentication Code
<b>PIN</b>	Personal Identification Number
<b>PKI</b>	Public Key Infrastructure
<b>POS</b>	Point Of Sale
<b>PRNG</b>	Pseudo Random Number Generator
<b>RNG</b>	Random Number Generator
<b>SAAS</b>	Software As A Service
<b>SET</b>	Secure Electronic Transaction
<b>SMS</b>	Short Message Service
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SRS</b>	Software Requirements Specification
<b>SSL</b>	Secure Socket Layer
<b>SQL</b>	Structured Query Language
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol

<b>TRNG</b>	True Random Number Generator
<b>UI</b>	User Interface
<b>UML</b>	Unified Modeling Language
<b>XML</b>	Extensible Markup Language



## Concept of Information Security

### **“LET LIKES BE SECURED BY LIKES”**

#### Concept Definition

Information Security simply entails using “*Confidential Data and Strategy*” to secure  
“*Confidential Data and Strategy*”

Aguoru K. C. (2006)

Intentionally left blank

# 1. PART 1 - INTRODUCTION

## 1.1 Introduction

Worldwide interest in electronic commerce has dramatically increased in recent years.

The reasons for this includes:

- The rapid growth of the internet and electronic commerce technologies.
- The benefits of buying from a universal marketplace.
- The need for effective methods for making real-time electronic payments online.
- The benefits of saving online merchants the cost of making expensive investments in ‘bricks and mortar’ businesses.

However, this interesting phenomenon is accompanied by a significant number of unresolved impediments, vulnerabilities and threats. These collectively establish a low-risk and anonymous route by which to carry out online card payment fraud. This has motivated criminals to deploy a range of methods to steal sensitive card information with the intent to commit card-not-present fraud at the expense of the merchant and cardholder.

In its broadest sense, every e-commerce technology can be thought of as a double-edged sword, with the possibility to both solve a problem and create a problem. The internet, as a key component in electronic commerce, is fundamentally an insecure technology. This fact has triggered a *technology-war*: and a rivalry between *problem-solving* and *problem-creating* internet technologies. Card payment is the predominant method of payment on the internet. However, it is impossible to transfer the chip-and-pin card payment authentication technology used in the ‘card-present’ environment to the card-not-present environment, which still relies on remote authentication with vulnerable and static card details.

As a result, in most reported card-not-present fraud, cardholders and their issuers are always protected, but the online merchant suffers the loss. This is because the merchant cannot provide a signed contract of authorisation by the cardholder, due to the fact that the card is not present at the point of sale (because the payment is completed electronically and remotely). In spite of that, none of the existing card-not-present solutions is

adequately solving the problem. Many merchants disappeared from e-commerce after a short period, when they could no longer tolerate the losses.

Many consumers do not want to use their card online because it is widely believed that card details are stolen by online criminals. This has had an adverse effect on the development of e-commerce.

For electronic commerce to develop without difficulties, online merchants need to be reassured that those making payment over the internet are really who they claimed to be. Card holders need a guarantee that their card details will not be stolen by online criminals in order to commit identity theft, and card issuers need assurance that they are not vulnerable in electronic commerce activities. In all of these considerations, concerns have been raised about the levels of trust that exist in electronic commerce and card-not-present transactions.

This research will unveil the major causes of card-not-present fraud, and will also try to solve the problem by introducing a low-cost and non-electronic method of dynamic authentication using the theory of analytic geometry. This is a feasible solution to card-not-present fraud, and aims to improve the security and trust of online card payments and strengthen the development of electronic commerce.

## **1.2 Problem statement**

This research is sponsored by Paymenex Limited, a British corporation which has its head office in London and regional offices worldwide.

### **1.2.1 About the sponsor**

According to Paymenex Limited (2012) “Paymenex is a universal electronic payments technology company that facilitates real time electronic payment between consumers and businesses and provides a global switching of electronic money transactions, payment processing, and real time gross settlement (RTGS) for financial institutions worldwide through its advanced network Paymenex TransNET.

Paymenex TransNET is an open membership and low-cost multichannel interchange network operated by the consortium of Paymenex Regional Administrators (PRA) worldwide and used by its members to deliver a range of bespoke electronic money account and payment systems to their customers such as: merchant acquiring, payment processing, electronic bill presentment and payment, gift and loyalty card management, RTGS, switching, and a versatile mobile technology with quadruple augmentation of mobile banking, mobile wallet, mobile payment and mobile loyalty capabilities called “xWallet Mobile”.

Paymenex contracts or partners with local technology companies in several countries to serve as the Paymenex Regional Administrator, overseeing the activities and administration of Paymenex members and agents. They frequently deliver statistical reports and analysis to Paymenex Limited to support strategic planning and business development (Paymenex Limited, 2012).

The mission of Paymenex is to become a leading provider of a sustainable and low-cost global interchange network, connecting financial institutions and licensed organisations on a secure transaction platform. However, the achievability and sustainability of this mission faces threats, including system and process vulnerabilities, exploitation, and illegitimate manipulations of system features (Paymenex Limited, 2012).

### **1.2.2 Background to the problem**

The most common solution offered by Paymenex TransNET enables merchants enrolled by Paymenex members, to accept payments made with a Paymenex card online. The cardholder is not present at the point of sale. This is known as a card-not-present transaction.

The anonymity of this environment has been exploited by cyber-criminals who steal card information with the intention to use it to make fraudulent online payments.

Making payment with a Paymenex card requires the cardholder to enter his card and billing address details in an online form. This method of payment has long been the traditional method of online card payment, and is also used by Paymenex competitors,

including Visa and MasterCard. However, with technology advancement, criminals have deployed a range of technologies to exploit this process. This poses a threat and has created a huge problem for merchants using the online payment services offered by Paymenex, Visa, MasterCard and other companies offering similar solutions.

The business model of Paymenex is designed to give buyers and sellers peace of mind in online transactions. It does this by eliminating the process and rule of charge-back in completed transactions by accepting the consequences, and absorbing the risk and losses. Being currently so exposed to system and process vulnerabilities, exploitation, and illegitimate manipulations of system features. Paymenex wishes to implement a solution that will prevent fraudulent transactions from taking place on its network.

To enable it to meet its mission and objectives, Paymenex seeks:

- Background research into the processes involved in online card payments to establish the causes of fraudulent transactions arising in this environment; how and why they are possible on the Paymenex network.
- A feasible solution that will thwart the threats posed by this fraudulent activity.

### **1.3 Research question, purpose and scope**

The card payment industry classifies card payment methods as either card present or card-not-present. The only difference between these classifications is the presence of the physical card: in card present the cardholder physically gives the card to the merchant to process a payment, while in card-not-present the cardholder only provides the card details to the merchant.

Card-not-present (CNP) transactions include all remote card payment methods where the card is not physically present at the point of sale (POS), including card payment made on the internet, by telephone, by fax, by email and all other methods of transmitting the card details to the point of sale or shop for the purpose of payment. However, this research is specifically limited to the investigation of the causes and consequences of fraud arising from card payment made on the internet and its impact on e-commerce development, as set out in the following research question, investigative purpose and scope.

### **1.3.1 Research question**

- What are the causes and consequences of online card-not-present fraud and what is the impact on the development of e-commerce?

### **1.3.2 The research purpose**

The purpose of these research was to:

- Investigate the processes involved in online card-not-present transactions and their related fraudulent infiltration techniques.
- Investigate the magnitude of impact that such fraudulent activity has upon e-commerce development.
- Find and develop a solution to combat the online card-not-present fraudulent infiltration techniques, thereby minimize the causes and consequences.

### **1.3.3 The research scope**

The research was carried out with the following scope and sequential order:

- a) An investigation into the e-commerce systems, process and life cycle of an online card-not-present transaction to understand the causes and consequences of the associated fraud.
- b) Critical analysis of the significance posed by the associated fraud to identify the impacts it imposes on the development of e-commerce.
- c) Evaluation of the strengths and weaknesses of the existing online card-not-present fraud solutions and justification of the need for an improved and effective solution compatible with the current methods of card-not-present fraud infiltration techniques.
- d) Development and evaluation of a solution proposed to combat the causes of card-not-present fraud.

## **1.4 The research motivation**

My research into card-not-present fraud is based on three primary motivations and one secondary motivation. These are detailed below.

### **1.4.1 Primary motivations**

#### ***Reviewing and updating existing research***

Previous research has been carried out (Aguoru, 2007) which has identified card-not-present fraud as a major problem that requires immediate attention. Though the research produced a solution called SMSV, the solution did not meet the sponsor's requirements and acceptability criteria because the computer timestamp method used in generating the random code suffers from insufficient entropy, which threatened the security of the code. Also the random code communication depended solely on an SMS message, meaning that, if a mobile network signal was not available or reachable at any point in time, the solution was not be accessible. Hence, further research is required to meet the sponsor's requirements and acceptability criteria, which includes security and availability.

#### ***Victimized merchant***

My first online business as a young entrepreneur started in 2002 in the city of London. During this period, online payment was new and the most widely used online payment methods were card payment, PayPal, and e-gold. Because PayPal is not globally available and many businesses in developing countries cannot obtain a merchant account to enable them to accept Visa and MasterCard payments because of bad credit or inaccessibility, I decided to take advantage of this problem to stand as a middleman between these businesses and their payment methods.

It was a business-to-business type of e-commerce model: the concept was to provide a third-party card-not-present payment processing system for businesses who could not obtain a merchant account from their bank, and could not access PayPal or alternative payment methods. I stood as the primary merchant account holder. Businesses who subscribed to my service were the secondary- or sub-merchants, because they depended on my merchant account to process payments online. In turn, I was dependent upon and



liable to, my bank in offering payment services to users. So the services my business provided were similar to the electronic money and payment services of PayPal.

Within one year of successful operation, this business model was exploited by online criminals who frequently used stolen card details to send money between themselves or make payment for goods and services that did not exist.

The darkest side of the business started when an illegitimate hosting company from outside the United Kingdom started making high volume transactions and sales. I was excited, as I thought business was booming - but in fact it was sinking.

On settlement day, I transferred the cleared balance to the fraudster's designated bank account outside the United Kingdom. However, before the second month's settlement, I started receiving endless chargeback letters from my bank, asking me to provide a signed agreement from the cardholder, and obviously I could not provide this because the transaction was completed remotely and entirely online.

Due to the volume and value of the transactions, my merchant account was terminated without notice, and the bank account was debited by over £14,760. This fund included my business fund and the funds of other legitimate sub-merchants who ended their business with me when they could no longer process payment on my system.

I lost my personal funds, I was dragged into further debt trying to pay back all other legitimate sub-merchants, and my bank could not help me.

I was highly dissatisfied with Visa, MasterCard, and my bank, and this formed the beginning of my thinking about card-not-present fraud and how it works.

### ***Insufficient academic research***

The most commonly known research degree is the Doctor of Philosophy, or PhD, which entails undertaking research for its own sake. The professional doctorate degree consists of practitioner research at doctoral level that enables the opportunity for researchers to combine academic, taught components with specific professional practical applications that are directly or indirectly relevant to their professional interests (Drake & Heath, 2011).

Research into card-not-present fraud is seen as a business activity for people involved in the process of accepting card payment online - for instance, the merchants, card issuers, acquirers and cardholders. Therefore this research sets out to bridge the gap between the academic and business worlds, and provide a mixed-methods approach to investigation into card-not-present fraud. It benefits from academic, taught components, and from professional business practices, in reaching its findings, and it is hoped that the project will encourage further academic research in this field.

### ***Academic Requirement***

This research is an academic prerequisite required by the board of examiners of the University of East London as a partial fulfilment of the requirements of the University of East London for the degree of Professional Doctorate in Information Security.

#### **1.4.2 Secondary motivation**

##### ***Curiosity, excitement and commitment***

The secondary motivation is my interest and excitement in building a problem-solving system in information technology, as well as my curiosity to find out how such a systemic problem could exist for so long without an effective solution. I combine this interest with my commitment and responsibility to solve the problem of my sponsor.

### **1.5 Related work and research**

This section provides a summary of research that has already been carried out in the field of card-not-present fraud, along with its limitations, and omissions, and compares it with the research carried out in this project. This review and comparison identifies and groups the related works in two categories: findings and solutions.

#### **1.5.1 Findings of related research**

There are several research publications that deal with the issue of card fraud, the security of e-commerce technology, and its security solutions. It is generally established that card-

not-present fraud, in the early years of electronic commerce, was minimal. But with the development of internet technologies and increased level of buying and selling online, card-not-present fraud has completely overtaken other types of card fraud, with a share of more than 54% of the total card fraud in the United Kingdom and in most leading economies. This is despite the different solutions that are being regularly introduced by many organisations (Semmens, 2002; APACS, 2012).

According to Bryan-Low (2011) and Masters & Boxell (2011), 2% of the British economy is being drained by internet crime and the consequences are largely borne by businesses. There has been a call for urgent action from government, private and public sectors to “*stem the rising of fraud*”. Governments have focused on law enforcement agencies to combat crime rather than trying to find a more effective and secure way to carry out payment operations online.

In discussing the trend of identity theft, Hoffman & McGinley (2010) said that financial gain has always been the most common motivation in such crime. Its history can be traced back to the biblical story of the twin brothers, named Jacob and Esau, the sons of Isaac and Rebecca. The news that Jacob was to inherit Isaac’s wealth motivated Rebecca to take advantage of Isaac’s bad eyesight and present Esau to Isaac in Jacob’s place, in order to mislead Isaac into promising his wealth to Esau. In contrast with the past, the development of the internet has allowed identity theft to extend its capabilities electronically.

### **1.5.2 Solutions from related research**

Recent studies, Crossley J. (2009) and Murdoch & Anderson (2010) examined 3D Secure, popularly known as “Verified by Visa” and “MasterCard secure code”, which was introduced by the card scheme more than a decade ago as a card-not-present fraud solution. This has remained the foremost solution promoted by the card association.

The studies found that 3D Secure technology has its own vulnerabilities, and that its lack of usability accounts for 30% of sale losses as a result of customer’s inability to successfully complete an order in which it is used. The static nature of the password used during a 3D Secure authentication and the redirection to third-party websites poses a

threat to card-not-present transactions, because the static information is vulnerable to theft. In addition many customers suspect a spoofing attack when 3D secure redirects them to another site.

According to a fraud review, (Card Technology Today, 2002) the use of the verification code - usually found on the signature strip on the back of a payment card, and also known as the card verification value (CVV) - and the billing address verification service (AVS) to authenticate cardholders during online payment has been in use for a while. However, this process is just as vulnerable as other static information used in online payments.

Other solutions that have failed, or are vulnerable, include the Secure Electronic Transaction (SET). This is not satisfactory because of the computational cost, message overhead and additional requirement of public key infrastructure (PKI). Solutions that rely upon data mining or behavioural analysis fail because the characteristics of online buyers and sellers change over time.

The research carried out by Aguru (Aguru, 2007) produced a solution by adding a one-time code authentication step in the card-not-present transaction process. However, this method suffers from insufficient entropy in the generation of the code, which posed a security threat. In addition, since the solution depended on a mobile network to communicate the one-time code, the solution could only be implemented whenever a mobile network was present.

Other research has focused on card-not-present fraud in the context of other online fraud, its impact and range of solutions, their vulnerabilities and why they failed. However, card-not-present fraud continues to be seen as a huge problem among the participants, and none of the related work has identified a satisfactorily solution to the problem, card-not-present fraud still requires more attention and a feasible solution. Further research towards this end is required.

As the internet and electronic commerce technologies grow, criminals introduce new technologies to exploit them. New research is therefore continually required to update existing research with current information. This research project therefore carefully

summarises newly discovered causes and consequences of card-not-present fraud, and presents a solution to address these.

## **1.6 Contribution to knowledge**

In researching and developing a solution to the sponsor's problem in the following ways, this project represents a significant contribution to knowledge in this field.

### **1.6.1 Presentation of a philosophy of identity theft and card-not-present fraud**

The project analyses and reports on the background, evolution and current trend of identity theft. It describes its advancement from "high-risk" physical theft and non-electronic impersonation to current "low-risk" electronic impersonation enabled by modern technology.

Today's criminals engage in a high level of psychologically manipulative activity to steal sensitive information electronically, with the intention to commit online card fraud for financial gain without exposing themselves to physical risk.

As the development of information and communication technologies continues, the social engineering technologies used to support this crime similarly transform into sophisticated and flexible tools. Most social engineering tools are developed to solve a problem, but fraudsters exploit these technologies to carry out criminal act.

### **1.6.2 Development of an academic framework for future research**

Electronic commerce technologies rely on software. The quality assurance of a software project requires a continuous process of monitoring, maintenance and validation throughout its life cycle. As information communication technologies become ever more complex, and sophisticated, the task of fully understanding them also grows. This task requires continuous research, validation and evaluation, to expand upon previous knowledge, and to replace legacy systems with ones that are fit for purpose.

Little academic research has explored card-not-present fraud in e-commerce payment systems, and there has been no conclusive investigation from an academic perspective of causes, consequences and solutions in this area. Rather, according to Murdoch & Anderson (2010), certain heavily promoted card-not-present solutions escaped academic scrutiny and evaluation because of their practical, rather than theoretical, nature.

This research fills the gap between theory and practice, by bringing together current business and academic perspectives on electronic commerce and card-not-present fraud. It identifies predominant and relevant social engineering technologies in use today, and the consequences they have on the development of electronic commerce. The proposed framework aim to serve as a blueprint for future academic research in this field.

### **1.6.3 Introduction of a non-electronic and low-cost CNP fraud solution**

Having established a current philosophy and framework of card-not-present fraud, its infiltration processes, its impact and consequences, this research goes on to propose a feasible solution designed in line with the current trend of card-not-present fraud.

The 3W-ADA Sentry system is a low-cost dynamic authentication system designed to solve the problem of card-not-present fraud by leveraging the Cartesian two-dimensional coordinate system.

The Cartesian two-dimensional coordinate system identifies a unique point in a plane, relative to a pair of numerical coordinates known as the origin. Such a unique point serves as an authentication token for a card-not-present transaction.

The token generated by the calculation of the intersection of the  $X$ ,  $Y$  axis is also used to protect an account holder's privacy online. Asking for the account holder's name and billing address by "Verified by Visa" and "MasterCard SecureCode" during online authentication exposes the account holder to the threat of identity theft. The 3W-ADA Sentry system avoids this vulnerability by uniquely identifying and authenticating the account holder in card-not-present transaction without revealing the account holder's personal information. A detailed specification and design documentation for this solution is provided in the relevant sections of this research.

### 1.6.3.1 Variation between existing solutions and the proposed new solution

The main problem of the card-not-present transaction is achieving an authentication solution that is not vulnerable to theft. This research compares the different characteristics of existing solutions and the new solution.

Cheswick, et al (2003) describes authentication, from the perspective of network security, with up to three main factors, as follows:

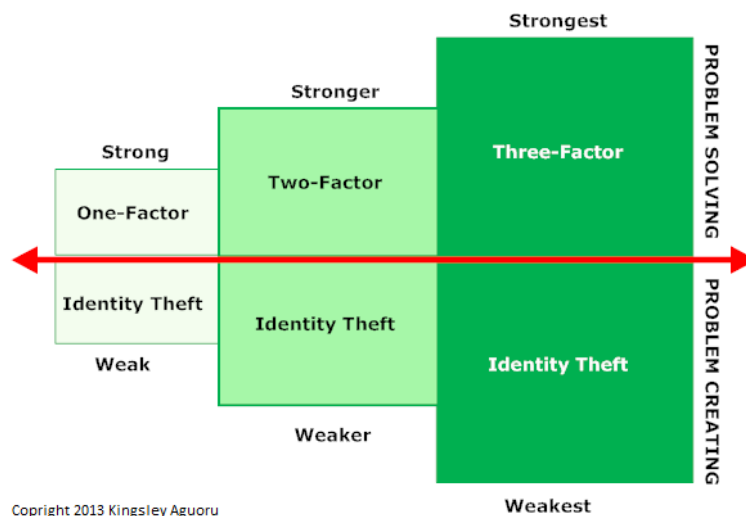


Figure 1: Relationship and strength of authentication factors

#### ***One-factor authentication: “What you know”***

The most common type of one-factor authentication is usually a static password. The easier a password is, the more a user is likely to use it. But the easier a password is, the more vulnerable it is. The more complex a password is, the more difficult it is to remember, so a user is more likely to write it down. The more a password is written down the more vulnerable it becomes. Therefore, neither a complex nor an easy-to-guess password is secure enough on its own merit for online authentication. 3D Secure is an example of a card-not-present solution using static password.

### ***Two-factor authentication (2FA): “What you have”***

The two-factor authentication sometimes called 2FA or multi-factor authentication, is an additional layer of security after the basic username and password and is often dynamic. It introduces the “*What you have*” concept and this can take different forms. For example, using a personal authentication card, electronic token devices, or a code card. The two-factor authentication process adds an additional level of security to authentication. Its main disadvantage is that users find the extra authenticate step to be tedious and time consuming, as they expect to be able to login quickly to access their secure area. Two-factor authentication also costs businesses additional resources to implement (Altinkemer & Wang, 2011).

### ***Three-factor authentication: “What you are”***

Three-factor authentication adds an additional level of security by using the “*What you are*” concept. This uses personal attributes for authentication, including biometric fingerprinting, iris scanning and voice recognition technologies. Each additional step creates an additional layer of security, additional time taken to complete a given authentication session, and additional delay caused to users, and involves additional resources to implement and manage (Altinkemer & Wang, 2011).

<b>Characteristics</b>	<b>One-Factor</b>	<b>Two-Factor</b>	<b>Three-Factor</b>
<b>Data</b>	Static/digital	Dynamic/digital	Static/physical
<b>Type</b>	Username, password	Card, device, token	Attributes, i.e. Biometric
<b>Environment</b>	Login, Access, CNP	Login, Access, CNP	Login, Access, CNP
<b>Vulnerability</b>	High	Low	Low
<b>Security</b>	Low	High	High
<b>CNP solution</b>	3D Secure	3W-ADA Sentry	

*Table 1: Authentication factors assessment chart*



### **1.6.3.2 Static vs. dynamic authentication data**

Most existing card-not-present fraud solutions rely on one-factor authentication. However, the factors are either a static data type or decision made by probability based on past history. This research shows that such factors do not add acceptable value to security requirements and instead exposes personal data to risk.

Static data types includes card numbers, serial numbers, CVV, card expiry date, billing address, date of birth and 3D Secure passwords. In addition to the fact that these details are static and vulnerable to identity theft, they also expose customers' privacy to other types of online fraud by making their personal details available on the internet. An instance taken from the 3D Secure popularly known as "Verified by Visa" and "MasterCard SecureCode", revealed that this approach, while attempting to solve the card-not-present problem, created more problems by putting the personal details of online shoppers at risk. Using the past transaction history of a card to make decisions is not reliable because cardholder's circumstances can change over time as a result of economic changes or fraud within the existing card history may not be detected.

In contrast, the 3W-ADA Sentry solution replaces the use of personal details with a personal authentication code drawn from the concept of analytic geometry, and thus makes the personal authentication code dynamic, flexible to use, low cost, and non-electronic to implement and manage.

### **1.6.3.3 Security of card and personal information in a CNP environment**

Most card-not-present fraud originates from card-not-present transactions carried out by the legitimate card holder. This is because cardholders are significantly exposed to identity theft each time they pay online. Fraudsters tends to use sophisticated technologies to monitor the personal computers of their victims. This includes installing spyware remotely through an email or web link. Once a personal computer becomes vulnerable via this spyware installation, whatever data that passes through the screen of the personal computer, including key strokes, are remotely monitored by the fraudster. The more a cardholder pays online the more vulnerable his card and personal details become.

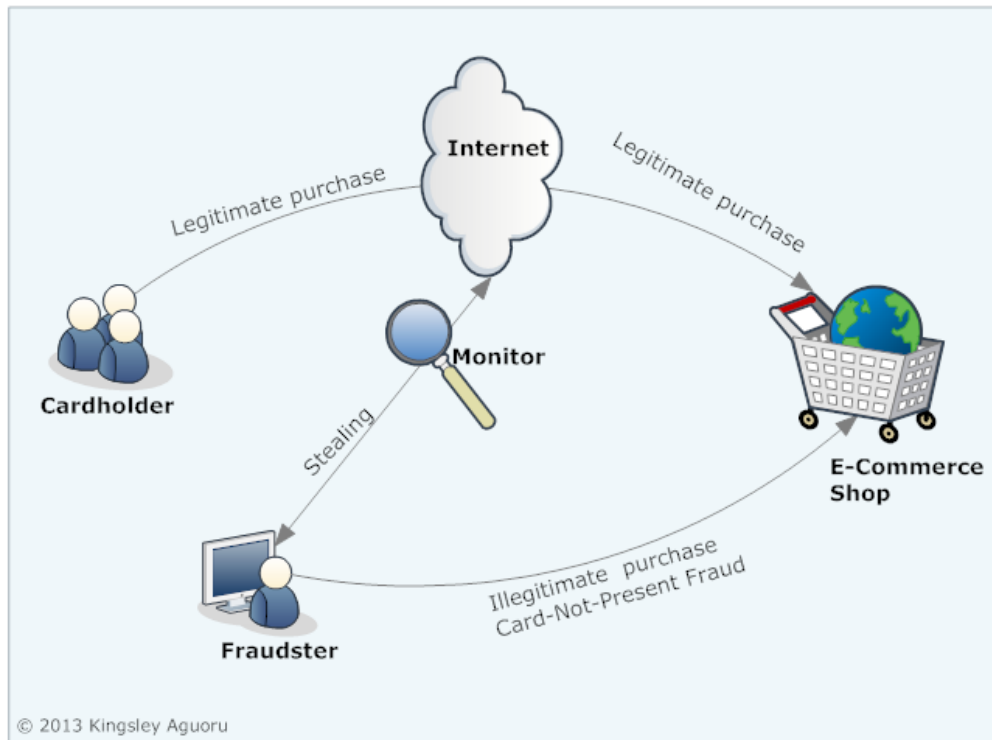
The wide use of personal information, including full name, billing address, and sometimes, date of birth by current solutions poses a great security risk and opens doors for other types of impersonation. In contrast, the 3W-ADA Sentry exchanges the requirement for personal information with a time limited dynamic token, while maintaining the profile of the customer. In the event of an interception, the interceptor can only capture the authentication token, which is already expired and meaningless.

#### **1.6.3.4 Benefits of replacing existing solutions with 3W-ADA Sentry**

The benefits of replacing the existing card-not-present solutions with the solution introduced by this research, are grouped under two headings:

##### ***Protection of personal identity online***

Full name and billing address are normal prerequisites to complete a card-not-present transactions and as the number of online shoppers increases, this also increases the volume of personal information submitted online. This has motivated criminals to implement various identity theft techniques to remotely steal personal and card information without the knowledge of the victim.



*Figure 2: Identity theft technique*

Replacing the existing card-not-present solutions with the 3W-ADA sentry solution will prevent customers from entering their personal information online to pay and thus reduce identity theft of personal information.

### **Security and authentication to prevent fraud**

Existing card-not-present solutions authenticate customers with static information transferred over an insecure network, which is therefore vulnerable to identity and impersonation because criminals can intercept the static information and use it to make fraudulent payments online.

Replacing the existing card-not-present solution with the 3W-ADA sentry solution will add an additional one-time dynamic token which even if intercepted cannot be used to make a successful payment online.

## **1.7 The research approach and context**

The method of this research is guided by the flowchart illustrated in Fig. 3 and the research approach framework in Table 2. The research result helps to understand the logic and preparation of a specification requirements for a new solution. The research approach is divided into three sequential categories:

### **1.7.1 Investigation**

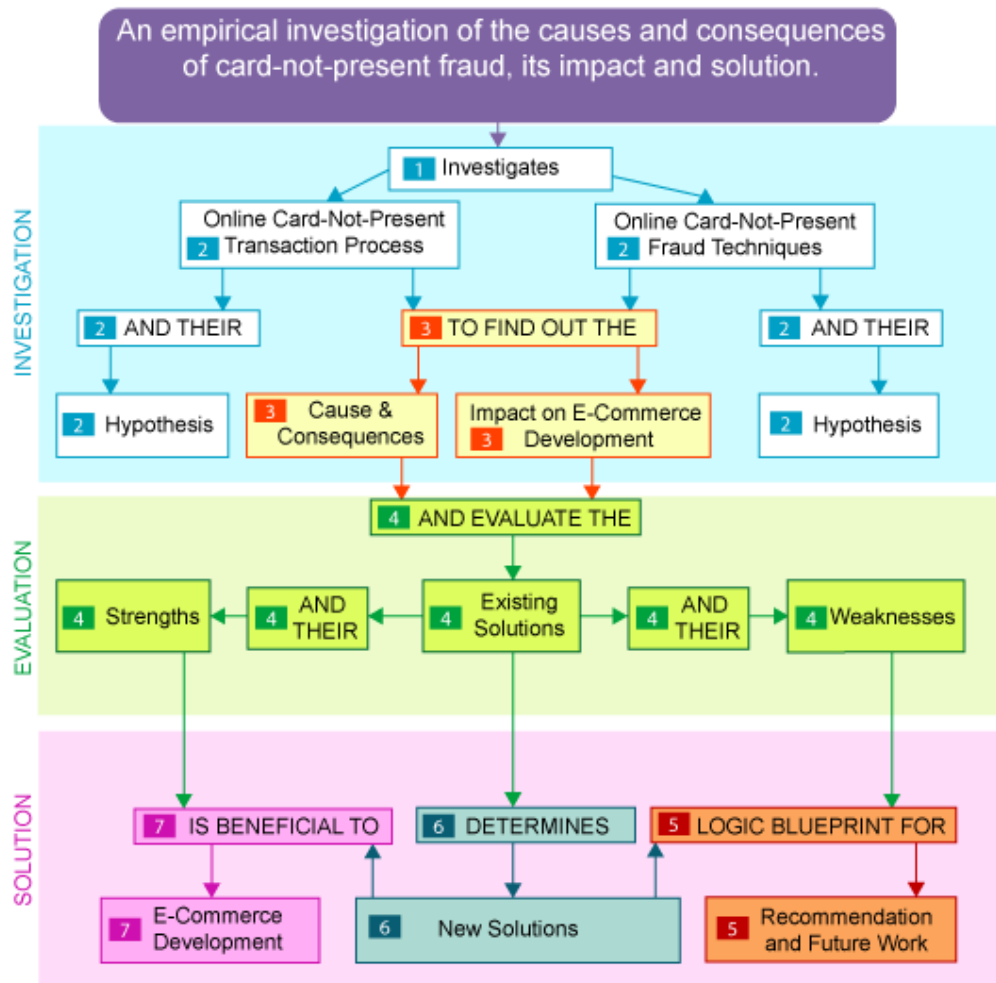
In this category, this research will investigate the online card-not-present transaction process and related fraud techniques, to find out the causes, consequences and impact on the development of electronic commerce.

### **1.7.2 Evaluation**

In this category, this research will evaluate the strengths and weaknesses of the existing solutions to establish where and why they failed.

### **1.7.3 Solution**

Finally, the result of the investigation and the evaluation of the existing solutions will determine, and stand as the blueprint for, the development of a new solution which will be beneficial to electronic commerce development, and provides a framework for future research on the topic.



Copyright 2011 Kingsley Aguoru

Figure 3: The research plan flowchart

To support the above flowchart, the approach is described further in Tables 2 and 3. These provides a guideline for achieving the objectives of each area.

Stage	Area covered by research	Research approach
1	Understanding the process and problem of card-not-present transaction, the fraud infiltration techniques, the strength and	Interview, literature review, case study and an observation of a card-

	weaknesses of the existing solutions and the problem requirements.	not-present transaction including existing hypothesis.
2	<p>Evaluation of the strengths and weaknesses of the existing solutions.</p> <p>Checking the fraud infiltration processes and techniques.</p> <p>Identification of the impacts on the development of e-commerce.</p> <p>Identification of the causes of the problem and the area which need to be addressed.</p>	<p>An empirical testing of the existing solutions with different types of cards in legitimate and illegitimate perspectives to understand their strength and weaknesses to determine the modus operandi and level of the infiltration processes of a successful fraudulent transaction.</p> <p>Further literature review, interview and case study.</p>
3	<p>Design and justification of the solution and its framework.</p> <p>Implementation of the prototype of the proposed solution.</p> <p>Evaluation of the new solution</p>	<p>Detailed specification requirements and design of the solution including the use of UML, Use Cases, Class, sequence and functional diagrams. User Acceptance Testing, and evaluation of the prototype and documentation.</p>
4	Reports and Thesis write up.	Thesis write up and documentation.

*Table 2: The research approach framework*

Research Method	Stages	Research method logic
Research and literature review	1, 2, 3 and 4	Preliminary research carried out to have a clear understanding of the problem and its characteristics by collecting and analysing journals, articles and resources relating to e-commerce card payment from reliable sources.

		Also review of the official documentations and reports carried out by APACS The UK Payment Association.  Review of report from the stakeholders.
<b>Interview</b>	1, 2, 3, and 4	Interview with the sponsor - Paymenex Limited, selected internet merchants from United Kingdom, Panama, USA, Canada, Ghana, and Cameroon, Regional Administrators of Paymenex Limited in 8 countries, staff from other card transaction network organisations, acquiring bank and Card holders to establish facts about the problem, perception and what they feel about e-commerce.
<b>Case Study</b>	1 and 2	Case study of the sponsor including selective case studies from other organisations. Reports from UK Payments Association.
<b>Feedback</b>	2 and 3	Feedback from user acceptance testing and where necessary, including during the testing and evaluation of the prototype.

*Table 3: The research method logic*

## **1.8 Research Structure**

The Research is structured in five parts as follows:

**Part One:** This part provides an overview of the research, its objectives, approaches, and methodologies. After reading this part, the reader will be equipped with the research question, purpose, scope and approach, including the overview of the research sponsor, motivation and problem statement.

It also outlines previous work and research in this area, the contribution of this research to the knowledge and understanding of e-commerce, card-not-present transactions,

related fraud and the perspective of its behavioural impacts among participants of electronic commerce.

**Part Two:** The aim of this part is to present the background of studies found in literatures relating to card-not-present fraud, its causes, consequences and impacts on electronic commerce, including all components related directly or indirectly to card-not-present fraud or its solution. After reading this part, the reader will understand the background of card-not-present fraud, infiltration process, causes, existing solutions, its relationship with identity theft, and the impacts on electronic commerce development.

**Part Three:** This part presents the background information and framework of the proposed 3W-ADA Sentry solution, including its concept, justification, and SWOT analysis. It further describes the overall roadmap of the solution development, from software requirements specification to design and user acceptance testing. After reading this part, the reader understand the background, design and implementation of the proposed solution.

**Part Four:** This part of the research presents the verification, validation and evaluation of the solution, drawing on reports from the software requirements specification, user acceptance testing, and live business application. After reading this part, the reader will understand how the solution is validated, verified and evaluated.

**Part Five:** This part of the research presents a summary and conclusion of the research, and suggestions for the direction of future research in related areas.



## **2. PART 2 – BACKGROUND AND LITERATURE REVIEW**

### **2.1 Introduction**

One of the most critical requirements of electronic commerce is the need to exchange payment electronically. According to Kim, et al. (2010), the development of electronic commerce will be strengthened if trusted and secured payment systems are implemented.

It is a general perception that trust is an intangible, vague concept - but a critical element that must be incorporated into electronic commerce without which the merchant is ruined (Beatty, et al., 2011).

According to Sullivan (2010), as the perception of risks and threats continues to increase in electronic commerce payment technologies, the need for information security and assurance of trust on the internet continues to be seen and acknowledged as a critical requirement.

As shown in a recent research (Montague, 2011), online card payment is the foremost of electronic commerce payment systems. It is classified by the payment industry as card-not-present (CNP) because the merchant is not in possession of the physical card when the payment is processed or the physical card is not present at the point of sale.

However, according to Bhattacharyya, et al. (2011) and Gold (2014), the level of credit and debit card fraud has drastically increased in the recent years. Criminals have learnt new and sophisticated technologies to harvest large quantities of card-related for several reasons which includes selling the data in the commodity market or using card details to commit card-not-present fraud.

Recent research (Gold, 2014) has shown how the vulnerabilities and flaws in online card payment have been exploited by fraudsters and online criminals who impersonate others to commit card fraud. Such fraud takes advantage of the current use of static payment card details and the weaknesses in the card payment approval process, which have been

established as unsafe and vulnerable to fraud. There are adverse effects, as a result, upon online merchants and consumers (Asokan, et al., 1997).

There is a need, therefore, for payment systems that users can trust, and that remove the perceptions of vulnerability, fraud and threat that are associated with payment systems used in electronic commerce (Bharat, 2013).

Authentication in CNP environment, to assure non-repudiation and legitimacy of payment, is the biggest challenge faced by online merchants. It requires maximum attention because the consequences of fraud, and of breach of security arising from this process is continuously growing and impeding the trust of merchants and consumers participating in e-commerce. The basic starting point of establishing trust online has been eroded (Suh & Han, 2003, p. 136; Yu-Hui & Stuart, 2007, p. 21).

Consumers making card payments online are apprehensive about the safety of their card details transmitted over the internet, and about the reliability of the merchant, while on the other side of the internet, merchants accepting card payments online are apprehensive about the legitimacy of the card details being received. Both parties cannot verify if the other party is who he claimed he was. Electronic commerce is an emerging technology but the unavailability of an acceptable and trusted payment system has adversely impacted its future development (Zhou, 2004; Laudon & Traver, 2004; Abrazhevich, 2004).

While it is widely believed that visible improvement in payment security strengthens trust among participants, it is also a fact that the security of an e-commerce payment system and the resulting trust of users boosts the development of e-commerce. Therefore, the perception of users, and their beliefs concerning the security of electronic payment systems, is a key element in the trend of e-commerce technology (Wilson & Abel, 2010).

It is important to understand who pays when a fraudster purchases goods and services online using stolen card details (Montague, 2011). Players in the card payment industry promote a range of solutions, including 3D Secure, to prevent online payment fraud, but they are careful to avoid the burden of the consequences of such fraud. In most cases, it is the merchant who bears the loss resulting from card-not-present fraud. In contrast, the

card payment industry and card issuers guarantee most card-present payment, which carries the lowest risk because it uses chip and pin technology that demands the presence of the physical card and knowledge of the corresponding PIN.

## **2.2 Information**

Information has different meanings in different contexts. However, by taking a logical approach to information we can express or identify information in three principal ways: information as a process or data; information as a knowledge or meaning; and information as a thing or entity. Sometimes, information can be expressed in ways that are hard to measure. It can also be expressed in many formats, and converted from one format to another (for example, from waveform or analog to symbol or digital). In recent years, the trend in information communication technology has been to use digital or electronic information, usually held or accessed through computer systems or other electronic devices (Buckland, 1991; Anderson & Johannesson, 2006).

### **2.2.1 Value of information**

As more information and data goes online, information is increasingly becoming a primary strategic asset that requires satisfactory administration in achieving organisation's objectives. However, within the business world, many organisations understand and treat information as an overhead cost, to be managed secondarily according to available resources, and in the event that a business is going through difficult financial times, information protection activities are among the first aspect to be reduced. (Quigley 2005; Porters & Millar 1985; Davenport & Cronin, 1988).

According to Bowonder & Miyake (1992), research has confirmed that information adds potential value to every individual and organisation. Several analyses have described the importance of information from many perspectives including:

- Information is the lifeblood of an organisation (Scarrott, 1985).
- Information adds value and enhances products' usability and meaning (Davenport & Cronin, 1988).

- Information is and organizational strategic asset (Quigley, 2005).

Irrespective of these wide and coherent descriptions and appraisals of information, the decision makers of many large organisations see the management of information as less important and therefore fail to adequately recognise information as an asset that adds significant value to their day-to-day business operations. This is the case, even though information is the key element of consumer-merchant interaction, via electronic commerce.

### **2.2.2 Information Security and Assurance**

Andress (2011) defined Information Security as the protection of our data, information and its systems from unauthorized access, theft, disclosure, usage, damage, modification and interruption, while (Gifford, 2009) summarised information security as the process of ensuring the confidentiality, integrity and availability of data.

Aguoru (2007) advanced a concept of information security using the catchphrase “*Let likes be secured by likes*” and argued that information security means using confidential data and strategy to secure confidential data and strategy.

Information Security and Information Assurance (IA) have their own individual meanings, even though they are wrongly used interchangeably. Information security deals with the protection of information, while information assurance, as its name implies encompasses all the roles of information security, information current state and information security countermeasures with descriptive sub-sets as illustrated in McCumber INFOSEC Model of Information Assurance. These form the building blocks to establish trust and confidence that the information is actually protected (Voas & Wilbanks, 2008, p. 10; Maconachy, et al., 2001, p. 306).

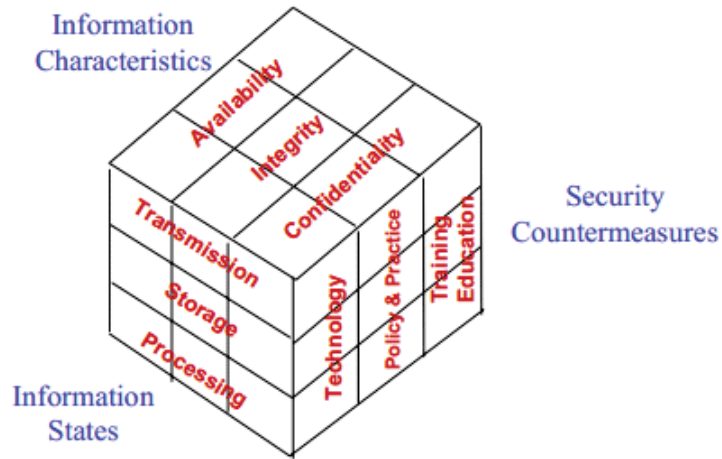


Figure 4: McCumber Information Assurance Model (Maconachy, et al., 2001)

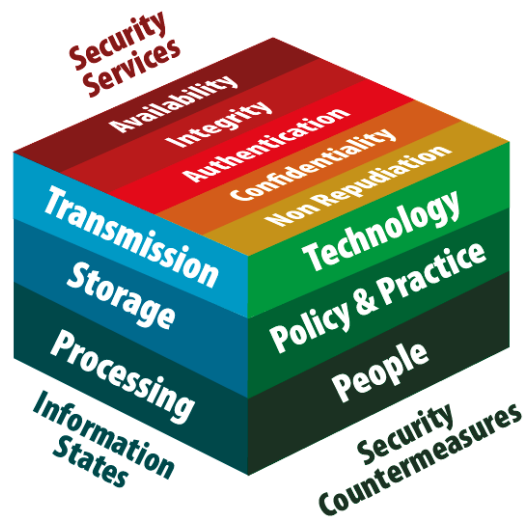


Figure 5: Modified McCumber Information Assurance Model (Maconachy, et al., 2001)

According to Maconachy, et al., (2001, p. 306) in today’s information-intensive economy, researchers and professionals have widened and modified the concept of the McCumber model in line with the trend of information superhighways, threats and security concerns.

The modifications resulted in the inclusion of subsets with the three designated domains of the model as illustrated in the following table:

<b>Security Services</b>	<b>Information State</b>	<b>Security Countermeasures</b>
a) Availability	a) Transmission	a) Technology
b) Integrity	b) Storage	b) Policy and Practice
c) Authentication	c) Processing	c) People
d) Confidentiality		
e) Non Repudiation		

*Table 4: Subset of Information Assurance Model*

### **2.2.3 Trust**

The Oxford English Dictionary defines trust as “*a firm belief in the reliability, truth, or ability of someone or something*”. While this definition is a common interpretation of trust, in the context of computer science it is difficult to measure reliability, truth, and ability.

According to Bidgoli (2006, p. 67), “*Trust is a willingness of a party, called a trustor to depend on another party called a trustee, for an action that is important for the trustor*”.

Trust in face-to-face interaction between the trustor and the trustee is significantly different to the trust in electronic and remote contexts, where the trustor and trustee are not face-to-face. Hence, building trust in electronic commerce without face-to-face interaction is a huge problem affecting the electronic commerce, and the greater the level of risk perceived in the interaction, the greater the level of trust required (Rocco, 1998).

According to Song, et al. (2007), there has been a tremendous surge in the use of the internet to exchange information following the spread of internet technologies. However, exchanging information online involves risk and threats of imprecise and bogus information, which raises huge reliability and trust concern among trustor and trustee. To prevent transmission of ambiguous, forged and untrusted information, system administrators must strengthen their information communication systems including user authentication systems.

#### **2.2.4 Research insight of Information and Trust in electronic commerce**

Information security, information assurance and trust have been identified as key factors in, and critical requirements of, electronic commerce systems, to assure information reliability, general performance, and acceptability among trustors and trustees. Unfortunately, the aspect of electronic commerce components involving online card payment systems have long-standing trust problems and difficulties. These problems and difficulties have resulted in the increasing incidents of online card fraud and identity theft, largely facilitated by the absence of physical interaction and an unacceptable level of trust that exists between the trustor and trustee.

Aligning trustor and trustee in the context of online card payment is difficult, as both the cardholder and the merchant have behavioural elements of trustor and trustee, and these are interchangeable depending on the activities and their context within the information system at any given time. During online card payment, the cardholder (acting as the trustor) must establish an acceptable level of trust with the merchant (acting as the trustee), which will motivate the willingness of the cardholder to transfer his card and personal details to complete an online payment. Conversely, when accepting an online payment, the merchant (acting as the trustor) must also establish an acceptable level of trust with the cardholder (now acting as the trustee) which will motivate the willingness of the merchant to accept the online payment, submitted remotely, with the belief that the payment is not fraudulent.

The information systems in use by the trustor and trustee in electronic commerce, including the electronic payment systems, have long been exploited by criminals in

different ways. The resulting perception of risks, threat, and fraud has intensified and influenced the trust of the parties involved.

## **2.3 Background to Electronic Commerce (E-Commerce)**

Electronic Commerce or e-Commerce technology began in the 1960s during the development of the Electronic Data Interchange (EDI) for the exchange of electronic transactions and business information between computers over a network without human intervention. There have been transitions in the meaning and use of the term “electronic commerce” within the past 40 years, during which time it has applied chiefly to technology that facilitates information exchange and business transactions – for example, purchase orders (Botha, et al., 2008, p. 434; Laudon & Traver, 2004, p. 337; Anumba & Ruikar, 2002, p. 267).

However, there were compatibility issues with the data format and protocols used by different businesses in this channel, so it was not possible for many organisations to send or receive EDI communications to and from other organisations. This was a challenge faced by EDI until the development and publication of the first version of ASC X12 in 1982 by the Accredited Standard Committee as an American national standard, chartered in 1979 by the American National Standards Institute (ANSI) (McKay & Piazza, 1992).

The meaning and use of electronic commerce expanded during the development of the Mosaic web browser at the National Center for Supercomputer Applications of the University of Illinois USA, and the introduction of different types of electronic payment cards and vouchers, Electronic Fund Transfer (EFT) and Enterprise Resource Planning (ERP) applications in 1990s (NCSA, 2009).

### **2.3.1 The trend of electronic commerce**

Today, electronic commerce largely means the buying and selling of goods, services, and the exchange of values and business transactions electronically with the use of computer systems and technologies such as the World Wide Web, telephone and facsimile.



Electronic commerce is a very popular activity on the internet. It has transformed the traditional face-to-face buying and selling marketplace, or "bricks and mortar" into a world of virtual, ubiquitous marketplaces of convenience, or "brick and click" (Gunasekaran, et al., 2002; Bushry, 2005, p. 3).

Sellers can not only sell their products and services through their established high-street shops, but can also achieve a virtual shop (available always and everywhere) with the power of the internet, by simply adding some images and descriptions of their products and services to a website application, and with the integration of a payment processing gateway to accept payment electronically. The worldwide access to information offered by the internet technologies has greatly widened the market reach for sellers to showcase their products and for buyers to search for products and services beyond their geographical location (Bhasker, 2006).

Electronic commerce or "e-commerce" derived its name from the traditional word "commerce" which generally encompasses exchanging, coordinating, buying and selling of goods and services. The term "electronic commerce" covers the use of any electronic methods in commerce, instead of face-to-face interactions, for example, the internet network and the World Wide Web (Mohapatra, 2012).

### **2.3.2 Types of electronic commerce**

Organisations and individuals participating in electronic commerce activities rely heavily on the internet network and information systems. The internet and the World Wide Web offers an important network between the seller, the buyers and other coordinators to enable electronic communication of information.

According to Mohapatra (2012, p. 77), the most popular type of e-commerce categories are Business-to-Business (B2B), Business-to-Consumer (B2C) and Consumer-to-Consumer (C2C). Other less common types include Business-to-Government (B2G) which refers to e-commerce dealing between companies and the government, and Business-to-Employee (B2E), which covers companies dealing with the employees such as requisitioning of supplies by employees. The channels of electronic commerce have extended to mobile devices, for which the term Mobile Commerce or m-Commerce

applied. In m-commerce, transactions take place through a wireless mobile device -for example, smart phone and tablets.

**Business-to-Business (B2B) e-Commerce:** Holzmuller & Schluchter (2002, p. 2), in discussing Business-to-Business (B2B), stated that organisations that are involved directly or indirectly in the buying and supplying of business products and services or other business activities that coordinate inter-organisational operations over an internet network, are participating in a business-to-business type of electronic commerce.

In the Business-to-Business category of e-commerce, companies are dealing directly with other companies. This can mean companies who are wholesale suppliers or manufacturers supplying their goods and services to other retailing companies who deal directly with the consumers, companies supplying their raw materials to the manufacturers, to support product, and organisations providing business services, for example, technology infrastructures, corporate financial services provided by banks and accounting firms.

**Business to Consumer (B2C) e-Commerce:** Business-to-Consumers (B2C) is consumer-oriented, and the most common category of electronic commerce, in which companies sell their products and services directly to individual consumers rather than companies. Business-to-Consumer can be further broken down into direct and indirect marketing, full and partial virtual marketing, proactive or reactive marketing, and electronic intermediaries business to consumer categories depending on business strategies (Bushry, 2005; Hu, et al., 2004, p. 177).

**Consumer to Consumer (C2C) e-Commerce:** Consumer-to-Consumer e-commerce involves buying and selling between a consumer and another consumer such as an online auction. A popular online auction e-commerce is eBay. Other examples include social network websites, which allow consumers to interact with other consumers to exchange ideas and services (Mohapatra, 2012).

### **2.3.3 Key essentials of electronic commerce**

This research has broken down the essential processes of electronic commerce into three key categories, as follows.

### **2.3.3.1 Business Model and Workflow Management System**

The business model is an essential element of electronic commerce. A business model covers all aspects and methods of generating revenue, arrangement of the organisation, and all methods of generating values through the internet. In particular, it provides a blueprint of what the electronic commerce business is all about, and its core operations. This includes the purpose, business strategies, offerings, process and procedures, to clearly depict how an organisation will capture its value and revenue (Jansen, et al., 2007).

The workflow management system is a coordinated process of activities or operations that are connected to achieve a business goal, including all day-to-day processes and procedures. Hence, workflow is a synonym for business process (Van der Aalst & Van Hee, 2006).

### **2.3.3.2 Shopping Cart and Content Management System**

According to Zheng, et al., (2009) Online Shopping Cart and Content Management System are a web based infrastructure powered by the internet to manage products and customers online in today's evolving e-commerce. Shopping cart software continues to advance to include many components that add flexibility to e-commerce. The most common features and components of a shopping cart includes:

- Catalogue and content management system used to add products images, descriptions, and prizes.
- Customer Relationship Management System used to manage customer information and orders.
- Payment system used to integrate online payment methods, such as credit card and electronic cheques.
- Shipping method used to manage the different available shipping methods, such as, standard, express and courier.
- Order Management System used to manage orders.
- Communication System, which this includes email and chat abilities used to communicate effectively with customers.

As this technology is becoming sophisticated and complex, and the number of people joining the online trend grows, fraud and internet crime also continue to grow. E-commerce operates remotely on the internet, which makes it almost impossible to verify the legitimacy of who is selling and who is buying. As a result, the security of a shopping cart infrastructure must be designed to protect both sellers and buyers from hackers and fraudulent activities - for instance, unauthorised access, card-not-present fraud and eavesdropping.

## **2.4 The B2C e-commerce transaction flowchart**

According to a recent research (Aguoru, 2007), to complete a purchase, including settlement of payment, in an electronic commerce transaction, the following parties are usually involved.

### ***The Card Association or Network***

Also called the card scheme, this is usually an organisation that operates an interchange or financial payment network. They process, clear and settles all transactions on their network on behalf of the card issuers and the acquirers - for instance, Visa, Paymenex, MasterCard, and American Express.

### ***The Card Issuer***

This is usually the bank or other financial institutions approved by the card association to issue cards. They maintain and manage the monetary value of the card and the paying party.

### ***The Acquirer or Payment Service Providers (PSP)***

This is usually any financial institution or payment service provider approved by the card association to process payment on behalf of the merchant. They act as the process gateway of the merchant to the interchange network and the point of contact between the merchant and the cardholder in settlement. In addition, they often provide merchant accounts. Some payment service providers require you to obtain your merchant account from your bank, while they do only the payment processing.

### ***The Merchant***

This is usually the seller: any individual or business with a valid merchant account issued the acquirer or payment service provider which enables him to accept payment.

### ***The Cardholder***

This is usually any person with a credit or debit card issued by a card issuer against his name. All cards are linked to an electronic financial account through which it will access funds for payment – for example, bank account, or electronic money.

The diagram below illustrates the process of an electronic commerce payment. The successful transaction flows from No. 1 to No. 14. If repudiation occurs, the additional process from No. 15 to No. 17 follows subsequently, which often results in chargeback, usually at the disadvantage and loss of the merchant.

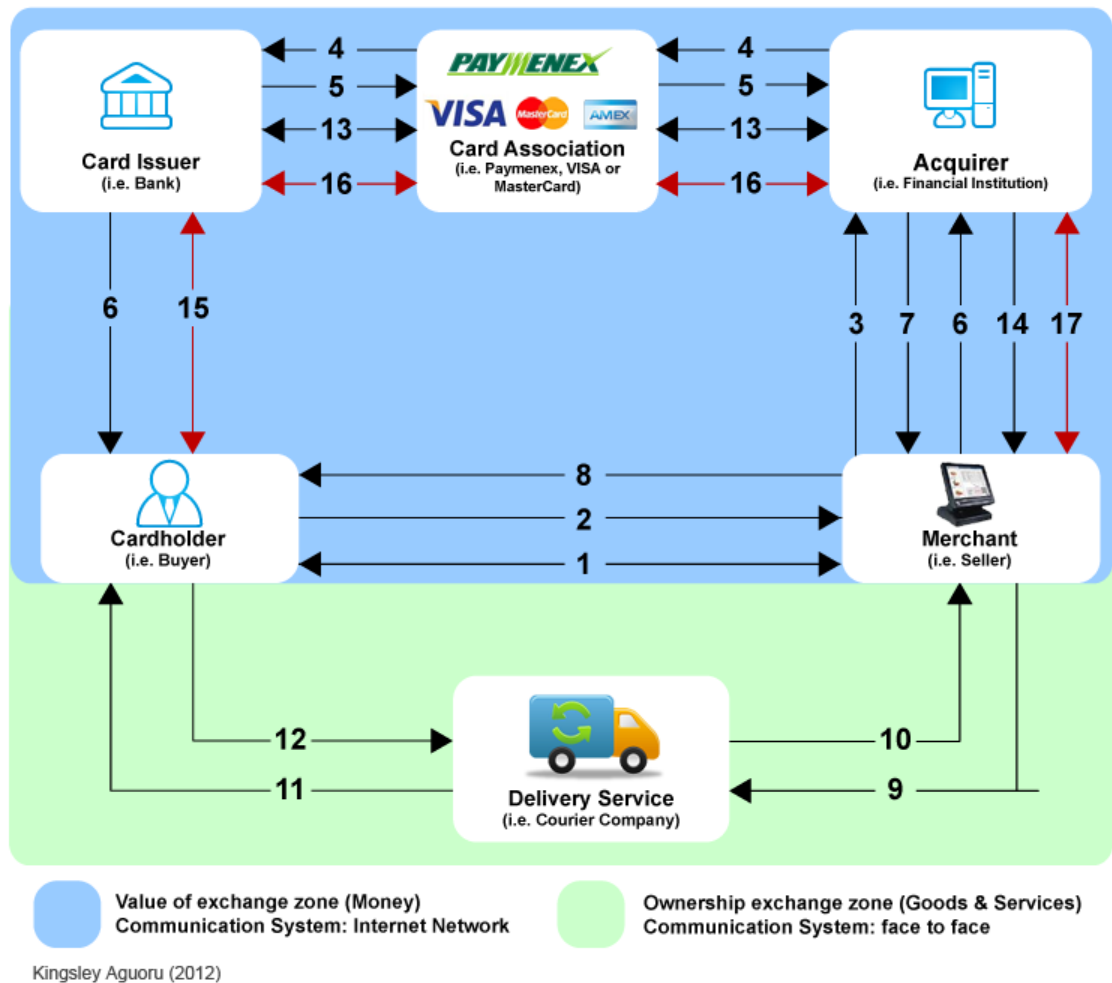


Figure 6: The Ecommerce transaction flowchart (Aguoru, 2007)

NO	ACTION DESCRIPTION
1.	Cardholder browses the merchant's shop, and chooses an item to purchase, and moves to the checkout page.
2.	Cardholder submits card details and any other required information set out on the merchant's website - for instance, billing and delivery address and dynamic token to enhance security.
3.	The Merchant forwards the information submitted by the cardholder to his acquirer or payment processor to obtain approval.

4.	The Merchant's Acquirer routes the authorisation request through the network of the card association to the card issuer, (The Card Association will identify the card issuer).
5.	The Card issuer makes a decision to either decline or approve the authorisation request, and route the response back to the Acquirer through the network of the card association.
6.	The Card Issuer Debits the Cardholder Account.
7.	The Acquirer sends back the request to the merchant to enable him complete the order.
8.	The merchant displays or sends the order decline/approval to the cardholder.
9.	In the event of tangible goods, the merchant hands over the item to the courier service for delivery, (Digital Goods are usually delivered electronically).
10.	The Courier Service signs accepting the goods for delivery to the cardholder.
11.	The delivery company delivers the goods to the cardholder, who is the buyer.
12.	The Cardholder signs the receipt of the goods.
13.	The Card Issuer and the Acquirer clear and settle the transactions through the card association who act as the middleman.
14.	The Acquirer pays the merchant.
	<b>ADDITIONAL PROCESS IF THERE IS REPUDIATION OR FRAUD</b>
15.	The Cardholder contacts his card issuer (financial institution) to deny having placed the order, or if the goods received are not as described on the website, (This usually occur when cardholder notice an irregular debit on his account statement).
16.	The Card Issuer opens an investigation into the transaction through the card association by filing a dispute.

17.	The Acquirer contacts the merchant and requests for a proof that the legitimate cardholder actually placed the order, (this is usually a request of a signed proof of payment). In most cases, the merchant cannot provide a signed agreement because the purchase was made online, and this results in the Acquirer debiting the merchant account in a process called chargeback, which sometimes includes a chargeback administration charge.
-----	---

*Table 5: Legend of e-commerce transaction flowchart*

## **2.5 Electronic commerce: pros and cons to businesses**

Businesses now do not need to make expensive investment in setting up retail shops on the high street and recruiting employees to manage different department of the shop. Rather shops are represented online by putting some webpages together, adding some products and the shop is open for business, the job that would have been done by staff is handled automatically by technology or managed by staff working from home. Electronic commerce also reduces the cost and time of processing, distributing and making information and products available where and when it is needed, businesses is open to sell their goods and services anywhere in the world and can operate from the comfort of their homes.

Despite the benefits of electronic commerce, it has some technological and non-technological limitations that have impacted on the growth and acceptance of electronic commerce. Selling entirely online means that the seller must also have corresponding electronic method to accept payment online, and in most events where a cardholder denies having placed an order or payment online, the card issuer files a chargeback to the merchant's acquirer who consequently revises the transaction and debits the merchant irrespective of if the merchant has already delivered the goods. Cardholders often deny having made payment online in some scenario where their card details where stolen and used online without their knowledge to place fraudulent order.

Other limitations includes non-availability of globally accepted security standards, legal and ethical issues, acceptable system security, and trust; while the non-technological



limitation includes the consumer perception of the insecurity and trust of electronic commerce which affects many consumers to shop online (Anumba & Ruikar, 2002).

## **2.6 The electronic commerce pros and cons to consumers**

According to Rainer and Cegielski (2011), electronic commerce technology has provided enormous benefits to mankind by placing national and international markets at the doorstep of every household: easily reached and accessed from anywhere and anytime, consumers do not need to be in the shop physically to buy their needs, goods and services can be purchased and paid for entirely online and have it delivered to the consumers' doorsteps.

Goods and services are easily searched for using the search engines, consumers do not need to parade through the streets to search for required goods or services from shop to shop, and by using the internet consumers can search, find, buy and get it delivered without leaving his location. Electronic commerce saves consumers the time and cost of transportation to shop locations - one could imagine the time, risk and cost to travel from United Kingdom to Japan simply to purchase an item.

Despite these benefits, electronic commerce is a double-edged sword as it also has range of disadvantages to the consumer. The cardholder making payment remotely is worried because his card details could be stolen online to commit fraud or concerned about placing an order with a fraudulent online merchant or criminal who actually will not deliver the purchased goods or services.

Shopping online does not allow the buyer to feel the real physical goods, rather goods are represented with electronic photographs and they might not appear in real life as they look on the photograph. Other disadvantages includes delivery time which can take some time as opposed to buying and taking your goods with you instantly (Aguoru, 2007).

## **2.7 Electronic Commerce payment systems**

According to Aguoru (2007) the more e-commerce activities is completed entirely on a remote network, the more it has its full claim as electronic commerce, and to support the buying and selling of goods and services completely done on the internet, buyers should have a means of sending payment electronically from a remote and anonymous location over the network and the sellers also should have the corresponding system to accept such an electronic payment as a means of exchange of value.

This raise a great concern of the level of security that exists in each phase of the process because money and goods are transferred without any physical contact of the buyer and the seller and the slightest recognition of the possibility of the absence of security, trust, confidence and adaptability in the payment system weakens the process thereby creating adverse impact on the e-commerce infrastructure, hence, several key factors must be assessed and considered before payment system is accepted or deployed, these key factors includes, Technology, Economic, Social, Institutional and Regulatory (Kuo, et al., 2002).

Electronic payment systems evolve comparably with the evolution of e-commerce, giving rise to the institution and advancement of different electronic payment methods by many organisations who issue them with a promise and agreement to exchange them with a legal tender, such as, (electronic money or e-money, e-gold, digital money, digital cash and e-Vouchers), Credit and Debit Card, Electronic Cheques, and Store Values. However their sources are rooted in the traditional payment method used in face to face payment: for instance cash, cheque, bank transfer and credit or debit card which remain the first and dominant use of e-commerce payment systems.

<b>Features</b>	<b>Credit Card Debit Card</b>	<b>E-money/ e- cash</b>	<b>Electronic Cheque</b>	<b>Store Value</b>
Place of Use	Online and offline	Online	Online	Online/Offline
Data required	Card and personal details	Account ID	Bank Account No/Cheque No	Card details
Data Format	Static	Static	Static	Static

Issuers	Financial Institutions	Operators	Banks	Store
Acceptability	60	10	12	18
Anonymity	Partially and Entirely	Entirely	Partially and Entirely	Partially and Entirely
Merchant Acquiring	Yes	No	Yes	No

*Table 6: Characteristics of electronic payment systems*

### **2.7.1 Electronic payment card system**

Payment card is the most popular and dominant of electronic payment systems in today's e-commerce, tracing its root more than 100 years ago when consumers and businesses dealt with cash, cheques, and non-electronic courtesy cards issued in a paper form specifically for entertainment and holiday, until 1966 when Bank of America Service Corporation established a general purpose card later renamed to Visa and other banks formed the Interbank Card Association as a competitor and later renamed as MasterCard. Both Associations remain the dominant operator of card networks (Baxter, 1983).

Other card associations or payment networks includes; American Express, Paymenex TransNET, Discover Network, JCB, Diners Club, and many more. Which continue to evolve with different features and innovations, in line with technology advancement.

The popularity of the internet and electronic commerce have greatly influenced the radical changes. From the manual payment card to electronic payment card, a payment card is a method of holding financial account data electronically in a piece of cardboard paper, or plastic in a format readable or accessible by payment processing systems when making electronic payment. Such method is acceptable by merchants as a method of exchange of values.

Following the trend of technology, methods of holding the financial account data on a piece of card continue to grow from manual laser printed and encoded magnetic strip data, to chip-based smart contact, contactless or proximity cards, making it more flexible and convenient for consumers to access their funds anywhere and anytime.

In a payment card transaction, the physical cash note or coin is not exchanged, but the data stored in the payment card is used to access cash value in a form of electronic money and exchanged electronically through a computer network remotely or face to face. It is because such electronic data has the feature of unlimited replication through electronic channel, this makes payment card vulnerable to misuse and impersonation.

### **2.7.1.1 Types of payment card**

Different types and features exist in electronic payment cards in circulation following the boom of electronic commerce, but the most widely used types of card are largely dominated by the payment cards operated on the Visa and MasterCard networks.

**Credit card:** This type of card is issued by financial institution with features to offer a line of credit to their customers, which allow them to pay for goods and services online or offline in store with a repayment plan, and interest calculated on the annual percentage rate. In some cases cardholders can be allowed to withdraw cash from Automated Teller Machine (ATM) at the payment of surcharge. Both cardholder and merchant pay more to use or accept payment made with this type of card.

**Debit card:** This type of card is issued by banks and usually linked to a traditional bank account allowing the bank account holder to spend from a bank account balance, it is free to use for payment especially when paying within the country, and cost less to merchants to accept payment made with this type of card. The Debit card initiative was launched in United Kingdom in 1987 and developed as a more convenient alternative to traditional cheque payment. Since cardholders can access money or manage bank accounts at any ATM accepting the brand anywhere in the world (Anderson, 2008).

**Prepaid card:** This type of card is prepaid with certain limit and can be reloaded and used to make payment, or withdraw cash from ATM. This type of card is usually for people who do not have access to credit or debit cards or travellers.

**Store value and gift cards:** This type of card is issued by chain or departmental store operators and accepted specifically in their store. It is used as a marketing strategy to keep customers coming back and can only be used to buy goods or pay for services. Most store value and gift cards cannot be used at ATM for cash withdrawal.

### MasterCard



### Visa



Figure 7: Forn

### American Express



*Figure 8: Format of a Diners Club and American Express Card (APACS, 2005)*

## **2.8 Card-not-present fraud in e-commerce transaction**

According to the Nilson Report (HSN Consultants Inc., 2013), world card payment transactions hit a total of £13,823 trillion pounds in 2012, with an estimated 11.4% increase from the previous year, and the fraud losses from this volume in same year hit £7.21 billion also having an estimated 14.6% increase from 2011. Within this total losses card issuers suffered 63%, while acquirers and merchants lost the other 37% which are significant to payment made through the card-not-present transactions channel and this has increased the overall fraud losses as percentage of volume.

Approximately 50% of European internet users do to not usually agree to shop or make card payments online because they believe that their card and personal information will not be adequately protected by the online vendor, and a recent survey conducted by Visa on 15 financial Institutions in the European Union confirmed that card-not-present transaction on the internet accounts for almost half of all complaints and fraud reports (Philippsohn & Thomas, 2003).

The European Union's law enforcement agency (Europol) similarly reported that card-not-present transactions in the European Union accounts for 60% of all types of card fraud valued at 900 million euros (Europol, 2012).

There has been significant global growth in card payment transactions where neither the card nor the cardholder is present at the point of sale, generally referred to as 'card-not-present' (CNP). Such as, online, telephone and fax card payments, as the number of online buyers continues to soar, unexpectedly, the accompanying identity theft and card fraud also continue to have equivalent growth, as the technology continues to become more flexible, compact and complex.

According a recent report (Europol, 2012), card details are the perfect unlawful product of the internet because they can be electronically transferred and replicated, and criminals have benefited from this information digitalization which offer them low risk but profitable criminal activities, motivated by the nature of card-not-present transaction usage especially the authentication.

Authentication and authorisation in card-not-present transaction only verifies the correctness of the card details, as opposed to the authentication and authorisation of card payment made when the card and the cardholder is physically present at the point of sale, which verifies the personal characteristics of the card and cardholder.

The ability to verify that the card information submitted over a remote network is done by the legitimate cardholder therefore remains the authentication goal and a huge problem to all merchants who are accepting card-not-present payment, and this has resulted in a high level of migration of card fraud operations from the "*card present*" environment which appears to be more complex and difficult due to chip and pin technology to "*card-not-present*" where process is very flexible and the risk-level very low (Hunter, 2006).

Accordingly to Anderson (2008), the potentials of the internet anonymity, complexity of internet tools, flaws in card fraud solutions and low level of compliance with fundamentals of card authentication, integrity and non-repudiation as the key essentials to e-commerce security created a low-risk and flexible channel for many fraudsters to carry out identity theft and impersonation which facilitates the placement of fraudulent

orders with merchants who operates remotely, main aim includes to exploit these low risk and flexible avenues to carry on their fraudulent activities for financial gain, (Hunter, 2004).

The process and method of card-not-present authentication used in attempt to legitimately identify ourselves during online transaction is still a long established problem and the related vulnerabilities have increasingly been exploited by fraudsters. Ironically, the chip and Pin technology has been seen as secure a authentication tool to protect cardholder at the point of sale using PIN verification system, but this trend has its drawbacks and problems. Specifically, a rise in the instances of fraud occurring in card-not-present scenarios such as online, phone and mail order purchases which is continuously posing a tremendous threat to participants for several years, and regrettably, the chip and pin technology has done nothing to combat this type of fraud (Furnell, 2006).

Card-not-present fraud is understood to be the biggest type of card fraud ever in the history of card payment and the consequences are building up into a perceptible impact on transacting parties and the world economy.

The accounted development of card-not-present fraud in leading economies over the past years, and the associated impacts outstretched the need for a feasible framework or solution because it has raised persistent concern and dissatisfaction among the merchants and cardholders to doubt the robustness, flexibility and benefits of electronic commerce.

### **2.8.1 Card-not-present fraud losses in Australia**

The location of Australia is somehow said to be isolated from the prying eyes of card fraud taking place in other parts of the world, however, with trend of information and communication technology which enables electronic transactions and payments through the computer network, Australia is no longer privileged. Rather, card fraud has become a huge problem for Australian law enforcement agencies (Smith, 1997).

According the Australian Institute of Criminology (2011) credit card fraud increased approximately 70% since 2006 valued at \$56,512,389 Australian Dollars and \$110,500,699 in 2009.



Year / Category	2006-07		2007-08		2008-09		Rate	
	No	A\$	No	A\$	No	A\$	No	A\$
Aust Card	150,646	39,959,984	220,053	63,491,661	332,396	2,162,968	121%	106%
O/S Card	47,795	16,552,405	79,929	25,131,480	110,065	28,337,731	130%	71%
Total	198,441	<b>56,512,389</b>	287,896	<b>88,623,141</b>	442,461	<b>110,500,699</b>	123%	96%

Table 7: Australia Card-not-present fraud 2006 – 2009 (Smith, n.d.)



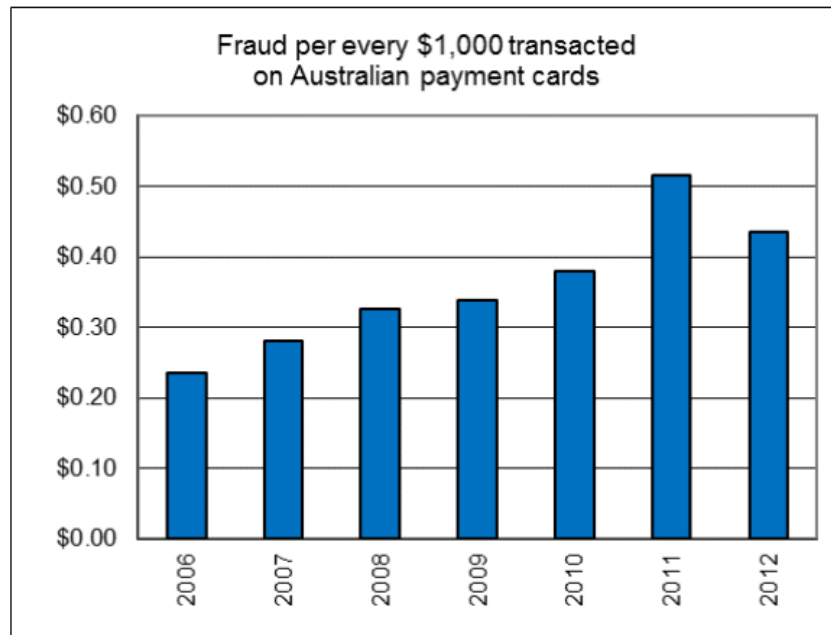
Figure 9: Australia Plastic Card Fraud by Type 2009 (Smith, n.d.)

The Australian Payments Clearing Association (APCA) reported a surge in card-not-present transactions up to 2010 where an estimated \$100 million Australian dollars has been defrauded through card-not-present transaction, which currently account for over 50% of other types of card fraud.

In a recent release (Australian Payments Clearing Association, 2013) card fraud in Australia show a year-on-year drop for the first time in 2012, card-not-present fraud dropped by 8% and this drop is attributed to the increase in the use of the 3D Secure – MasterCard SecureCode and Verified by Visa.

Scheme Credit, Debit and Charge Card Fraud Perpetrated in Australia and Overseas on Australia-issued Cards						
1 January 2012 - 31 December 2012						
Category	In Australia		Overseas		Total	
	Transactions	Value (\$)	Transactions	Value (\$)	Transactions	Value (\$)
Lost/ Stolen	83,636	14,414,354	21,889	8,318,853	105,525	22,733,207
Never Received	25,262	6,780,682	1,185	446,470	26,447	7,227,151
Fraudulent Application	5,185	3,409,868	274	93,059	5,459	3,502,927
Counterfeit/ Skimming	37,484	13,047,707	45,035	14,602,763	82,519	27,650,470
Card Not Present (CNP)	360,221	72,645,147	609,655	110,155,844	969,876	182,800,990
Other	3,016	714,014	1,352	355,619	4,368	1,069,634
<b>Total</b>	<b>514,804</b>	<b>111,011,772</b>	<b>679,390</b>	<b>133,972,608</b>	<b>1,194,194</b>	<b>244,984,380</b>

*Figure 10: Australian Scheme Credit, Debit and Charge Card Fraud 2012 (Australian Payments Clearing Association, 2013)*



*Figure 11: Fraud per every \$1,000 transacted on Australian payment card (Australian Payments Clearing Association, 2013)*

### **2.8.2 Card-not-present Fraud losses in Canada**

According to the Canadian Anti-Fraud Centre (2013), Card-not-present fraud is recognised as one of the developing card fraud types in Canada and in 2011 the Canadian Banking Association (CBA) reported that the card-not-present fraud accounted for \$259,498,535.00 showing an increase from the previous year, while 2012 also shown a 3.50% increase from 2011.

	2011	2012	
<b>Credit Card Fraud - (American Express Canada, MasterCard Canada, Visa Canada)</b>			
	<b>Loss in \$CAD</b>	<b>Loss in \$CAD</b>	<b>%Change</b>
Lost	\$10,757,451	\$8,663,910	-19.46%
Stolen	\$21,692,185	\$18,322,777	-15.53%
Non Receipt	\$4,736,900	\$3,628,009	-23.41%
Fraudulent Applications	\$6,075,704	\$8,522,715	40.28%
Counterfeit Domestic	\$88,356,720	\$68,652,172	-22.30%
Counterfeit Cross Border	\$31,809,823	\$49,457,366	55.48%
Card Not Present (Fraudulent e-commerce, telephone and mail purchases)	\$259,498,535	\$268,573,473	3.50%
Account takeovers & Other	\$13,661,440	\$13,543,195	-0.87%
<b>Total: Credit Card Fraud</b>	<b>\$436,588,757</b>	<b>\$439,363,617</b>	<b>0.64%</b>
<b>Interac Debit Card Fraud - (Interac Association - Not including other debit card fraud sources)</b>			
	<b>Loss in \$CAD</b>	<b>Loss in \$CAD</b>	<b>%Change</b>
<b>Total: Counterfeit</b>	<b>\$70,000,000</b>	<b>\$38,500,000</b>	<b>-45.00%</b>

Figure 12: Credit Card Fraud losses in Canada 2011-12 (Canadian Anti-Fraud Centre, 2013)

### 2.8.3 Card-not-present fraud losses in United States

United States generates 23.5% of the world's card payment transaction volume, even though it still accounts for 47.3% of world's card payment fraud losses. The majority of this can be attributed to the absence of chip and pin technology, hence, fraudsters counterfeit payment cards to defraud merchants at card present environment, and because the United States is leading in buying, selling and accepting card payment online, it also record the highest volume of card-not-present losses (HSN Consultants Inc., 2013).

## 2.9 Card-not-present fraud losses in United Kingdom

According to APACS (2012) lost and stolen type of card fraud has been the highest problem and pressing card fraud in United Kingdom within the 1990s when e-commerce technology was still at its infancy, and the number of people buying online was very low. However, in 2004 the fraudulent activities and losses arising from the card-not-present

transaction surged and overtook other types of card fraud and established itself as the more important type of card fraud with the value of losses having a continuous annual increase until 2009.

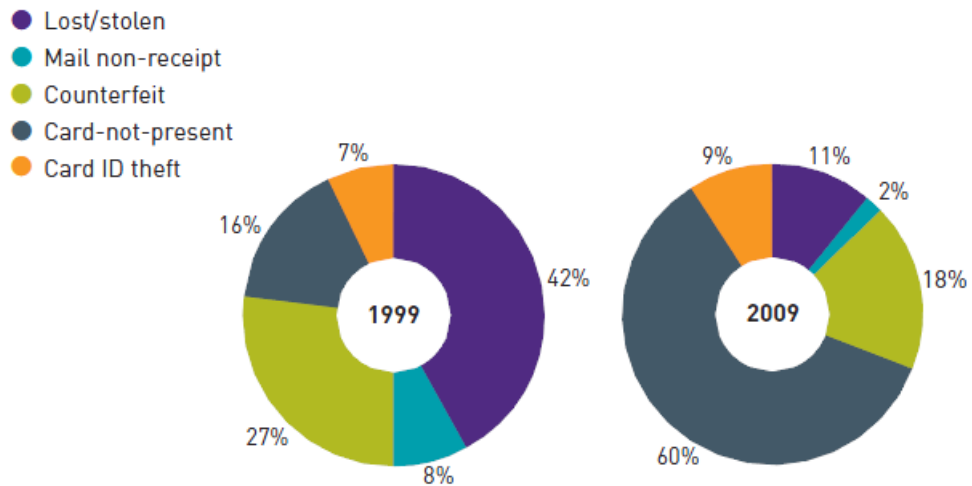


Figure 13: Percentage of Card fraud losses split by types (APACS, 2010)

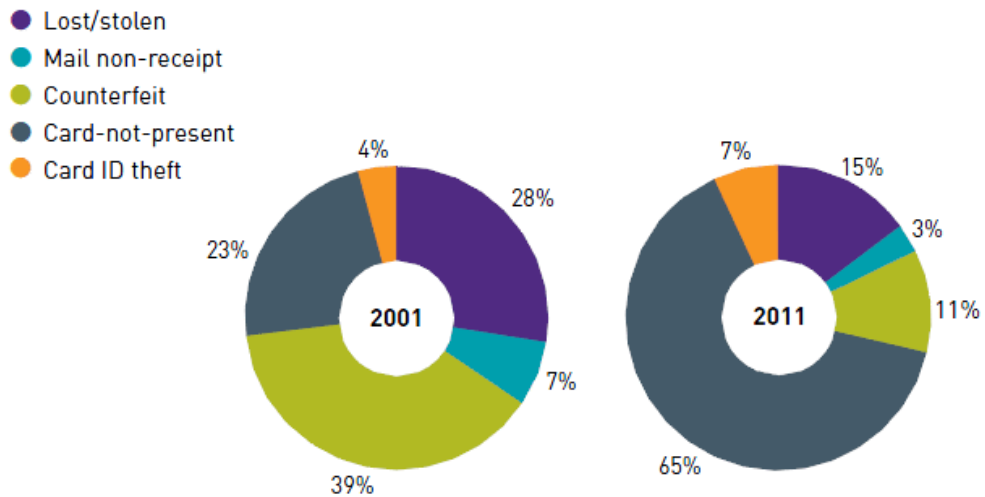


Figure 14: Percentage of Card fraud losses split by types (APACS, 2012)

The following table presents the analysis of card-not-present fraud losses in United Kingdom from 1995 to 2012:

<b>FRAUD TYPE</b>	<b>YEAR</b>	<b>LOSSES (in million Pounds)</b>	<b>Rate %</b>
Card-not-present	2014	479.0	+6%
Card-not-present	2013	450.4	+16%
Card-not-present	2012	245.8	+11%
Card-not-present	2011	220.9	-03%
Card-not-present	2010	226.9	-15%
Card-not-present	2009	266.4	-19%
Card-not-present	2008	328.4	+13%
Card-not-present	2007	290.5	+37%
Card-not-present	2006	212.7	+16%
Card-not-present	2005	183.2	+21%
Card-not-present	2004	150.8	+24%
Card-not-present	2003	112.1	+11%
Card-not-present	2002	110.1	+15%
Card-not-present	2001	95.7	+31%
Card-not-present	2000	72.9	+149%
Card-not-present	1999	29.3	+115%
Card-not-present	1998	13.6	+36%
Card-not-present	1997	10.0	+54%
Card-not-present	1996	6.5	+41%
Card-not-present	1995	4.6	84%

*Table 8: Card-not-present fraud losses on UK-issued cards – 1995 - 2014 (APACS, 2005); (Financial Fraud Action UK, 2014).*

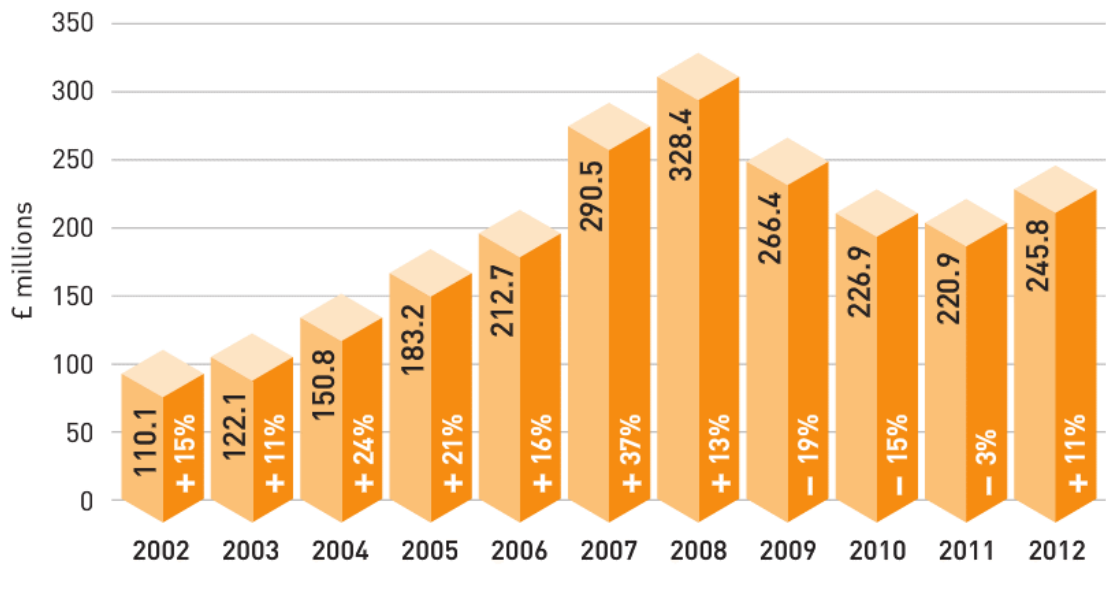


Figure 15: Card-not-present fraud losses on UK-issued cards 2002-2012

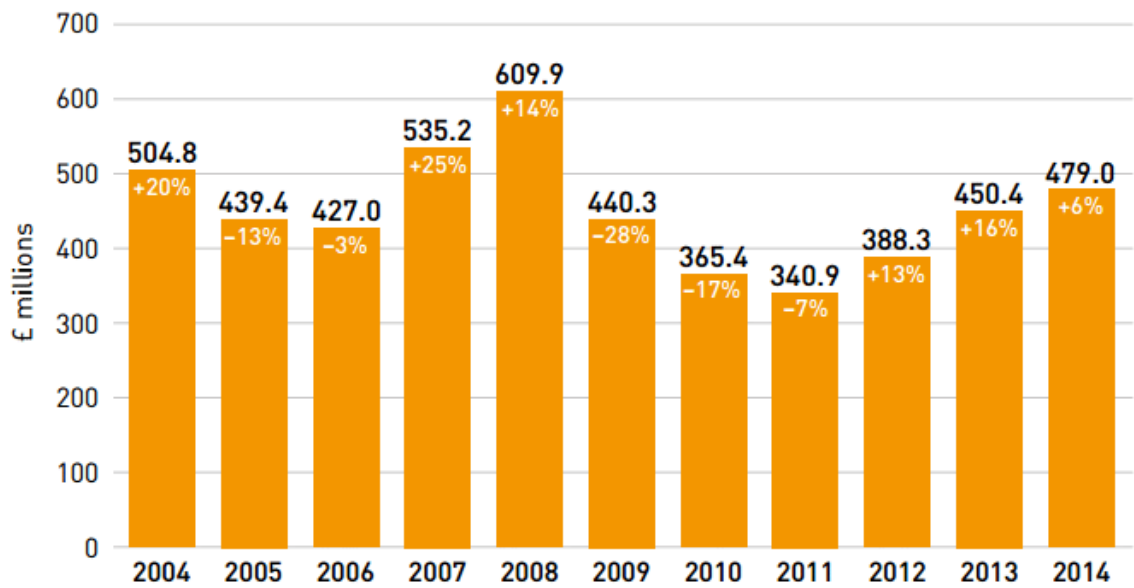


Figure 16: Card-not-present fraud losses on UK-issued cards 2004 - 2014

According to the Financial Fraud Action UK (2009) Card-not-present fraud losses have been on annual increase for 13 years non-stop, Hence, from approximately £4.6 million in 1995 to a staggering £328.4 million in 2008, and it is responsible for about 65% of all types of card frauds in United Kingdom, but these losses have to be understood in the perspective of a high level of growth in card-not-present spending over the past ten years, especially over the internet.

### **2.9.1 Card-not-present fraud level controversy**

It is been claimed over the past five years that card-not-present fraud dropped for successive years in the United Kingdom between 2009 and 2011, and the UK Card Association claimed that the reasons behind what is perceived to be a continuous decrease includes, the increasing use of sophisticated fraud screening detection tools by retailers and banks, as well as the growth in the use of American Express SafeKey, MasterCard SecureCode, and Verified by Visa, by both online retailers and cardholders (Financial Fraud Action UK, 2009)

In another review the Australian Payments Clearing Association (2013) also confirmed that card-not-present fraud losses dropped by 8% in 2012 following the increase in the use of the 3D Secure solutions provided by the card association.

In United Kingdom, in 2009 probably opened the door for good news as card-not-present transaction fraud losses experienced its first reduction in 13 years with a 19% fall from 2008, while the year 2010 and 2011 further recorded a 15% and 03% fall respectively, however, the percentage of these reductions reflected a diminishing result compared to the level of reduction in 2010, but this was overlooked, surprisingly, card-not-present returned back again with an 11% increase in 2012 from 2011 (Financial Fraud Action UK, 2013).

Today, “Fraud the Fact” report published by Financial Fraud Action UK (2014) shows that; the annual incremental losses from card-not-present fraud in the United Kingdom has recorded what is seen as the third consecutive year of increase.



Even though it was reported that the increase in the use of the 3D secure influenced the level of card-not-present fraud reduction, it should also be recognised that the 3D Secure solution has been around for the past 10 years, and while it has been in use since then, it failed to sufficiently reduce the card-not-present fraud. Adding that criminals exploited the static data vulnerabilities in 3D Secure which made it virtually impossible to shield from threat of phishing attack.

On the other hand, according to a survey (Network Security, 2000) by a UK credit rating agency – Experian, it is believed that only 57% of businesses reports occurrences of credit card fraud, meaning that 43% of credit card fraud occurrences are not reported or taken into account.

Nonetheless, in a recent review of E-finance & payments, Law & Policy (2012), the incidence of card-not-present fraud losses have fallen in the past few years, but this might be misleading, despite the fact that the statistics might be seen as encouraging and a fact to claim that card-not-present fraud solution has been finally achieved.

However, what appears as a problem solved is simply a camouflaged weakness, and the less reassuring reality of card-not-present solutions, because numerous indirect factors that affected the trend of card-not-present transaction in the recent years following technology advancement were not recognised in the report.

Despite other factors that may have caused the reduction of the card-not-present fraud in United Kingdom, the recent 11% increase in card-not-present fraud in 2012 confirms that the review of E-finance & payments, Law & Policy (2012) might be accurate and a remarkable warning to merchants selling online about an unresolved problems of card-not-present fraud.

### **2.9.2 Undisclosed factors behind the drop in card-not-present fraud losses**

This research analysed the undisclosed key contributors to the recent reduction in card-not-present fraud in the following classes.

### **2.9.2.1 Aggressive measures of handling card-not-present transactions**

Card issuers and financial institutions have been taking drastic and radicalized measures in the verification and declining of transactions, especially transactions happening outside the United Kingdom and this results in only 10% of declined transactions being actually fraudulent. Obviously this stultified strategy to card-not-present fraud reduction may indeed reduce fraud and impact on the statistics of fraud losses, but it is also causing great dissatisfaction to cardholders, affecting the interest in electronic commerce card payment, loss of revenue to participants, and cost the card issuers in administrative resources (E-finance & payments, Law & Policy, 2012).

### **2.9.2.2 Introduction of Alternative Payments**

For decades payment card has been the primary and dominant method of online payment. The benefit of making payment without carrying cash and accepting payment instantly and remotely from anywhere in the world without the need for a face to face interaction contributed to its success. However, in recent years, merchants and customers are shifting to alternative payment methods. The primary reason for this movement are security concerns with online card-not-present payment, access to merchant account services which enables merchants to accept card payment transactions, and high fees or charges.

In research about securing online credit card payment (Hwang, et al., 2003), approximately 60% of adults in United States of America do not usually transact on the web because of privacy and security reasons, even though it is claimed that 93% of payment is done through credit card. However, the Information Technology Association in their own findings confirmed that 74% of United States residents believe that their personal information could be stolen when used online during card payment.

And the same conception is perceived by 50% of European internet users who would not want to use their card and personal details online for fear of the unknown (Philippsohn & Thomas, 2003).

Alternative payment methods such as Paymenex, ACH, xWallet, PayPal and Skrill have taken precautions from the concern of consumers in online card payment and

implemented a different concept of alternative payment method that protects personal information, while many alternative payment methods use credit or debit cards as funding source, but the card and personal information are provided once during initial setup and verification. Once verified, the customer can continue to make payments online without entering his personal or card details in subsequent online payment, other alternative payments are totally introducing a “*no credit or debit card payment*” alternative, but funding to the payment account is through cash payment at agent locations or through a cash payment networks.

There are several reasons for the introduction of alternative payment methods and the phenomenon varies and depends on political, economic, social and ethnic backgrounds, some of the common reasons are as follows:

### **Security and identity theft**

Most card payment methods still rely on collecting sensitive personal and card information online. The level of personal information that payment processors or gateways collects varies, sometime, date of birth and bank account information are requested in a bid to strengthen the authentication. However, most customers are reluctant to give away their card and personal information online for fear of fraud and identity theft. Therefore, prefer to pay with alternative method where personal and sensitive information will not be revealed during online payment. Oddly, Paymenex Panama LLC (2013) reassuring its customers of online payment with Paymenex card stressed that “*Customers do not need to enter the names of their ancestors to pay online*”.

For the past few years the process of not asking customers to enter their personal details online has been seen as a competitive advantage for payment service providers who do not always ask customers to enter their personal information and at the same time have their own strategic framework to authenticate customers online.

### **Card-not-present fraud losses and chargeback risk**

The merchants are becoming weary of online fraud since most accounted online card fraud are pushed to them, hence, merchant seek low-risk and secure alternative to accept payment online.

### **Bespoke payment methods**

Merchants prefer to have as many methods of payment as possible to be able to reach out to more customers and increase their sales, especially those who cannot get their own debit or credit card can choose to pay with alternative payment methods, this is a common trend for merchants selling internationally who usually seek to provide payment method that is local and accessible to all classes of customers, irrespective of the geographical locations.

### **Access to Merchant Account**

Many merchants cannot be able to open their own merchant accounts to enable them accept card payment. This problem is usually affected by bad credit reports, geographical location, or the selling of prohibited products.

So merchants in this situation seek for alternative methods to accept payment.

### **No Credit and Debit Card Solution**

Problems of credit cards are enormous, these includes: chargebacks, fraudulent transactions, no guarantee of processed payment, high processing fee, merchant account fee, deferred settlement of processed payment. Therefore payment service providers try to implement alternative payment methods that will reduce the listed problems as much as possible to give them a competitive edge.

### **Source of Revenue**

Processing payment and helping online sellers to accept payment electronically is a business model with many revenue channels, businesses can start their own business operations as a payment service provider with prime objectives to process or facilitate electronic payments and impose processing, refund, setup fees or gain from providing foreign exchange if providing services in multi-currency.

### **Flexible payment option for customers**

Adding several alternative payment methods to an online shopping cart system offers the customers the opportunity to choose from a variety of payment alternatives instead of forcing customers to stick to card payment. Basically, a company is providing alternative payment services if they allow customers to pay and be paid through computer systems,

and within recent years the number of alternative payment service providers has increased significantly with different processes and concepts of processing payment. Some of the alternative payment providers are shown on the following table.

Paymenex	Ukash
Skrill	MTN Money
Airtel Money	PayPal
Sofort	iDeal
Sporopay	WebMoney
Giropay	BPay
xWallet	CashU
Alertpay	Direct Debit
Astropay	ELV
Bitcoin	Zong
Mi-Pay	Text2Pay
TigoCash	PayForIt

*Table 9: Alternative Payment Providers*

## **2.10 Causes of card-not-present fraud**

This research classifies the causes of card-not-present fraud into three main categories that are inspired by a range of motivating factors.

### **2.10.1 Identity Theft**

Identity theft has received many definitions from different people and in different context, but most can be streamlined to two words: “stealing” and “impersonation”.

According to Matejkovic & Lahey (2001) identity theft is defined “as the obtaining and use of another individual’s personal identifying information such as names, date of birth, social security numbers, card and account information to obtain access to that individual’s account or credit, or to establish new accounts or credit in the victim’s name without his involvement or knowledge, and the use of those accounts and/or credit to obtain goods and/or services”. In another context, Gonzales & Majoras (2007) argued that, “Identity theft is the misuse of another individual’s personal information to commit fraud”.

Archer, et al., (2012) defined identity theft as “the unauthorized collection, possession, transfer, replication, or other manipulation of another person’s personal information”.

Identity theft also means stealing with intent to impersonate and commit fraud without victim’s consent or knowledge.

Eisenstein (2008) said that the perception of identity theft is new and many researchers have called for more research on the topic, however, the research of Hoffman & McGinley (2010) and Kaminsky (2000) confirmed that the history of identity theft can be traced back in sixth century BC to the biblical story of twin brothers named Jacob and Esau born to the family of Isaac and Rebecca, but the news that Jacob was to inherit Isaac’s wealth motivated Rebecca to take advantage of Isaac’s bad eyes sight by devising a strategy and presenting Esau to impersonate Jacob with hairy look purposely to mislead Isaac into believing that Esau is Jacob and giving away his inheritance to Esau. The parallel with the how the development of the internet technology has made identity theft to extend its capabilities electronically is clear.

Identity theft practices can occur in many contexts, either identity theft by visual and physical object representation or digital and electronic information representations. Visual and physical objective representation is where people can present themselves or object in place of others or other objects, for instance in the biblical story above, Esau presented himself to Isaac claiming to be Jacob because Isaac’s bad sight cannot allow

him to visually differentiate between Jacob and Esau. This type of identity theft carries the highest risk because the impersonator must be present at the scene for a face-to-face interaction that exposes the impersonator to physical risk if caught in the act. While the digital and electronic information representations involve the use of electronic data to impersonate others and require no physical or face-to-face interaction. This type of identity theft carries low or no risk because the impersonator can operate remotely from an unknown location out of the scene, and this benefit has fuelled and diverted criminals to this concept of identity theft thus making identity theft a household name in every digital economy.

This research believes that the background of identity theft discussed by Eisenstein (2008) hovered around identity theft by digital and electronic information representation which is now the background concept of card-not-present fraud including most impersonations carried out online or through electronic systems.

This research classifies the motivation of identity theft into three main categories:

**Reproducing Identity:** This category of identity theft can aim at taking advantage of a good attribute of another by reproducing or mimicking the same attribute. For instance, in a recent news the UK Border Agency (2013) announced that a Nigerian woman without the right permission to live in the United Kingdom had impersonated the identity of a Dutch woman in an attempt to fraudulently obtain the right to live in the UK and gain employment as a support worker at a UK Care Home. The aim is to deceive the employer into believing that she is a Dutch woman with same rights as every other European Union citizen, instead of her original identity as a Nigerian woman. Motivation of this impersonation can be attributed to obtaining necessary immigration permissions and financial interest.

**Financial and Resources Gain:** This type of identity theft targets financial instruments like card details which are commonly used to commit card-not-present fraud by placing illegitimate orders with online merchants. This type of criminal activity is the most commonly known motivating factor for identity theft and the activity that has contributed to widespread identity theft.

**Crime:** It should also be noted that not all identity theft are intended for financial or resource gain, some identity theft can aim at masquerading the legitimate identity to commit crime. For instance, Mr. Jones presenting himself as Mr. Philips to commit murder, the motivation can be to label Mr. Philips as a murderer or to evade the responsibility of murder.

In a recent research Anderson, et al. (2008) argued that identity theft received radical advancement following the recent trend of electronic payment. Buyers and sellers depend on data linked electronically to a financial account to buy or sell goods and services without seeing each other physically. Therefore, fraudsters adopt many methods to capture these data from their victims that they will use fraudulently to imitate the link.

Identity theft has developed into a household brand with many domains, such as identity theft techniques, identity theft technologies and identity theft fraud. This development stimulated in the discovery and phenomenon of information technology that relies greatly on digital information to accomplish major tasks and its existence has transformed information security into a key requirement in computer science.

Using names and card numbers keyed in with computer input devices is now one of the solutions for credible online card payment identification, because every competent person in such an area with same information can do same as the bearer.

Online card-not-present payment depends on data submitted online irrespective of the physical appearance of what represents the data, and an e-commerce transaction can be completed entirely online this way as opposed to by card present payment which requires the physical card, PIN and or signature of the cardholder exchanged in a face-to-face environment, and the development of identity theft is driven by this vulnerability.

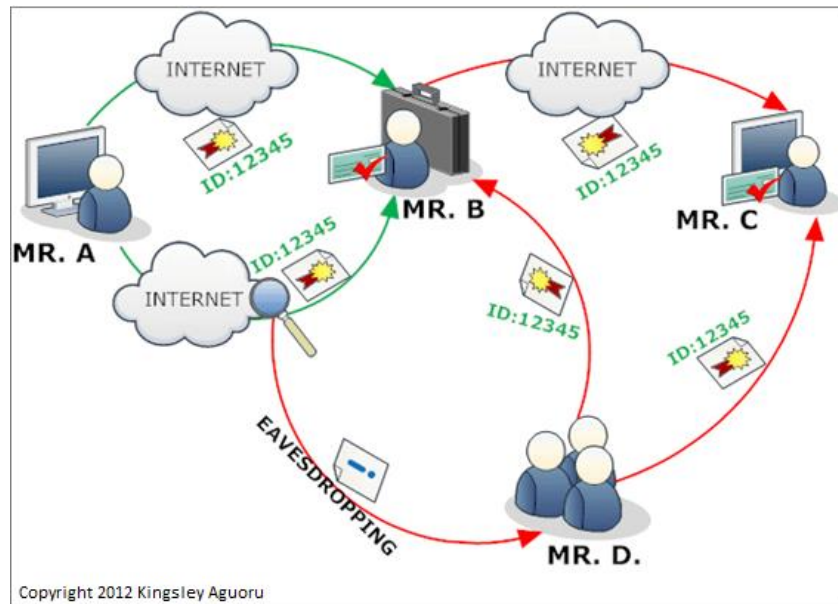
In today's evolving digital world, causes of card-not-present fraud continue to increase with the trend and complexity of technology and the learning development of users.

Fraudsters stole card details of others to commit card-not-present fraud, therefore, there will be virtually no card-not-present fraud without an associated identity theft process, as internet fraud is growing in complexity and in the level of occurrences, identity theft as a major facilitator is expanding in responsiveness.



In a recent research, Bohn & Mason (2010) has shown that naming conventions are social artefacts suited for the social events, nevertheless, names usually are no longer effective to distinguish their bearers among a large community or public because many people will respond to the shout of the word “Dad” or common names like “John” or “Smith” in public places. At the same time, the adoption of using unique numbers on credit card numbers to identify its bearers in online card payment at first makes it meticulously unique, but as technology develops, the argument shows that, if knowing card numbers is to be evidence that puts any person that knows it as the bearer, then, there must be a dynamic method or different secret numbers for every other person to whom one’s identity is to be proven at any point in time, because the person to whom one’s identity or credit card number is proven to, will know the card number at same point in time which automatically makes him also the bearer of the same card number.

Card details entered on the internet for payment travels through different computer nodes from the originating computer or device to the destination server making it vulnerable to interception or theft, hence the more a card’s details is used to pay online the more it loses its credibility . Many organisation's strategy of information security management is very poor and vulnerable, not only in compliance with the security technology trend and policy, but in some cases dubious employees pose a great deal of concern in identity theft within the organisation, giving rise to high risk of unacceptable information compromise. However, salvaging this situation on the card-not-present environment, the cardholder needs a different secret number each time he is required to identify himself to the merchant because using the card information over and over again to pay online reduces the reliability and trust of the card and this forms a major part of the identity theft and fraud resulting from online card payment.



*Figure 17: Flaws in remote Identification with static numbers*

If **Mr. A** is attached to the identity No: 12345 which identify him remotely to **Mr. B** (i.e. merchant), Then **Mr. B** will know the identity No: 12345 to verify that it is actually **Mr. A** at the point of verification and this automatically put **Mr. B** as the second bearer of the same Identity No: 12345. And if **Mr. B** so wishes, he can use the identity No: 12345 to identify himself to **Mr. C** that he is **Mr. A** which will also position **Mr. C** as the third bearer and it can loop infinitely thereby multiplying the bearers of one identity.

And if **Mr. D** (i.e. a fraudster) intercepted the communication or is listening to **Mr. A** when he was verifying himself to **Mr. B**, then, **Mr. D** will know the identity No: 12345, and can use it in another sequence to identify himself as **Mr. A** to **Mr. B** and **Mr. C**.

In the above illustration, the legitimate identity bearer – **Mr. A**, made only two identification actions to **Mr. B** on two occasions shown with the green arrows, but three additional identification actions were made shown in red arrows, one identification action by **Mr. B** who supposed to be a trusted party in the process and, two by **Mr. D**, who is a thief. **Mr. B** and **Mr. D** succeeded with their identification attempts to their other parties to impersonate **Mr. A** commonly because the identification number is static and valid for subsequent uses to give chances to **Mr. B** and **Mr. D**.

The identity No 12345 used in an online environment is in no way a true likeness of the bearer, rather it is an artificial identity to represent the bearer on the computer system, and as with every other data that can be replicated endlessly, the same identity can be replicated to act as an online identity for a million people as long as they are in possession of the said identity number.

**Mr. A** could have been salvaged supposing the identity No. 12345 was invalidated immediately after he completed the first successful identification to **Mr. B** and replaced with a new identity No. 67890. In such a case, **Mr. B** and **Mr. D** would have not succeeded in their impersonation attempts because they will still be presenting the Identity No. 12345 which has been cancelled.

Identity theft can be accomplished by the application of different forms of stealing, whether carried out electronically or manually. Any method deployed to steal the identity of another with intent to impersonate automatically becomes a method of identity theft. As it is widely accepted that technology is a double-edged sword, it has greatly facilitated most of the methods of identity theft used nowadays.

### 2.10.1.1 Methods of identity theft and infiltration techniques

The identity theft types can be classified into two bases, (1) Physical-Low Tech Base theft – the thefts that requires physical confrontations, and (2) Technology-High Tech Base – the thefts that are done through the use of computer systems.

NO	PHYSICAL LOW-TECH	TECHNOLOGY HIGH-TECH
1	Dumpster Diving	Phishing
2	Shoulder Surfing	Hacking
3	Mail Theft	Spyware & Trojan
4	Skimming	Pharming
5	Buying Stolen Data	Telephone Scam

6	Lost and Found	Eavesdropping
7		Bogus E-Commerce Shop

*Table 10: Bases classification of identity theft methods*

### **Phishing**

Phishing is a form of technical manipulation and spoofing or social engineering that impersonates identity of others to trick users into divulging sensitive information such as account and credit card numbers in response to a communication request, commonly by email and web link. It is a sort of Internet attack that imitates a legitimate website for the purpose of obtaining confidential information of others (Abdelhamid, et al., 2014).

Identity theft is perceived by criminals and thieves as an extension of the old idea of exploitation. In phishing attacks criminals masquerade with the identity of others to fool others into spontaneously releasing their sensitive information (Kruegel & Kirida, 2006).

Phishing attacks are seen as epidemic to internet users and criminals continue to use several phishing technologies to trick users into giving out their sensitive information (Hamid & Abawajy, 2014).

The long existing method of phishing is the spam email and web link, but as technology advances, more new sophisticated methods of phishing are discovered, for instance the server-exploit phishing attack.

#### **Email and Web-link Phishing**

This is the most common type of phishing, originated from email communication which directs the victim to a web link where the fraudsters collect the user's sensitive information.

In this scenario, the victim will receive a spoofed email purporting to be from a legitimate or trusted entity, for example, the bank or credit card company, asking the user to click on a web-linked embedded in the email to verify his account information. However, the

web-link will redirect the victim to a constructed form which looks exactly the same as the legitimate entity.

Victims who actually have arrangements with the impersonated entity are usually trapped because they believe that they are dealing with the legitimate entity.

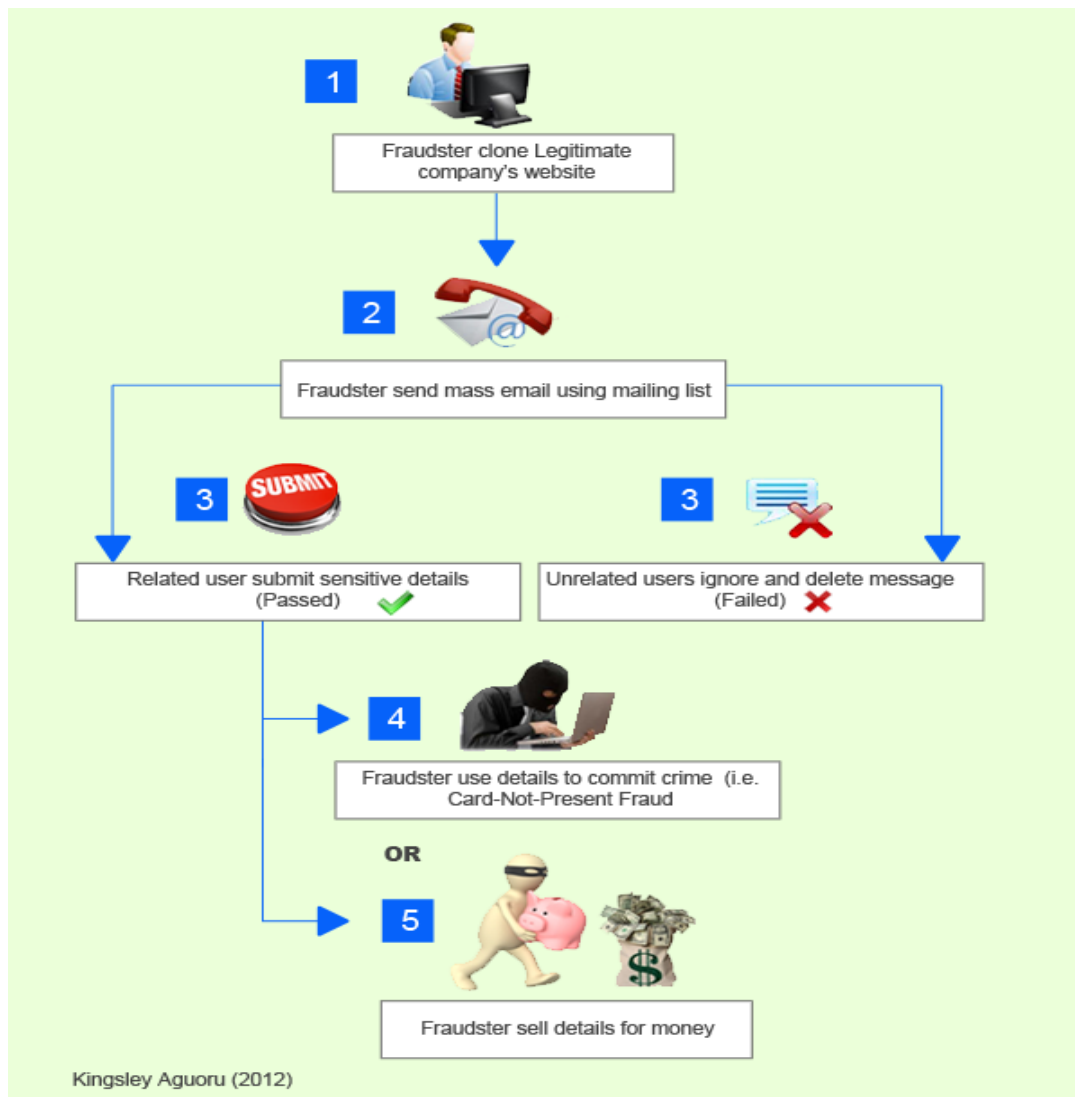


Figure 18: Email or web-link Phishing flowchart



Dear SunTrust Bank client,

The SunTrust Bank Technical Department is performing a scheduled software upgrade to improve the quality of the banking services. By clicking on the link below you will begin the procedure of the user details confirmation.

<http://www.suntrust.com/ibswebsuntrust.cmserver.welcome/confirm.cfm>

These instructions are to be sent to and followed by all SunTrust Bank clients. We apologize for any inconvenience and thank you for cooperation.

SunTrust Bank Technical Service

© SunTrust Banks, Inc. All rights reserved. - Equal Housing Lender - Member FDIC

Figure 19: Email screenshot Received in 2008 by Kingsley Aguoru

The screenshot shows the SunTrust FIA Card Services website. At the top right, it says "FIA CARD SERVICES". Below this is a "SECURE LOGIN" section with a lock icon. It contains a "Login Name:" field, a "Password:" field, and a "GO" button. Below the password field is a link: "Forget Your Login Name or Password?". To the right of the login form is a "NETACCESS Online Account Servicing" section. It contains the text: "Enrolling your account is just a few clicks away. Get up-to-the-minute account activity, make payments, view and download statements, and complete address changes and other requests via our Account Services page. [Learn More](#)." Below this is a "Register Now!" button. Further down is a security notice: "Your information is protected by 128-bit SSL encryption. [Security Statement](#) | [Security Tips](#)". Below the security notice is a "Secure Account Servicing" section with the text: "You can use our secure e-forms to maintain your account without ever picking up the phone. After you login, simply click the Account Services tab to view a complete list of secured online requests." At the bottom of the page, there are links for "Contact Us", "Privacy", "Security Statement", and "Terms of Use", followed by the copyright notice: "© 1999-2006 FIA Card Services, N.A."

Figure 20: Web-Link Redirection Page

## **Server-Exploitation Phishing**

Server exploitation is gaining unauthorized access to a server belonging to other entities and using it to host malicious software to gather sensitive information, disrupt services or commit crime. Cresson Wood (2003) said that the password is the first line of defence that can prevent abuse of access to computer systems, while Vu, et al (2007) confirmed that username and password offers lesser security than other authentication systems such as biometric systems.

Fraudsters deploy many techniques to capture or reset server access information to enable them gain access to the server.

## **Criminal Hackers and Crackers**

Hacking is a very broad domain and a practice that takes a lot of time to learn. It has several categories of individual concentration, the common categories of hackers include: Security experts, Criminal hackers, Script kiddies, Ideological hackers, corporate spies and many more. However, among these categories, criminal hackers hack commonly because they want to perpetrate theft or cause damage, they include those criminals that hacks into the computer systems of several financial institutions and payment processors to steal card and personal information (Strebe, 2002).

According to Computer Fraud & Security (1999), the criminal hackers can also be known as the crackers because they use sophisticated technologies to crack passwords and break into systems.

Motivation of criminal hackers' activities can include curiosity, vandalism, extortion, fraud and many more.

## **Spyware and Trojan**

According to recent research (Abraham & Chengalur-Smith, 2010) spyware and Trojan horses are malicious software that targets user's computer with the intention to collect confidential information on the user's computer without his knowledge. It gives hackers access to computer systems and enables them to carry out range of activities in the infected computer which includes: stealing of sensitive information, modification,

deletion, and repossession of computer files, An example of malicious software is the key logger application which resides unnoticeable in personal computers and logs all key strokes made by the computer user and then transmits collected information to the fraudsters. Some key loggers also take screen shots to give the fraudster a view of user's activities. Most spyware and Trojans are distributed remotely using several deceptive and hidden methods: for instance, a misleading email attachment or download link. In most cases it can be installed, and accessed remotely without the knowledge of the computer user through the steps provided in Fig. 22 (Erbschloe, 2004).

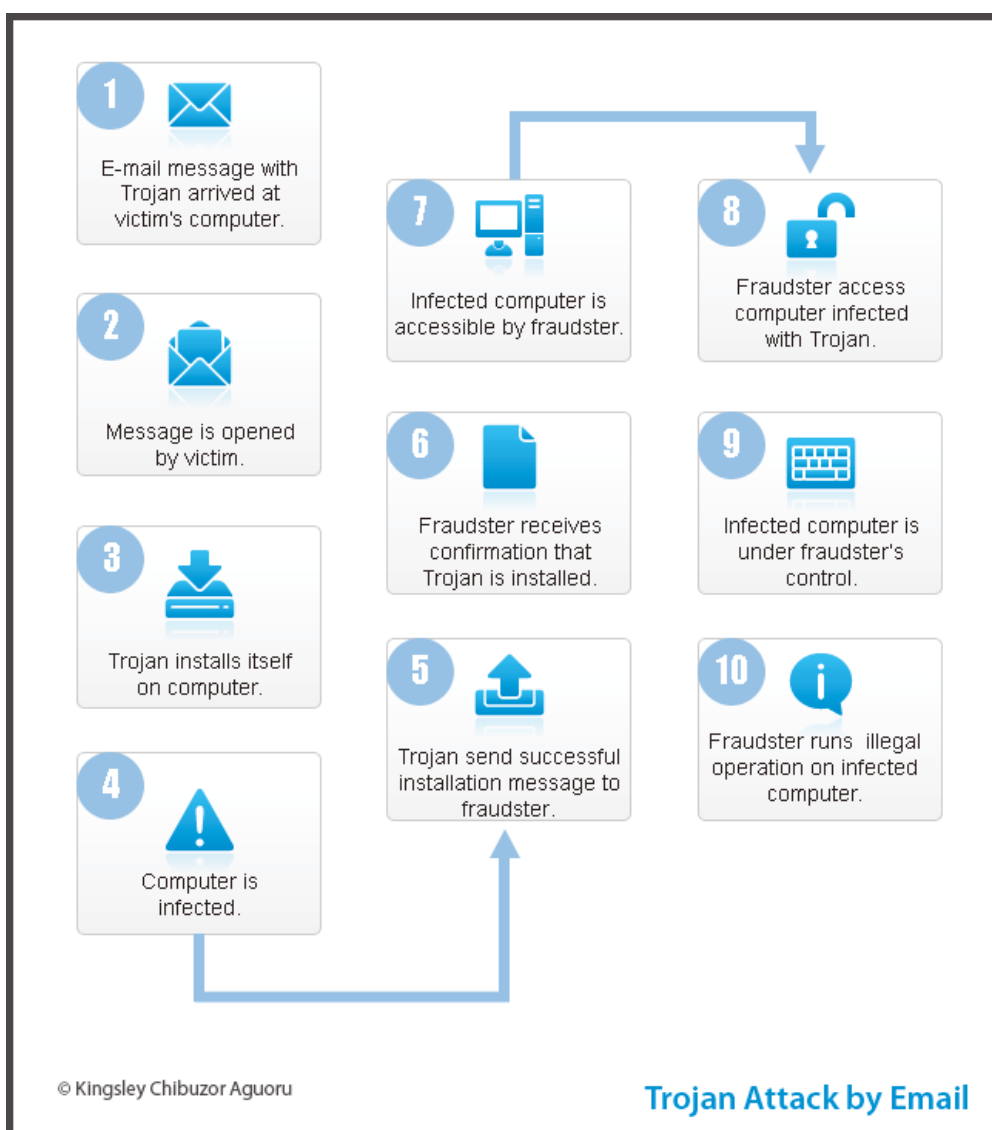


Figure 21: A flowchart of a Trojan attack by Email



## **Pharming**

Pharming and Phishing share some characteristics, but they are still two different types of identity theft. The Pharming method is more complex; it involves the modification of files stored in users' computers, including website addresses and internet protocols (IP), with the intent to redirect them to a different website where information will be collected, or where the user is deceived with the presentation of wrong information or notices. It is also called domain spoofing (Rodriguez, 2009; Biegelman, 2009).

This is one of the vulnerabilities of 3D secure, because when a 3D secure authentication is invoked and the user is redirected to another site, they often suspect pharming attack and in some cases will stop payment.

## **Telephone Scam**

Not all cold calls actually intend to do business with your organisation, or offer you a consumer service. Some are intended to obtain your confidential information, such as card details, by offering you some cheap services and asking you to guarantee it with your Debit Card. For instance, by promising to reduce your cost on gas, insurance or electricity supply by some percentage, they will inform you that your card will not be charged now to increase your confidence.

## **Eavesdropping**

The Oxford English Dictionary defines eavesdrop as “*secretly listen to a conversation*”, and in the context of identity theft, criminals physically or remotely listen to users' conversations on the telephone or internet - for instance, while making a card payment over the telephone in a public place, or on the web by sniffing through the network and intercepting the communication in transit.

## **Dumpster Diving or Bin Raiding**

Some methods of identity theft are self-created, some fraudsters are interested in searching through the bin at residential homes or offices for useful personal information.

In recent research (Zhang & Li, 2005) fraudsters targets customers' bins for credit card information with the intent to commit crime because many residents do not use paper shredders at home or take sufficient further steps to make sure they destroyed all unwanted banking or financial documents beyond recognition.

Bank account and credit card statements contains full name, address, account numbers and balances of the account holder and when disposed into the bin without adequately destroying the ability to recognise the information, it automatically poses a threat to self-caused identity theft and becomes a handy tool for the fraudsters to commit identity theft.

As Biegelman (2009) said, "Enterprising criminals were more than willing to "get down and dirty" in the trash looking for and often finding valuable information"

### **Shoulder Surfing**

"Who is watching you from behind?" it has been a known advice from financial institutions to their customers, to cover the visibility of their transaction on the Automatic Teller Machines (ATM) while they input their PIN to authenticate themselves, or while entering their card details on the internet in a public place. According to (Huston, 2009), shoulder surfing is a method of identity theft that is concerned with the direct observation of one's activities, with the intent to copy confidential information.

The value added feature of smartphone camera introduced within the recent years has been seen as beneficial and a handy tool to capture information and events without much preparation, on the other hand, it has served as a handy tool to shoulder surfers to take snap shots or record sensitive information from their victim activities.

### **Mail Theft or Redirection**

This type of identity theft aims to steal letters from postal delivery box by fraudulently applying for post office mail redirection service using the identity of others. The aim is to redirect and then read mails of their intended victim in search of sensitive information for fraudulent activities. Residents who are moving homes are the most vulnerable to this type of identity theft.

## **Skimming and Scanning**

The Australian Competition & Consumer Commission (2013) said that “Card skimming is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam”.

Criminals use pocket-sized skimming devices to record card information of their victims. The information stolen in this way is used to produce fake credit cards for fraudulent activities (Biegelman, 2009).

## **Lost and Found**

Just because many criminals have turned to technology to steal personal information and sensitive data does not mean that the old style has vanished. Some low-tech fraudsters still rely on pickpocketing and physical theft to steal personal information especially information contained in mobile devices, laptops, wallets and diaries. Misplaced personal information can also be found by a criminal: lost and found card and bank account information has been a self-caused easy access to identity theft (Biegelman, 2009).

## **Buying Stolen Data**

Some criminal hackers concentrate on finding ways to hack into the system of financial institutions or payment services providers in search of active credit card numbers to steal. Their intentions include obtaining card information and selling them to other criminals who will carry out the actual fraudulent transactions. For example, in the United States, vulnerabilities in CardSystem Inc. caused a hacker to access over forty million credit card information (Computer Fraud & Security, 2005, p. 1).

## **Bogus E-Commerce Shop**

Just as the cardholders are unwilling to provide their card information to an online merchant for payment because they believed their card information might be stolen by the merchant, some bogus merchants can offer their products at very low prices to attract online shoppers to their website to place orders; however, once the order is placed and card information received, the bogus merchant will notify the online shopper that the item

ordered is no longer in stock meanwhile the customer's card information has been received and ready to be used fraudulently.

### 2.10.2 Growth of Internet Users

Aside from the causes attributed to identity theft and the vulnerabilities or flaws that exist in the card-not-present payment process, the number of card holders shopping online has seen rapid growth in parallel with the evolution of e-commerce technologies.

According to the Office for National Statistics (2010), household internet access in the United Kingdom developed rapidly and accounted for 73% of UK households in 2010. 75% of users' activities on the internet are finding information about goods and services.

Year	Per cent	No of Households (millions)	Percentage change on previous year
2006	57	14.3	-
2007	61	15.2	7
2008	65	16.5	8
2009	70	18.3	11
2010	73	19.2	5
2011	77	--	8
2012	80		3
2013	83		3

*Table 11: UK household internet access 2006 to 2010 (Office for National Statistics, 2010)*

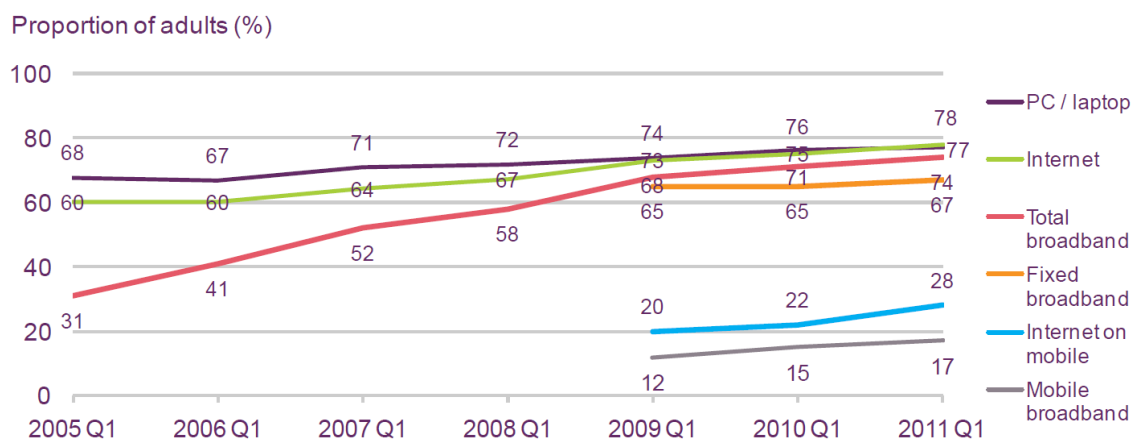


Figure 22: UK Household internet access 2006 to 2010 (Ofcom, 2011)

As more business operations continue to shift to the internet for various operational reasons, the value of online card payment and associated fraud losses continue to soar thereby increasing the vulnerability of e-commerce participants and the exploitation of identity theft technologies in a bid to steal card information. According to (APACS, 2010), there has been a tremendous growth of card-not-present spending by consumers in recent years as a result of the evolution of e-commerce and growth of internet users in United Kingdom.

### 2.10.3 Exploitation of Trust among parties

The anonymity of the internet has affected the level of trust that exists among the e-commerce parties because there is an absence of physical contact. In recent research (Palvia, 2009), the background of a long-term business relationship in online business transactions is built around trust. The absence of trust is a high level warning that must not be ignored because trust is one of the important factors in establishing a reputable online relationship.

Internet technology has developed its features and capabilities as a major factor and key for the introduction and trend of e-commerce. However, this development could be adversely meaningless and a threat in some greater level if there is no acceptable level of trust among all entities involved in e-commerce. The existence of an ineffective trust

relationship is one of the factors that can cripple e-commerce development (Ahmad, 2008).

The problem of trust in e-commerce plits opinion. While some are finding ways to improve the trusts to boost e-commerce acceptability, a recent study (Xu, et al., 2008), has contradicted this belief and argued that trust is not on its own sufficient to enhance e-commerce acceptability, but suggest that parties look for a new method.

In a review of trust in an e-commerce context (Nieschwietz & Kaplan, 2003) state that, “trust refers to a consumer’s willingness (the trustor) to give Web sites (the trustee) personal and financial information in exchange for goods or services and promises to follow stated policies and procedures”.

#### **2.10.4 Flaws in card-not-present systems and solutions**

As with the popular belief that no technology is 100% secure, the little insecurity of such technology could be thwarted and exploited by fraudsters for many reasons. In a recent report (Nirshan, 2000), the same systems that created good and new opportunities for e-commerce have also created new opportunities for online fraud.

Many technologies have been developed as solutions to secure online payment during e-commerce transaction. However, no technology has effectively prevented the fraud resulting from online card payment.

##### **2.10.4.1 The CVV and the AVS**

The Card Verification Values (CVV) and the Address Verification System (AVS) was developed by the card association to create an authentication process in online card payment as fraud threats heightened. The CVV aimed to verify the 3 or 4 digits on the reverse of the card, while the AVS is set to verify the numeric values of the billing address.

However, the CVV and the AVS verification did not raise merchants’ trust because both are as flawed as every other piece of static information used repeatedly online: they are vulnerable to all types of identity theft. As with the card number, the CVV and AVS do

not change frequently, and such changes mostly occur during moving home or card replacement. Without any of these, they remain the validation integer for the CVV and AVS until such a time the address or card change (Card Technology Today, 2002).

This research also found that the Address Verification System is not widely used in all card-not-present environments, so the added validation of this value will not be taken into account in card-not-present channels that failed to implement this additional verification parameter.

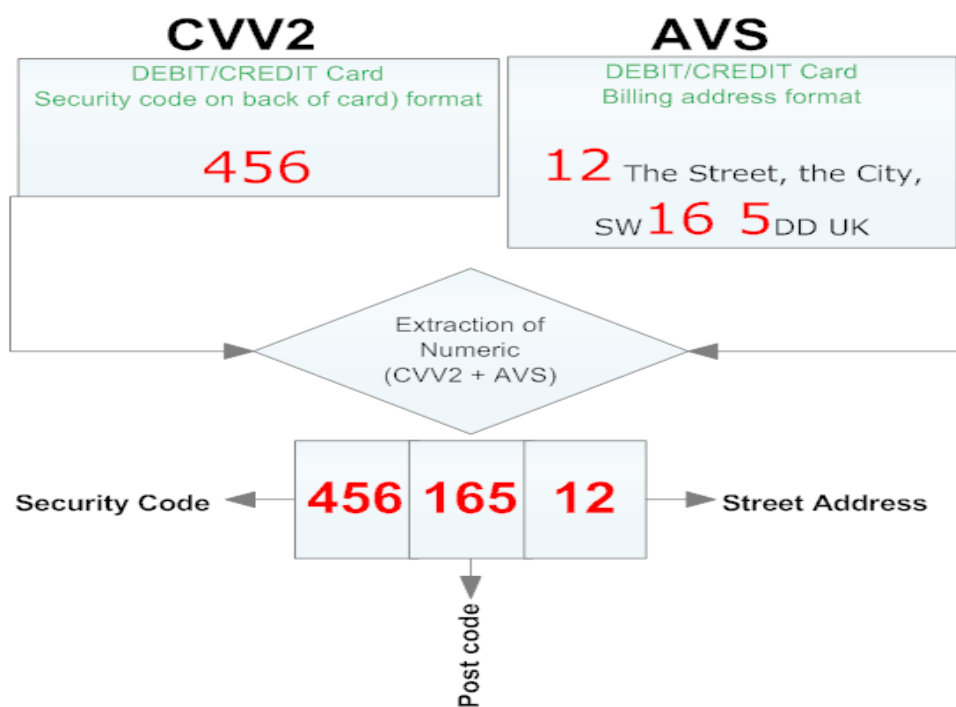


Figure 23: CVV and AVS Validation Flowchart (Aguoru, 2007)

The integer 456 165 12 represents the CVV and AVS of the cardholder and is used during card-not-present transactions as an additional feature to verify the cardholder. However, the static nature of the CVV and AVS place them in the same threat category as the card information. The CVV and AVS remain 45616512 until such a time the card is replaced or the cardholder's billing address changed: in the event of any identify theft incidence,

for instance, phishing, spyware, or hacking, the stolen information remain valid for the criminals to commit card-not-present fraud (Aguoru, 2007).

#### **2.10.4.2 Secure Electronic Transactions (SET)**

The Secure Electronic Transaction, popularly known as SET, is open encryption and security to protect credit card payment promoted by VISA and MasterCard designed to restore trust among e-commerce participants.

SET's main strength is the use of cryptographic protocols and dual signatures to assure confidentiality, maintain payment integrity and authenticate participants.

The six core participants of SET are:

The *Cardholder* buying on the internet.

The *Merchant* selling on the internet.

The *Acquirer* processing card transactions for merchants.

The *Payment Gateway* - an interim processor working on behalf of the merchant and the acquirer in processing transaction messages.

The *Issuer* who issued the card to cardholder.

The *Certification Authority* - which provides cryptographic certifications for the cardholder, merchant and payment gateway to assure that they participated in the transaction.

The Secure Electronic Transaction protocol addressed the following problems in card-not-present transaction.

**Integrity and Confidentiality of Information:** Secure Electronic Transactions assure the integrity of information across the network by ensuring that payment and order information is not altered. To maintain the trust of cardholders in card-not-present transactions it is important to ensure that the credit card information travelling over the network is protected and received by the intended recipient by the use of digital signature and certificate.



**Cardholder and Merchant Authentication:** buying and selling over a remote network without seeing each other reduces trust among the buyer and the seller. SET use certificate authority to reassure the cardholder that the merchant is authorised by the financial institution to accept credit card payment for orders, and on the other hand, the merchant is reassured that the cardholder is authorised to use the credit card account by the use of a digital signature and certificate.

According to (Kahate, 2003) and (Manzoor, 2008), assuming the three parties are in possession of digital signatures and certificates issued by the Certification Authority, a Secure Electronic Transaction would have the following sequence.

**Cardholder (Ordering Process):** The Cardholder's credit card details forms the Payment Information (*PI*) and the Order details form the Order Information (*OI*) and when hashed it will produce the Payment Information Message Digest (*PIMD*), and Order Information Message Digest (*OIMD*). Both are further hashed to produce the Payment and Order Information Message Digest (*POMD*). The Cardholder will finally encrypt the *POMD* with his private key to produce the Dual Signature (*DS*) and because the *POMD* contains the Payment Information and Order Information is now called Dual.

The Cardholder then delivers the Order Information (*OI*), Payment Information Message Digest (*PIMD*), and the Dual Signature (*DS*) to the Merchant and further delivers the Payment Information (*PI*), Order Information Message Digest (*OIMD*) and Dual Signature (*DS*) to the Payment Gateway.

**Merchant (Processing Order):** The processes described in the diagram shows that the merchant never receive the Payment Information (*PI*) and so the threat of dubious merchants stealing payment information (credit card details) is clearly eliminated.

The merchant computes his Order Information Message Digest (*OIMD*) and the Payment Information Message Digest (*PIMD*) sent by the cardholder to produce his own Payment and Order Message Digest (*POMD* (1)) and further decrypts the Dual Signature (*DS*) to produce the Payment and Order Message Digest (*POMD* (2)).

The merchant finally compares the POMD (1) and POMD (2) and if both match, the merchant approves the Order. However, if both do not match that is a warning that cardholder did not authorise the order and so merchant declines the order.

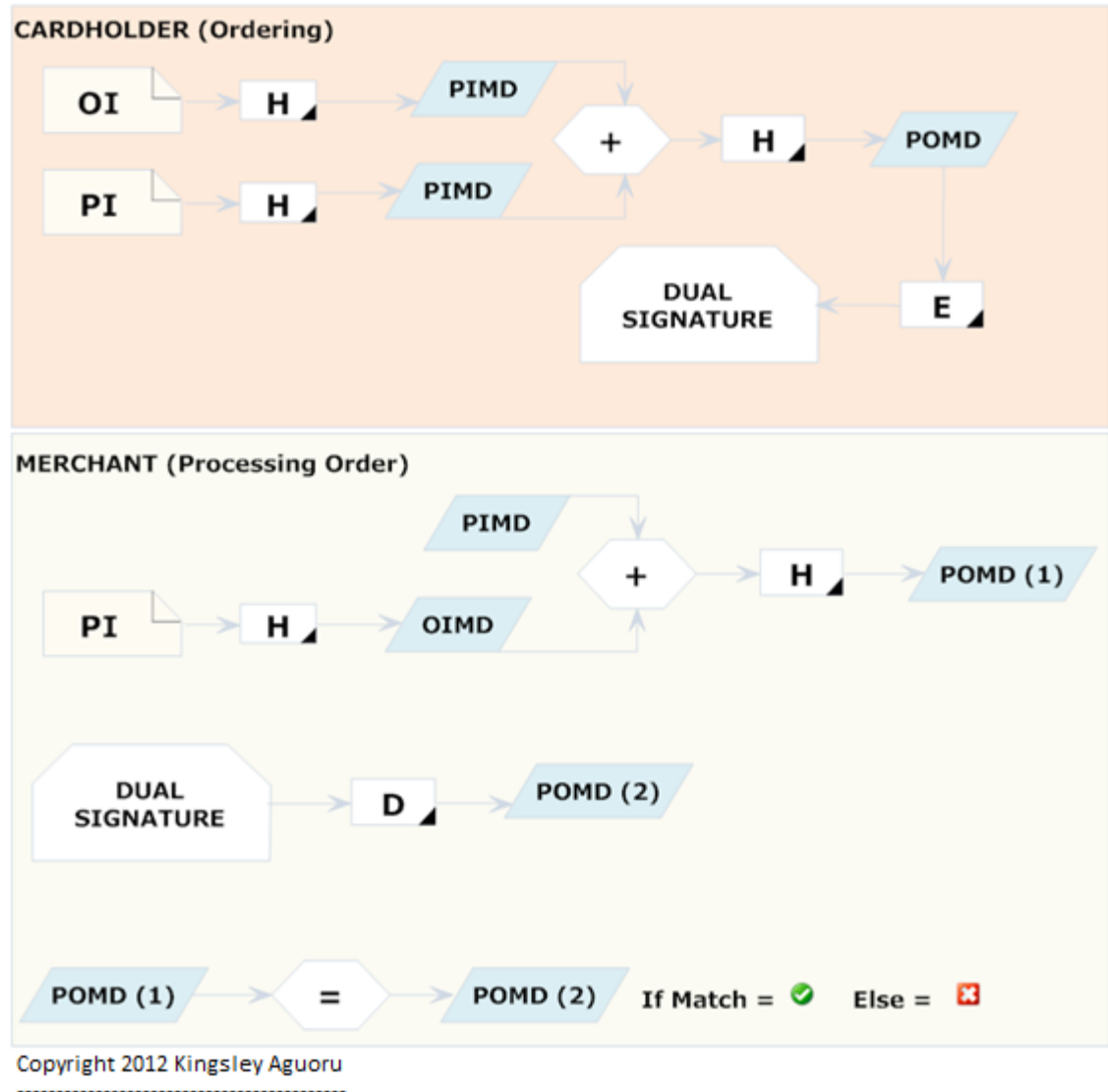


Figure 24: SET Ordering and processing flowchart

Despite the security strength promised and established by SET, it still has its weaknesses and vulnerabilities.

A recent study (Zhang & Li, 2005), has revealed that the exploitation of card fraud has been increased by the security weaknesses in card payment processing systems following

the monotonous use of exposed static card details in the authentication of cardholders. This is notwithstanding the introduction of the Secure Electronic Transaction (SET) protocol to swap card details during payment addresses. Regrettably, SET failed to be exceptionally satisfactory because of computational cost, message overhead and additional requirement of public key infrastructure (PKI). The studies of (Bella, et al., 2002) and (Herreweghen, 2000) further summarised some challenges faced by SET including; multiple nested encryption, duplicate message fields, sheer size. SET is secure to some extent and vulnerable to others because a successful transaction verified by SET does not give the SET gateway the legal guarantee that the cardholder authorized the transaction since ensuring non-repudiation in e-commerce transaction requires more than digital signatures.

#### **2.10.4.3 Secure Socket Layer (SSL)**


The Secure Socket Layer or SSL is a cryptographic protocol developed by Netscape Corporation to secure data in transit between two or more communication end points - for instance, client-side and server-side. While it has become more convenient to do business online, it has also become more difficult to ensure reliable and secure data exchange and communications.

#### **2.10.4.4 3D Secure**


The 3D Secure technology popularly known as Verified by Visa or MasterCard SecureCode was developed by Arcot Company for the card associations to protect cardholders during card-not-present transactions. It has received numerous accreditations and recommendations within recent years as one of the leading solutions for card-not-present transactions because the 3D secure solution uses the services of an intermediary in the process of authenticating the merchant and the cardholders.

During card-not-present transactions, the cardholder would be redirected to his issuer who will ask for a password to authenticate the cardholder. With 3D Secure, enrolment is required both by the merchant and the cardholder, the cardholder is required to create a

password after confirming his name, date of birth and card information (Card Technology Today, 2002).




**Step 1**




**Step 2**

Figure 25: Example 1 of 3D Secure enrolment



**Step 1**



**Step 2**

Figure 26: Example of 3D Secure enrolment

The two diagrams above illustrate the 3D Secure enrolment processes from two banks showing the actual information collected during 3D secure enrolment. It is clear that whoever has the card and personal information is able to enrol the card in the 3D secure program. Therefore, assuming that a criminal already has the personal information of the cardholder, and later received the card information before the legitimate cardholder enrolled his card in the 3D secure program, the criminal is able to enrol the card and choose his own password even before the legitimate cardholder does, this also confirms the fact that even though the 3D secure protects cardholders from card-not-present transaction fraud to an extent, it still has significant vulnerabilities which argues its ability to adequately solve the problem of card-not-present fraud.

According to Lomax (2006), Verified by Visa, MasterCard SecureCode and JSecure programs promise additional levels of authentication using the password provided during the card enrolment through an intermediary. However, it is vulnerable to identity theft as are all static passwords used on a remote network.

Also the circumstances surrounding the framework of 3D Secure often triggers confusion to cardholders because whenever 3D Secure system is invoked during card-not-present transactions, it will direct the customer to another website or call another web address that is different from the current web location of the customer, and it is virtually impossible for the customer to verify that the web address is actually a legitimate website for the 3D secure password verification. This is because it is similar to the concept of identity theft techniques used by criminals to harvest cardholders' information. Therefore in this process, many customers will stop and close the browser when this happens and this will mean the merchant losing the business, and if the customer continues, he might probably be redirected to a phishing website, hence recent research argued that the 3D secure solution escaped academic scrutiny (Murdoch & Anderson, 2010).

#### **2.10.4.5 Telephone Fraud Screening**

Research has shown that within the recent years, banks have adopted the use of aggressive measures to verify card-not-present transactions, this usually occur when a cardholder placed an order online, the bank would try to call the cardholder using the

telephone number held on file - in some cases it will be an automated call. This call is to verify that you made the payment, and this enables cardholders to confirm that they made payment with their card online or to decline having made any payment. Usually if the banks failed on several attempts to reach the cardholder on phone to verify the transaction, the card in question will be suspended and any future transactions will be automatically declined until the bank is able to speak to the cardholder. It is believed that even though this telephone screening methods helps to reduce card-not-present fraud, it also have significant issues which includes.

### **Cancellation of legitimate payments**

Nine out of every ten cross-border card-not-present transactions are cancelled because banks believe the transactions to be fraudulent. This is most common when a cardholder travelled outside his usual country of resident and used his card to make payment from abroad, banks would follow their normal fraud screening telephone call and because the cardholder is abroad, he may not be able to respond to the call or be aware in any way that his bank tried to contact him. The cardholder will usually notice that something is wrong when he tries to use his card again to make a payment or withdraw cash abroad and all attempts failed or are declined (E-finance & payments, Law & Policy, 2012).

### **Cardholder dissatisfaction**

Cardholders are often disturbed by the regular unscheduled telephone calls from banks trying to validate payments done online or getting their card blocked while they are abroad limiting their access to cash. Many cardholders get stranded abroad because their cards were used outside their normal country of residence and so their bank restricts access to their account through the card.

#### **2.10.4.6 Neural Network Credit card fraud detection**

The aim of neural network credit card fraud detection is to analyse transactional history of an account and provide a risk analysis report in a form of score which will enable decision making on a transaction The check includes a background check on and evaluation on spending pattern, previous history of reported fraudulent activities, location

of the order and comparing shipping address with the billing address, the major process of the neural network detection is gathering data and comparing the data with the existing pattern to identify variation, in some cases where the amount used fraudulently from the card falls within the existing spending pattern, or fraud that occurred within the location of the legitimate cardholder, this will affect the score and may not give an accurate report or correct decision (Ghosh & Reilly, 1994; Aguru, 2007; Patidar & Sharma, 2011).

## **2.11 Impact of card-not-present fraud on e-commerce development**

There is a belief that e-commerce contributes to the development of every economy that adopts it in its business operations. This belief is motivated, among other things, by the cost effectiveness in the implementation of e-commerce technologies that makes it easier for every organisation to start selling online without delay in a global marketplace as opposed by the brick and mortar type of business that has more investments cost requirements and reaches only an aspect of the marketplace. However, there are huge impediments that generate adverse impacts on the development of e-commerce: these key impediments can be categorised as physical, technological, and socio-economical (Molla & Licker, 2005).

According to Wales (2003) and Walton (2005), card-not-present fraud is an unresolved problem faced by e-commerce participants, but consumers, often cardholders are largely protected against any financial loss because there is no signed receipt by the cardholder to authorise transactions done through this method, and contrary to popular belief, it is not the card issuer that has to bear the burden either because the issuer is an intermediary party between the cardholder and the merchant and simply acts as the facilitator in transaction processes and arbitrator in the event of dispute, but the risk and responsibilities of fraud in e-commerce card-not-present transaction are mostly the burden of the merchant. The merchant bears the full risk and losses of dispute if the legitimate cardholder repudiates the card-not-present transaction and this has resulted in many e-commerce businesses disappearing after some time. In addition, the level of repudiation and chargeback in card-not-present transactions is very high because the merchant has traded with cardholders they cannot physically ask to sign the authorisation of the order, and so cannot provide a signed receipt to confirm that the legitimate

cardholder made the transaction. In such cases the bank cannot guarantee that transactions done without a signature of authorisation is genuinely initiated by the legitimate cardholder and so are generally good about responding to challenges and giving refunds, but it would be better for all e-commerce participants if the number of fraudulent card-not-present transactions could be reduced.

The biggest problem with electronic commerce technology is the security of all the systems and processes to prevent unauthorised access and fraudulent transactions, the impact of card-not-present fraud in electronic commerce is enormous because this type of fraud directly affects the financial resources and reputation of the business, some of the common impacts can be classified as follows:

### **Financial Loss**

Card-not-present causes the merchant to directly lose the full cost of the items and in some cases additional charges in administering the charge-back process. This incidence starts with a criminal placing an order with the online merchant with a stolen card, and the merchant would process and ship the ordered items in good faith believing the order is a legitimate order placed by the card holder, sometimes it takes up to two months for a dispute to be opened against an order requesting the merchant to provide a signed document showing that the legitimate cardholder place the order, even though the full money will be debited from the merchant, the disputing authority is not concerned about returning the goods which has already been shipped to the criminal. Therefore, the merchant will lose both the cost of the item shipped including any shipping cost and most times with additional charge.

### **Low Sales**

Because of the financial losses involved when card-not-present fraud occurs, merchants are reluctant to approve transactions, especially transactions with higher amount and orders placed from abroad. Merchants will consider what they will lose in the event the order becomes fraudulent, and in most cases the merchant cancels high valued orders that are paid online and orders placed from abroad and this affects the volume of sales a merchant will generate because the cancelled orders will be a mix of legitimate and illegitimate orders.



On the other hand, some customers terminate their orders halfway when 3D Secure is invoked because of a suspicion of phishing attack or when the payment process implemented by the merchant to enhance security is more complex and ambiguous.

### **Restrictions and Reputation Impairment**

Acquirers have charge-back measuring criteria for merchants. This process allows the acquirers to review each merchant's account based on the number of fraudulent transactions received and this is considered on case by case basis, merchants with frequent and rampant occurrences of charge-backs or fraudulent transaction reports often lose their reputation with their banks and most like will have their merchant account terminated. In some cases this might mean a complete inability to process payment online if the merchant does not have an alternative method to accept payment online.

### **Trust**

This research has extensively analysed the effects and importance of trust in electronic commerce. It is understood that trust affects how cardholders participate in electronic commerce and how merchants approve orders placed online because they have insufficient level of trust about electronic commerce, especially card-not-present transaction, this is because the problems and fraudulent activities occurring in electronic commerce is visibly causing adverse effects, for this reason many cardholders choose to return back to the traditional method of buying from a local store where they will be physically present with the seller while merchants are migrating to alternative payment methods.

If e-commerce is to be fully embraced with trust and reliability with other internet technologies, then the merchants need to be reassured that the people on the other side of the internet making card payment are really who they say they are, so that the payment they received online will not be disputed which will indirectly steal their goods. If cardholders are to trust the trend of e-commerce, then they need to be reassured that their privacy and the confidentiality of their card and personal details are protected and the person receiving their data are to be trusted to prevent criminals stealing their sensitive

information. Also, the card issuers need to know that the transaction between a cardholder and the merchant is not fastening them into carrying burden of negative consequences (Card Technology Today, 2002).

## 3. PART 3 – 3W-ADA SENTRY SYSTEM

### 3.1 Introduction to dynamic authentication

Giot, et al. (2009) and Cheswick, et al. (2003) identified three key factors widely recognized to authenticate human to a computer:

- **Knowledge** or *what you know*: known as *one-Factor authentication method*, uses a static password known to the user, – for instance, password or PIN.
- **Possession** or *what you have*: known as *two-Factor authentication method*, uses a one-time password or token that changes in each authentication session, – for instance, one-time password, or token.
- **Inherence** or *what you has*: known as the *three-Factor authentication method*, uses personal attributes of the user, - for instance, biometric information.

There is no decisive list of dynamic authentication method, it is said to have been achieved when a two-factor or more methods are implemented using any technique (Liao, et al., 2006). Dynamic authentication is seen as a long-term solution that meets the requirement of a strong authentication, the method uses a new authenticator that is valid, unique and significant to an authentication session between the claimant and the verifier (Grance, et al., 2010; Li & Zhou, 2010).

According to (Aguoru, 2007), to achieve a dynamic authentication method that meets the requirements of a two-factor authentication, the approach must adhere to the following rules:

- Use of one-factor authentication through a communication channel to setup an authentication session with the server or verifier.
- Use two-factor authentication through an isolated channel to generate an entirely new authenticator that is relevant to the authentication session already established using a logic that is known to the user and server.
- Ability to send the generated authenticator to the server or verifier to authenticate the user.

### **3.1.1 Random number generator (RNG)**

According to Omer (2007), Random Number Generator (RNG) is seen as a cryptographic application for dynamic authentication, the aim is to dynamically and uniquely produce an uncertainty, unpredictability and irreproducibility to authenticate a user. There are two common categories of random number generator; the True Random Number Generator (TRNG) and Pseudo Random Number Generator (PRNG).

True Random Number Generator achieves its randomness through an external device or real world event, for instance, radioactive decay, atmospheric noise or thermal random noise and this process has high entropy but its procedure can be difficult, inefficient or expensive to build. True random number generator includes, dice roll, hardware token, USB security token and Smartcard token devices.

Pseudo Random Number Generator (PRNG) uses a computer software algorithm of a mathematical formula that is deterministic to generate its sequence of randomness. The implementation is easier and cheaper, and operation is efficient, however the entropy output is low. Some mathematical formula for PRNG includes; Analytic Geometry, Definite integrals, Timestamp, hashing, Integration and other formula or logic that can produce randomness using computer software.

### **3.1.2 Hardware dynamic authentication method (True Number Generator)**

In recent years, several dynamic user authentication schemes have been proposed for a secure channel between participants on client-server model environment, and several modifications also proposed in response to the weaknesses discovered in the existing schemes. These schemes uses smartcard, USB and other token devices equipped with cryptographic technology to generate its token. It is classified as True Random Number Generator, aimed to strengthen the use of password in one-factor authentication model introduced by Lamport in 1981. (Fengtong & Xuelei, 2012).

In 2004, Das, et al. (2004) introduced a dynamic ID-based user authentication method using smart card, the method is divided into three phases comprising registration, authentication and password-change. It does not maintain a verifier table, but allows users

to choose and modify their password, this scheme is proposed to protect users against identity theft and resist reply and forgery attacks. Awasthi (2004) claimed that the scheme introduced by Das, et al. (2004) is completely insecure, and using it is like accessing a system without a password. I-En, et al. (2005) proposed a slight modification of the registration and authentication phases to strengthen the weakness discovered in the scheme.

In 2009, Wang, et al. (2009) claimed that the scheme proposed by Das, et al. (2004) and enhanced by I-En, et al. (2005) did not achieve mutual authentication, therefore, could not resist identity theft attacks. And further proposed a more efficient and secure dynamic ID-based remote user authentication scheme that claimed to maintain all the merits of the existing schemes. Other proposals and modifications of existing proposals in the same domain are schemes contributed by Juang & Wu (2009), Li, et al. (2013), Aljawarneh, et al. (2010), and Fengtong & Xuelei, (2012).

Keystroke dynamic authentication method derive its authentication value through the process of analyzing the way a user types at a computer by recording the keyboard strokes many times and attempt to identify them based on habitual rhythm patterns of their style of typing (Joyce & Gupta, 1990). In 2011, Giot, et al. (2011), shows that the main drawback of keystroke dynamic authentication lies on its requirement for a large number of data during enrollment which makes it restrictive and barely usable.

### **3.1.3 Software dynamic authentication method (Pseudo Random Number Generator)**

The GSM mobile network has been seen as a useful and mobile tool for our daily interactions, several approaches to dynamic authentication have adopted the use of short message services (SMS) to deliver a one-time password (OTP) to mobile phone over GSM network as an effective channel to meet up with the requirement of two-factor authentication (Elderawy, et al., 2012; Trupti & Manisha, 2012; Aguru, 2007).

In 1981, Lamport & Ashenhurt (1981) proposed a description of a secure method that assumes a secure one-way encryption function. This proposal claimed that even if there is an interceptor, the security of the authentication between user and the computer is not

compromised. However, high hash overhead, necessity for password resetting, and the storage of verification table are the three main shortcoming of this proposal (Liao, et al., 2006).

Scheme/Characteristic	2FA	Type	ETPY	Comp	DYM	Cost	Setup	CTB	MD
Das, et al. (2004)	Yes	HW	High	High	Yes	High	Slow	No	On
Wang, et al. (2009)	Yes	HW	High	High	Yes	High	Slow	No	On
I-En, et al. (2005)	Yes	HW	High	High	Yes	High	Slow	No	On
Juang & Wu (2009),	Yes	HW	High	High	Yes	High	Slow	No	On
Li, et al. (2013)	Yes	HW	High	High	Yes	High	Slow	No	On
Fengtong & Xuelel, (2012)	Yes	HW	High	High	Yes	High	Slow	No	On
Elderawy, et al (2012)	Yes	SW	Low	High	Yes	Medium	Slow	No	On
Trupti & Manisha (2012)	Yes	SW	Low	High	Yes	Medium	Slow	No	On
Aguoru (2007)	Yes	SW	Low	Low	Yes	Low	Fast	Yes	On
Lamport & Ashenhurt (1981)	Yes	SW	Low	High	Yes	Low	Slow	Yes	On
3W Sentry	Yes	SW	High	Low	Yes	Low	Fast	Yes	On/Off

**Legend:**

**HW** = Hardward; **ETPY** = Entropy; **SW** = Software; **CTB** = Compartible; **COMP** = Compute; **DYM** = Dynamic; **ON** = Online; **OFF** = Offline; **MD** = Mode.

*Table 12: Characteristics comparison table of dynamic schemes*

Research focus on dynamic authentication has been expressively on access to user protected areas – for instance online banking, none of the proposals has shown a systematic method of implementing any of the schemes on card-not-present environment. Therefore, implementation of dynamic authentication on card-not-present transaction has been insignificant not represented.

In 2007, Aguru (2007) proposed a scheme that uses a mathematical algorithm to generates a one-time numeric password that is delivered to the user’s mobile phone when the user invokes an authentication session by submitting a Paymenex account serial number during card-not-present transaction, but this scheme could not pass the User

Acceptance Test (UAT) of the sponsor, because of the overhead cost associated with SMS delivery at every authentication session, and mobile network unavailability.

This research describes an effective way to use the analytical geometry technique to generate random number online or offline, and how to implement it on card-not-present environment to enhance the scheme proposed by Aguru (2007). In this process, the random number can be calculated offline using the PAC card when the mobile network is not available.

Scheme/ Security/Function	ENVI	RA	PH	MIM	MA	VT	Setup	CNP
Das, et al. (2004)	One	Yes	Yes	Yes	No	No	Slow	No
Wang, et al. (2009)	One	Yes	Yes	Yes	No	No	Slow	No
I-En, et al. (2005)	One	Yes	No	Yes	No	No	Slow	No
Juang & Wu (2009),	One	Yes	No	No	No	No	Slow	No
Li, et al. (2013)	One	Yes	No	No	No	No	Slow	No
Fengtong & Xuelei, (2012)	One	Yes	No	No	Yes	No	Slow	No
Elderawy, et al (2012)	One	Yes	No	No	Yes	Yes	Slow	No
Trupti & Manisha (2012)	One	No	No	No	Yes	Yes	Slow	No
Aguru (2007)	One	No	No	No	Yes	Yes	Fast	Yes
Lamport & Ashenhurt (1981)	One	No	No	No	Yes	Yes	Slow	No
3W Sentry	Two	No	No	No	Yes	No	Fast	Yes

**Legend:**

**ENVI** = Environment; **RA** = Reply Attack; **PH** = Phishing Attack; **MIM** = Man-in-the-middle Attack; **MA** = Mutual Authentication; **VT** = Verifier Table; **CNP** = Card-not-present.

*Table 13: Security and functionality comparison table of dynamic schemes*

The reasons for using the framework proposed in 3W-ADA sentry system is to propose an enhanced model which allows to maintain an offline random number generator, this generator will not require the need of a mobile phone or SMS delivery to initiate or completes the proposed dynamic authentication method. This process will prevent the shortcomings of the related SMSV solution. And the justification is presented in **Part 3.2.7** of this research document.

### **3.2 An Overview of the 3W-ADA Sentry System**

The **Who-Where-When** Account Dynamic Authentication Sentry system (3W-ADA Sentry system) is a pseudo-random number generator based dynamic authentication system with the mathematical formula approach of a coordinate or analytic geometry.

The two-dimensional coordinate system identifies its unique point in a plane by a pair of numerical coordinates popularly known as Cartesian coordinates, the identified unique point is used by the 3W-ADA Sentry System to formulate its one-time dynamic authentication token.

The token generated by the calculation of the intersection of the  $X$ ,  $Y$  axis also alternates the requirement of account holder's personal information online, for instance, asking for account holder's name and billing address in online card payment, which exposes account holder to the threats of identity theft and phishing. However, with the alternation of the requirement to enter personal details while making payment online with the 3W-ADA Sentry System, the account holder's personal details and privacy are protected and at the same time, the dependability of the authentication is not broken because the account holder is in each instance uniquely authenticated with a one-time authentication token making each authentication unique and feasibly prevents the threat of identity theft.

The main benefits in choosing and designing the random number generator offered by the 3W-ADA sentry system are as follows:

The pseudo-random number generator model used is efficient, easier and cheap to implement.

Method has high speed and low entropy, but random number generated is aligned or joined in multiples to increase the entropy.

The pseudo-random number generator communication or notification process can be both an electronic and non-electronic procedure.

It can be used anywhere and on all technology environments.

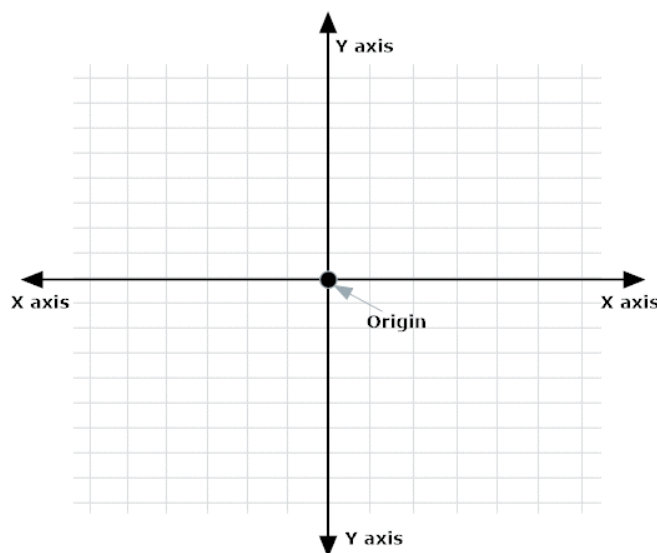


### 3.2.1 An overview of coordinate or analytic geometry

Rene Decartes was a great mathematician, philosopher and scientist from France who made a novel contribution to science. His views about relationship, knowledge, and credit for discovering analytic geometry have been very influential over the past three centuries and in one of his publications and study of geometry he showed how to systematically apply algebra in geometry leading to the discovering of Cartesian or coordinated geometry (Sharma, 2005).

Coordinate geometry - also called analytic or Cartesian geometry - is the study of geometric figures on a flat surface that stretches in both ways endlessly - known as the plane. The plane comprises the “ $X$ ” axis which stretched parallel, and the “ $Y$ ” axis which stretched perpendicular over the “ $X$ ” axis and the point where the “ $X$ ” and “ $Y$ ” axes intersect is called the origin and a right angle is formed at this point (Schultz, et al., 2007).

Coordinate geometry has long been an important concept in the location of unique points and positions, the concept is used in the development of the Global Positioning System or GPS which today offers great advantage to car navigation systems to locate streets and roads in a city. It is used for mapping by calculating the Latitude (North - South or “ $Y$ ” axis) and Longitude (East-West or “ $X$ ” axis) of a location on the Earth known as the geographic coordinate system.



*Figure 27: Coordinate geometry on a plane*

### **3.2.2 Concept of Coordinate geometry plane in 3W ADA Sentry**

According to (Schultz, et al., 2007), in coordinate geometry, the “X” axis is horizontal and the “Y” axis is vertical, and because they are perpendicular they meet to form a right angle. Where this intersects, four quadrants are formed, and since these intersection points can be identified by the calculation of the “X and “Y” axis, the 3W-ADA Sentry concept adopted the framework of representing each intersection point with a random-generated numbers to form its personal authentication code (PAC), and during each authentication 3W-ADA Sentry system will ask for the numbers in two or more randomly selected intersection points, and these numbers are placed in an order in which they were asked to form the personal authentication code for a transaction section authentication.

Each set of coordinate plane has a serial number which acts as an identifier and is used to link the plane to an account to enable a personal access code authentication or it can be unlinked or disabled to remove the 3W-ADA sentry authentication to make it more flexible for users to choose when and where not to use the authentication depending on the environment.

### **3.2.3 Random Number generator for the 3W-ADA Sentry PAC**

The 3W-ADA Sentry system approach to Random Number Generation is the Pseudo Random Number Generation model.

A PHP programming language function is used to generate cryptographically secure pseudo-random integer. A range of available functions includes:

```
int random_int ( int $min , int $max )  
string openssl_random_pseudo_bytes ( int $length [, bool &$crypto_strong ] )  
string random_bytes ( int $length )
```

Every other type of programming or scripting language has its own method for this purpose. Additional logic was formed by placing each pseudo random number generated in an intersection of a coordinated plane and randomly using the intersection point to form

a new unique random number known by the system and the user and also to make it unpredictable.

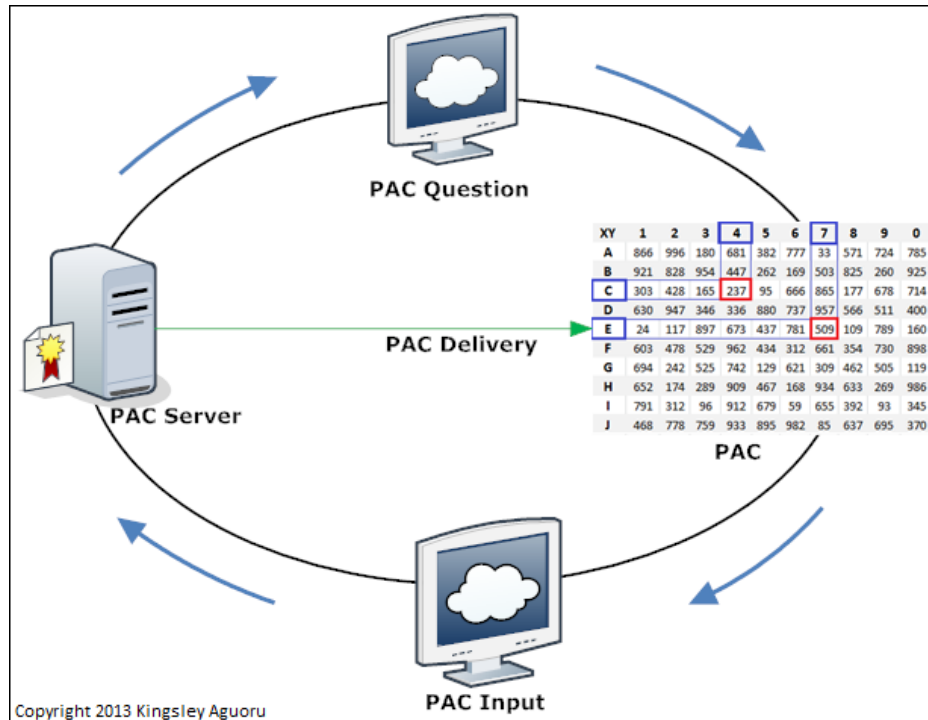


Figure 28: PAC Request and Response Architecture

### 3.2.4 How the 3W-ADA Sentry System Works

The investigation and analysis described in this research project revealed that the focal cause of card-not-present fraud is the constant use of static card details and password to authenticate cardholders during card-not-present transaction. This includes the most popular authentication solution known as Verified by Visa and MasterCard secure code or collectively known as the 3D Secure introduced by Visa and MasterCard.

This makes the static information valid and useful within a considerable period if captured by criminals and this time allows criminals to impersonate the cardholders by using the captured card details to place fraudulent orders on the internet.

The 3W-ADA Sentry system addresses this vulnerability using a non-electronic and low-cost tokenization mechanism introducing the framework of coordinated geometry, or Cartesian coordinates, to obfuscate personal details during card-not-present transaction making each transaction unique.

This process adopted the two-factor authentication with mixed static and dynamic information.

The 3W-ADA Sentry system is not limited to providing dynamic authentication to online card-not-present transactions, it is also an invaluable authentication system for access to online member only or restricted areas, for instance online banking systems. However, for the purpose of this research, the illustration described in this document will be limited to card-not-present payment or electronic commerce environment.

During checkout from an e-commerce shopping cart, user is redirected to a payment page where summary of shopping cart value will be displayed and available payment method, customer select Paymenex as the payment method, enter his account or card serial no and proceed, the integration done at merchant shop will send required information to the gateway through the 3W-ADA Sentry system.

The 3W-ADA Sentry system will use the submitted serial number to identify linked coordinate plane from the plane directory and a corresponding session identification code generated. When the customer inputs his PAC response, this will be checked against the stored numbers and session identification code to identify match.

Account Serial No	<input type="text" value="11124711"/>	
Enter Card No	<input type="text" value="6001350253588859"/>	
Enter <b>Third</b> Digit of WebKey	<input type="text" value="2"/>	
Enter <b>Fourth</b> Digit of WebKey	<input type="text" value="6"/>	
Enter PAC <b>E7</b>	<input type="text" value="509"/>	
Enter PAC <b>C4</b>	<input type="text" value="237"/>	
Card Expiry Date	Month : <input type="text" value="12"/>	Year : <input type="text" value="2017"/>
Payment Amount	GBP 10.0	
Today's Conversion Rate	1 GBP = GBP 1.0	
Total to be Debited	GBP 10.0	
	<input type="button" value="Submit"/>	

Figure 29: 3W-ADA Sentry dynamic authentication

The illustration above shows a page schematic of the proposed user interface of the 3W-ADA Sentry system in an online payment environment where four unique questions marked in red are used to form the authentication token.

Two random digits of the Webkey, for instance, the *third* and *fourth* digits of a six digits integer – 812698 were asked and which resulted in 2 and 6. The six digits integer known as the Webkey is a security code linked to a card account and only known by the card holder.

Each set of Webkey are not known in advance by the cardholder same way they know their PIN, and are different in each transaction session, the 3W-ADA Sentry has inbuilt logic of presenting each set of random Webkey digits combination questions during each transaction section.

XY	1	2	3	4	5	6	7	8	9	0
A	866	996	180	681	382	777	33	571	724	785
B	921	828	954	447	262	169	503	825	260	925
C	303	428	165	237	95	666	865	177	678	714
D	630	947	346	336	880	737	957	566	511	400
E	24	117	897	673	437	781	509	109	789	160
F	603	478	529	962	434	312	661	354	730	898
G	694	242	525	742	129	621	309	462	505	119
H	652	174	289	909	467	168	934	633	269	986
I	791	312	96	912	679	59	655	392	93	345
J	468	778	759	933	895	982	85	637	695	370

Figure 30: 3W-ADA Sentry coordinate plane

The diagram above shows the coordinate plane used for the dynamic authentication token known as Personal Authentication Code or PAC.

Calculation of the PAC does not require any electronic device but it is done by the manual calculation of the point where the “X” axis intersects the “Y” axis known as the origin.

Two random PAC questions are also uniquely asked and not repetitive.

Therefore, our calculation for the 3W-ADA Sentry dynamic authentication code for this transaction is as follows:

- a) Third Digit of Webkey = 2
- b) Fourth Digit of Webkey = 6
- c) PAC E7 or E7 of XY Coordinate = 509
- d) PAC C4 or C4 of XY Coordinate = 237

3W-ADA Sentry dynamic token = abcd (26509237), hence, in this transaction the code **26509237** is the dynamic authentication code and will never be repeated in the life history of the account used.

### 3.2.5 The 3W-ADA Sentry system Models

3W-ADA Sentry system can be developed as an integrated module and incorporated within an electronic account management system environment or a standalone and third-party authentication system providing authentication services to external electronic account management platform through application programming interfaces.

#### 3W-ADA Sentry system as an Integrated Model

Implementing 3W-ADA Sentry system as an integrated module within an existing electronic account management platform allow operators to maintain a low-cost and secure payment network with built-in 3W-ADA security module.

This development will require modification of internal codes or interfaces to integrate seamlessly with the 3W-ADA Sentry module, this will be a light integration that will work like an “add-on”, and also will be fast to implement and manage. There will not be any external or remote connection between the 3W ADA sentry system and the payment network or the card account management system, this will make the response time fast and effective.

The architectural layout of such implementation can be seen as follows;

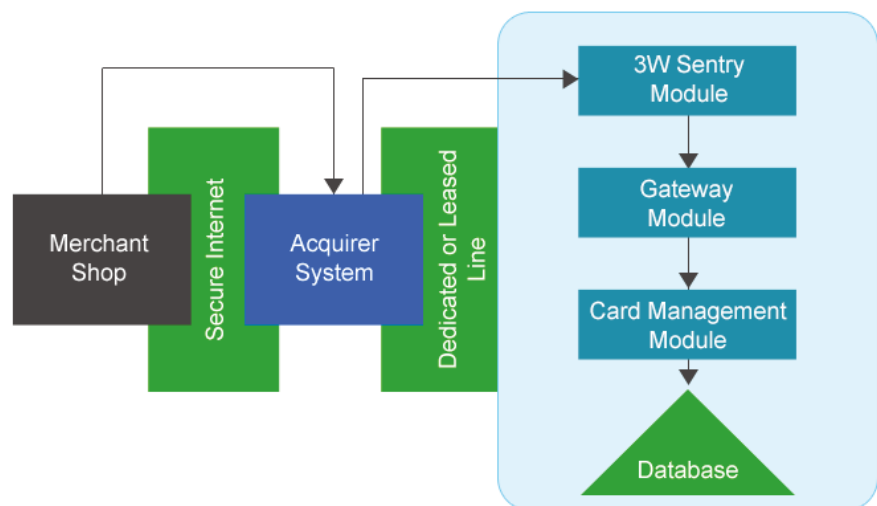


Figure 31: 3W-ADA Sentry integrated Model

### 3W-ADA Sentry system as a standalone Model

Implementing 3W-ADA Sentry as a standalone or third-party system requires the new development of an authentication platform with the 3W-ADA Sentry system software requirement specification document.

This will enable the developer to offer the 3W-ADA Sentry system as a service, and existing electronic payment account management and network operators can subscribe to and benefit from this implementation by interfacing with the third-party system using application programming interface (API) over a secure channel such as virtual private network (VPN) or any other type of web service protocol.

This implementation will require two phases of work, firstly, developing the 3W-ADA Sentry system and secondly developing a range of application programming interfaces for merchant, and for payment processors or network operators.

This implementation also is invaluable for organisations wishing to focus on providing secure authentication services to other businesses. In such a case, the project needs to be expanded to accommodate customer relationship management (CRM) systems which will enable the organization to manage the profile of the corporate organisations using their authentication services.

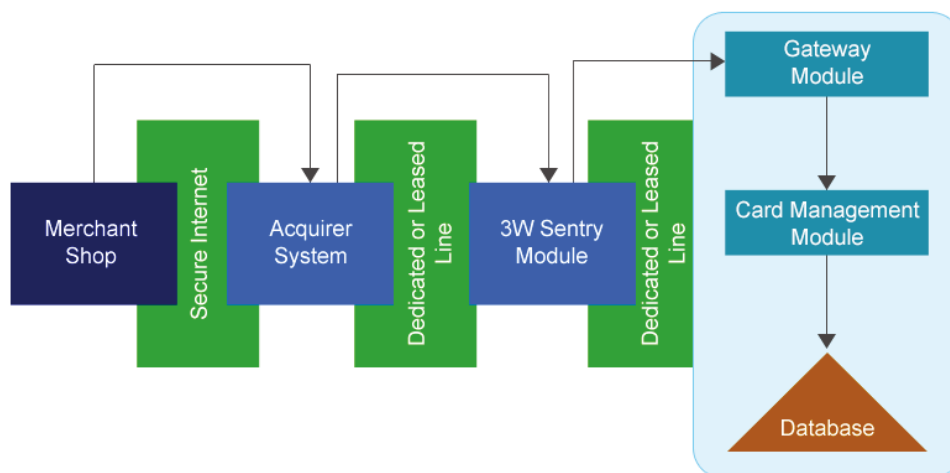


Figure 32: 3W-ADA standalone Model



Whether the 3W-ADA Sentry is implemented as a standalone system or integrated into an existing system, the card-not-present authentication follows the same process. The software produced by this research project was developed using the framework of the integrated model of 3W-ADA Sentry system development.

The purpose of choosing the integrated model is because the project sponsor is a payment network with an existing card account management system and has provided their development platform for the necessary modification to suit the requirements of the 3W-ADA Sentry system framework, and also for testing and implementation.

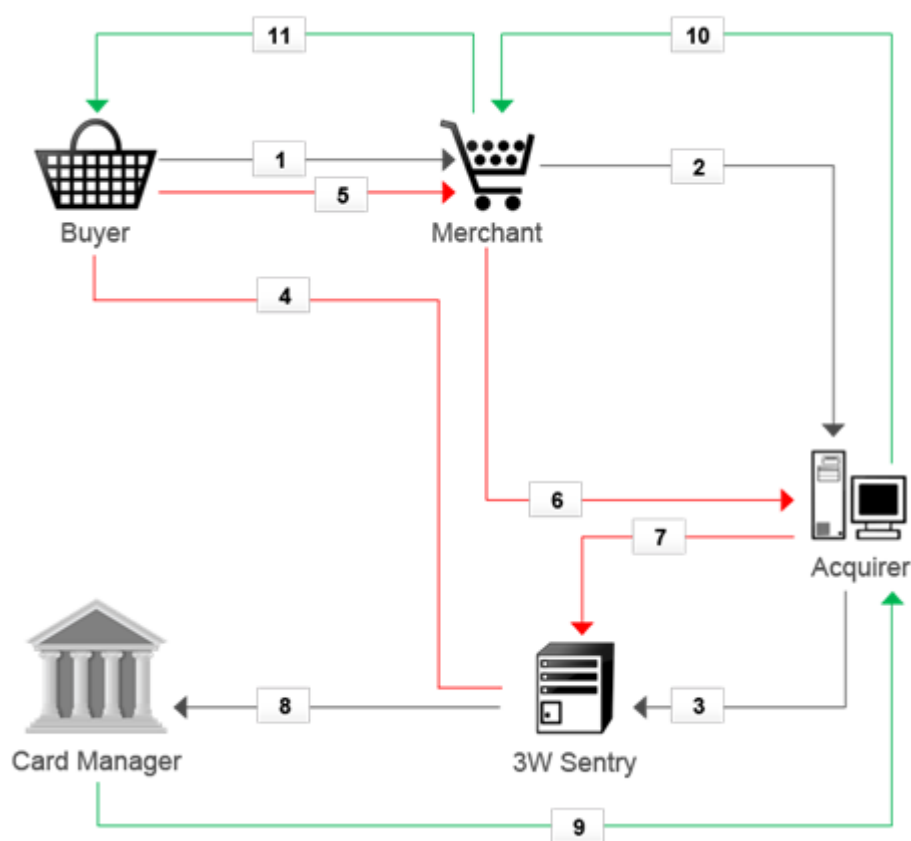


Figure 33: 3W-ADA Card-not-present Transaction flowchart

The sequential flow of event as illustrated in Figure 34, is described in the following 3W-ADA transaction table.

No	Origin	Destination	Value	Action Details
1	Cardholder	Merchant	Serial No	Cardholder Input Card serial no at checkout of merchant's shop
2	Merchant	Acquirer	Serial No,	Merchant route serial no, shopping cart information, (i.e. amount, currency, and order no) to Acquirer for processing.
3	Acquirer	3W-ADA	Serial No,	Acquirer forward the data supplied by merchant to 3W-ADA to delegate authentication of cardholder.
4	3W-ADA	Cardholder	Webkey, PAC, Card No, Exp Date,	3W Sentry identify cardholder with the Serial No, and send out Webkey & PAC query to cardholder (Only at this time will cardholder know the three-factor authentication token, which he can compute using his PAC card, or received the token by SMS.
5	Cardholder	Merchant	Cart Info, Webkey, PAC, Card No, Exp. Date	Cardholder input new variables on step two at merchant shop.
6	Merchant	Acquirer	Cart Info, Webkey, PAC, Card No, Exp. Date	Merchant forward same information to Acquirer.
7	Acquirer	3W Sentry	Cart info, Webkey,	

			PAC, Card No, Exp. Date	Acquirer routes same information to 3W Sentry
8	3W Sentry	Card Manager	Cart info, Card No, Exp Date	3W Sentry finally sends cart info, card account no to be debited to card manager for processing.
9	Card Manager	Acquirer	Serial No, Status, Merchant ID, amount, transaction ID	Card manager log entry, and send complete transaction information to Acquirer.
10	Acquirer	Merchant	Serial No, Status, Merchant ID, amount, transaction ID	Acquirer Log entry and send transaction report to merchant
11	Merchant	Cardholder	Order ID, Transaction ID, Transaction Status	Merchant process order and send email to cardholder

*Table 14: 3W Sentry transaction flowchart*

Though the PAC can be communicated through the short message services of a mobile operator to the registered mobile number of the account, the PAC card is provided to increase the service availability, for instance if the mobile network is not reachable.

XY	1	2	3	4	5	6	7	8	9	0
A	802	621	942	991	155	797	56	559	470	653
B	933	929	499	418	994	434	66	479	178	587
C	653	953	766	710	873	831	925	869	336	287
D	904	633	655	758	204	866	970	942	823	744
E	630	905	676	319	748	431	860	504	104	351
F	813	704	255	780	399	325	471	236	565	344
G	729	920	687	325	795	419	212	322	110	775
H	830	312	476	407	553	173	975	215	361	629
I	184	680	799	577	600	910	114	199	221	987
J	544	262	172	796	284	904	487	811	581	260

Figure 34: Sample PAC card (Plane)

### 3.2.6 SWOT Analysis of the 3W-ADA Sentry system

The following analysis presents the 3W-ADA Sentry system using the framework of SWOT analysis.

#### 3.2.6.1 Strengths - 3W-ADA Sentry system

- Tokenization of the payment information to make each card-not-present or online authentication unique.
- Obfuscation of cardholder personal information to prevent identity theft.
- Can be offered as a standalone or third-party security authentication service or integrated into an existing system.
- Low-cost to implement and easy to manage.
- Platform independent.
- Non- electronic.
- Cross-platform and can integrate seamlessly with all systems.

#### 3.2.6.2 Weaknesses - the 3W-ADA Sentry system

- Vulnerable to identity theft if PAC Card is lost or stolen with the card.

- GSM network through which the PAC is delivered to the cardholder's mobile phone might not be reachable and hence PAC will not be delivered or the delivery will be delayed.
- The security solution is introduced by a source that is not well known in the payment industry; hence adoption of solution might be difficult to some extent.
- Since it's an optional additional security measure to protect account holders in card-not-present environments, some customers may not like to experience additional steps to pay online and so may not enroll on the security program.

### **3.2.6.3 Opportunities - the 3W-ADA Sentry system**

- The 3W-ADA Sentry system was developed for a leader in alternative payment, and with the trend of alternative payment and the adoption especially in African countries, the 3W-ADA sentry system stands a good chance to gain market and awareness in areas where alternative payment methods are used.
- This research has tried to prove the concept and feasibility of 3W-ADA sentry system, if the authentication can feasibly protect card-not-present fraud, and conceal cardholder's personal information, merchants and payment service providers will be attracted to a solution that works.

### **3.2.6.4 Threats - The 3W-ADA Sentry system**

- Tokenization devices used by banks may be restructured to work in card-not-present environments, and this will cause the banks to promote their own product over any other third-party security systems.
- Adoption of 3W ADA sentry system by the leading card association for instance Visa and MasterCard may not be possible, because they are currently promoting their own solution known as 3D Secure, even though this solution has significant vulnerabilities, they might choose to upgrade their existing system instead of implementing entirely new solution.
- The project owner may not want to commercialize the solution.

### **3.2.7 Justification of 3W-ADA Sentry**

This research presents a justification for the use of the 3W-ADA Sentry system as a feasible solution to prevent card-not-present fraud, via the following main points:

#### **3.2.7.1 Research Findings**

The investigative research carried out during this research discovered that the obvious problem of the existing card-not-present solutions is the static nature of data used to authenticate the cardholders over the insecure internet network, and this further exposes the card details and customers' personal data to the vulnerability of internet threats, for instance, identify theft. Not only are customers' cards used fraudulently online but at most times their personal information are also stolen and used in other fraudulent activities, but the solution proposed in this research solved the problems in the following ways:

#### **Enhancement of the SMSV Scheme**

The main problem of the SMSV is its reliance on mobile phone which has cost and network availability implications. The 3W-ADA sentry system presents an enhanced scheme that modified this process by using an analytical geometry model which allows to maintain an offline random number generator, this process removed the mandatory requirement to deliver the random number through the user's mobile phone.

#### **Dynamic authentication in card-not-present transaction**

The 3W-ADA sentry system proposed a dynamic authentication process in card-not-present transaction.

The dynamic concept used in developing the 3W-ADA Sentry system makes each transaction over the internet a unique cardholder's experience using an instantly generated unique token, and the corresponding transaction session identification code is valid only for a payment transaction requested. The token is compared with the stored transaction session identification code before authentication can be approved.

When a cardholder requests to make payment online, the 3W-ADA Sentry gateway returns a Personal Access Code (PAC) questions to the cardholder's user interface or

environment, and a copy of the transaction session identification code interpreting the personal access code.

When the personal access code is submitted by the cardholder, the 3W-ADA Sentry system compares and validates the personal access code input with the transaction session identification code to make sure both matched.

The 3W-ADA Sentry uses a dual session based authentication process by firstly comparing the transaction session identification submitted by the customer's browser to make sure it is submitted by the same person, and the authentication of the personal access code on the second phase only takes place if the first phase is completed successfully.

This concept of dynamic process incorporated in the 3W-ADA Sentry system's payment process algorithm makes it difficult for fraudsters to re-use the data stolen from card-not-present payment transaction in future and as such will counter the motivation of identity theft because it will be same as useless data.

### **Concealing of personal information**

The current card payment method practiced by Visa and MasterCard asks customers to input their personal information in an online webpage, but with the concept of the 3W-ADA Sentry system customers do not need to enter their names, addresses, in some cases, name of issuing bank and date of birth to pay online, the use of personal and billing information during payment is replaced with the dynamic token and transaction session identification code.

### **3.3 3W-ADA Sentry Software Requirements Specification (SRS)**

#### **3.3.1 Introduction**

This section describes the requirement specifications of the 3W-ADA Sentry system and provides a blueprint for its development. The role of this software requirements specification (SRS) section is to provide a description of the 3W-ADA Sentry system as a software, the basis for developing its architectural design either as an integrated or a stand-alone model of 3W-ADA sentry system, and to act as the reference point to verify that the completed software satisfies the requirements.

##### **3.3.1.1 Purpose**

The purpose of this part of the document is to define the requirements specification and architectural design of the 3W-ADA Sentry system and provides a coherent guideline and plan for its development phases and process cycle. It also delivers a clear documentation of its compositions, functionalities, limitations and specifies the necessary operational sequences to be carried out in functional terms.

To enable a detailed understanding for the Paymenex technical team and the project supervisors about how to develop the accurate software that meets the requirements specifications and enable the supervisor to make analyses of its adaptability to the requirements document or the solution proposed.

Nevertheless, this software requirement specification describes the complete requirements of both integrated and standalone model of 3W-ADA sentry system to give developers varieties of choice to choose according their requirement.

##### **3.3.1.2 Project Scope**

The software system to be produced is an online account dynamic authentication system that uses the Cartesian two-dimensional coordinate system to establish a non-electronic dynamic authentication token used for its real time authentication branded as the WHO-



WHERE-WHEN Account Dynamic Authentication System or simply the 3W-ADA Sentry system.

The token is generated by the calculation of the intersection of the *X, Y* axes and it enable Paymenex Limited to alternate the use of account holders' personal information online, for instance, asking for the individual account holder's name and billing address in online card-not-present payment authentication, which expose the account holder to identity theft threats and to strengthen the current static details used for online Paymenex card payment with a dynamic token which reassures customer's protection from threats of online identity theft.

The 3W-ADA Sentry system is also invaluable to other online service providers, payment networks and payment processors faced with similar card-not-present fraud problem as Paymenex, this includes Visa and MasterCard and their related participants.

The 3W-ADA Sentry system is middleware and intermediates between the Paymenex merchant's payment system and the Paymenex payment processing gateway or the Paymenex card management system. The level of integration depends on the Paymenex technical team.

The 3W-ADA Sentry system is designed to be a low-cost, flexible and effective non-electronic dynamic system that can integrate seamlessly into Paymenex xTransNET system or any other payment processing gateway or used as 'software as a service' (SAAS) that offers on-demand verification and dynamic authentication solution.

The dynamism in 3W-ADA Sentry system makes it suitable to wither the threats of identity theft and prevent card-not-present fraud.

The concept of the 3W-ADA Sentry system can be developed and implemented as an external or third-party middleware system or developed and implemented as an internal module which seamlessly integrates with existing card management and interchange platform.

However, the scope of this project is limited to the development and implementation of the 3W-ADA Sentry System as an internal module that will serve as add-on or plug-in to

Paymenex xTransNET and can be adopted by similar systems who want to leverage 3W-ADA Sentry system to counter card-not-present fraud.

### **3.3.1.3 Definitions, Acronyms and Abbreviations**

The definition and abbreviation used in this specification requirement document is provided in the glossary table.

### **3.3.1.4 References**

The specifications requirements section is prepared according to the recommendation of IEEE and ISO standards (Systems and software engineering, 2011).

## **3.3.2 Overview**

This section of the document is grouped in sub-sections with each sub-section providing a detailed description to support the development of the 3W-ADA Sentry systems.

*Introduction:* Provides a summary of the 3W-ADA Sentry Specification documentation, its purpose and scope.

*Overall Description:* provides summary of the high level functional requirements of the 3W-ADA Sentry system, including product perspective and high-level functionalities, User classes and characteristic, general constraint, documentation, assumptions and dependencies.

*Specific Requirements:* this section describes all required interfaces, including external interface, user interface, communication interface, hardware and software interfaces.

*Functional Requirements:* This section describes the detailed functionalities of the 3W-ADA Sentry system divided in categories and sub-sections, detailed functional description of setting up the payment networks and card account management systems, setting up SMS and Email communication gateways, functional requirements for enrolling cards.

Use Cases: This section describes a detailed Use Cases of the system and all sub-systems as a flowchart to illustrate how to develop the sequence of event.

Non-Functional Requirements: Finally, this is not a functional requirement, but provides additional requirements that support the effective operation of the system, it describes guidelines necessary to ensure that the developed system is secure, reliable, available to use, safe and performs at an acceptable level.

### **3.3.3 Overall Description**

This section describes the 3W-ADA Sentry system and its operational functions, usages, and environments.

#### **3.3.3.1 Product Perspective**

Card present transaction is attributed to using physical object for identification and verification because making card present payment involves the cardholder physically presenting the card to the merchant who will insert the physical card into a payment acceptance device for validation and authentication with personal identification number (PIN), this process is called the “*chip and pin technology*” which is fundamentally preferred by merchants as a safer method for card payment acceptance.

Generally, using physical objects for identification is expensive to replicate, less vulnerable to fraud threats, and difficult to reproduce by third-parties or criminals because any added secret by the original producer or owner may not be easy to replicate or cloned, and face-to-face identification also gives more credibility, trust and opportunity to physically examine and identify the object. However, this is not the case for remote identifications such as card-not-present transactions when no physical object is involved, because it uses static card and personal information to complete payment online giving rise to card-not-present fraud and the existing solutions developed to prevent the fraud also could not resolve the problem because most solutions use static passwords which can be stolen by criminals.

The 3W-ADA Sentry system replaces the existing system by introducing a new model which eliminates the use of vulnerable static data during online card-not-present payment

authentication and replaces the process with a low-cost, non-electronic and dynamic authentication token to make each card-not-present authentication a unique experience and prevent the customer from entering personal details each time payment is made online.

### 3.3.3.2 Product Functions

This research identified the causes of card-not-present fraud to be the exploitation of a flawed payment process that uses static data to complete online payment, motivation to steal for financial gain, and identity theft practices.

The success rate recorded in this type of payment is attributed to the fact that the data remain static and can be reused over and over again for a certain period.

However, the 3W-ADA sentry system removed some of the non-effective static data requirements and replaced it with a non-reusable and dynamic token that stands as additional factor to protect cardholders' personal information. The following table presents the comparison between data used by existing systems and 3W-ADA sentry system.

Data Description	Data Type	Existing Solutions	3W-ADA Sentry
Card Serial/Reference No	static	Not Used	YES
Card No	static	YES	YES/NO
Card Expiry Date	static	YES	YES/NO
Card Start Date	static	YES/NO	Not used
CVV (security code on back)	static	YES	Not used
Name of Customer	static	YES	Not used
Customer's Address	static	YES	Not used
Customer's City	static	YES	Not used
Customer's Country	static	YES	Not used

Customer's Post Code	static	YES	Not used
3D Secure Password	static	YES	Not used
3W-ADA Sentry PAC	dynamic	NO	YES

*Table 15: 3W-ADA Sentry system data requirement relationship*

All the static information contained on the 2<sup>nd</sup> to 4<sup>th</sup> rows on Table 13, even though are vulnerable to identity theft, cannot be used to complete a card-not-present payment on their own merit. The information contained on the 5<sup>th</sup> to 12<sup>th</sup> rows are also vulnerable to identity theft and adding these information to the previous can successfully complete a card-not-present transaction and at the same time expose personal information to other types of identity theft fraud and this is the main point of the problem.

The 3W-ADA Sentry system avoided all static data requirements that expose personal details to identity theft threats and replaced them with a one-time dynamic token called personal authentication code or PAC, using a low-cost and non-electronic authentication mechanism as indicated on the 13<sup>th</sup> or last row.

During a card-not-present transaction powered by 3W-ADA Sentry system, a customer is required to enter his account's serial no on the first step, this will enable 3W Sentry to validate the enrolment of an account with the given serial no in the enrolment directory, and identify its aligned PAC account.

At this point, the process is still at 3W-ADA Sentry system, the card issuer has not been contacted. To validate that the serial no is submitted by the legitimate cardholder, 3W-ADA Sentry will respond with further authentication questions including two dynamic and four static data. The dynamic data in some cases is communicated to the legitimate cardholder using the mobile number enrolled in 3W-ADA Sentry system, or the cardholder will manually identify the answer using his PAC Card.

The Cardholder must present the correct responses to both static and dynamic data question to complete the payment.

### 3.3.3.3 User Characteristics

The users of 3W-ADA Sentry system are classified into the following classes;

#### **Technical User**

This class of users includes the technical team and software engineers at Paymenex Limited or a related company using the 3W-ADA sentry who already have knowledge of their platform and the available application programming interfaces;

Class: Developer, Software Engineers, Software programmers.

Frequency: During new integration, implementation and day to day technical support.

Area and Function: Application programming interface to integrate and implement the system and the graphical user interface to manage the system.

Technical Knowledge: Experience in Advance Encryption standard protocol, XML and general programming.

#### **Non-Technical User**

This class of user includes customers wishing to make payment online or, he is the vulnerable user whose card and personal information needed to be protected from identity theft. And also includes the merchant, payment service provider and payment network operator who will implement the 3W-ADA sentry system at their online payment gateway, they are also vulnerable to card-not-present fraud.

Class: Business, Merchant, Cardholder, Manager, Administrator and General Staff.

Frequency: Day to day management and usage of the system

Functions: Graphic user interface to enable cardholder's verification and payment from the merchant's online shop, and graphic user interface to enable business administrators to manage the system, including enrolling new account and general system monitoring.

Technical Knowledge: Not required.

#### **3.3.3.4 General Constraints**

Paymenex Limited failed to approve our request to integrate the 3W-ADA sentry system directly to its TransNET platform, however, this project presented a useful guideline sufficient for a normal programmer to integrate the 3W-ADA sentry system.

HTML codes shall meet at least the version 4.0 standard and server side scripting language for the merchant extension shall be PHP.

Other classified constraints includes;

- Compatibility and Compliance Constraints.
- Deployment Constraints.
- Quality and grade of System.
- Government legislation and Policy.

#### **3.3.3.5 User Documentations**

Handbook or Manual for Administrators who will be using the graphical interface for general operation and management of the 3W-ADA sentry system.

Technical documentation for the application programming interface for merchants to enable them to integrate the 3W-ADA sentry authentication interface within their shopping cart environment.

#### **3.3.3.6 Assumptions and Dependencies**

- Linux Server (LAMP) running PHP 5 or higher for the merchant extension.
- Paymenex TransNET system's language and Database version or type.
- Good internet connection between personal computer and server.
- Short Message Services HTTP gateway to enable SMS communication.
- mCrypt module for PHP installed on the merchant's server and similar orientation on Paymenex TransNET.

### **3.3.3.7 Deliverables**

The deliverables of this project are divided into two parts. The first part is the 3W-ADA Sentry merchants' interface, which is designed to be installed and used at the merchant shopping cart. The second part is a design and illustration of required update and changes designed to be carried out by the technical team at Paymenex Limited to meet up with the requirements.

### **3.3.4 Functional Requirements**

The functional requirements include all related functions of the 3W-ADA sentry system and its related API function implemented at the merchant shop.

#### **Graphic User Interface – Web-based**

This includes all administrative, customer service and cardholder interfaces that provides graphic user interface to the account enrolment and management features, merchant registration, key management and PAC management modules, and card authentication interface for cardholders, which provides the interface for cardholders to enter their card details and PAC information for authentication and payment.

#### **Application Programming Interface**

The application programming interface is based on NVP and XML technology and works as a machine-to-machine interface without human intervention. It enables 3W-ADA sentry to communicate with the merchant system to authenticate account holder directly at the merchant shop and if the development is using the standalone model, additional interface with the payment network to pass verified payment transactions for processing will be required.

#### **3.3.4.1 3W-ADA Sentry System functional requirements**

##### **Setup Payment Network and Setting**

Before a card issued by a network can be enrolled in the 3W-ADA sentry system the network configuration is required, and its communication pathway setup to enable the 3W-ADA sentry system to request validation and submit payment messages.



- The system shall enable the listing of all integrated Networks and Payment systems.
- The system shall enable the ability to modify, edit, suspend, cancel or delete any network.

This component is required if the development is using the framework of the standalone model where the 3W-ADA sentry system will be external to the card account management system or payment network.

### **Setup SMS Gateway**

3W-ADA Sentry requires SMS gateway to enable its short messages services communication and all integrated SMS gateways shall appear in SMS Gateway listing.

- System shall be able to add new or remove existing of SMS gateways.
- System shall allow for the setting of SMS gateway credentials.
- System shall be compatible with common SMS gateways.
- System shall allow adding multiple SMS gateways.

This component is required if the development is using the framework of the standalone model where the 3W-ADA sentry system will be external to the card account management system or payment network.

### **Setup Email Gateway**

3W-ADA sentry system requires Simple Mail Transfer Protocol (SMTP) settings to enable it send out email messages to recipients.

- System shall allow the settings of SMTP host address and port.
- System shall allow the setting of email account username and password.
- System shall allow sending email using both external and internal mail servers.
- System shall allow adding multiple mail server accounts.

This component is required if using the standalone model because the 3W-ADA sentry do use email as part of its communication method during authentication.

## **Authentication Settings and Configurations**

Authentication credential and key management functionalities are required because the 3W-ADA sentry system stands in the middle of external third-party system and communicates over either internet or relevant networks, it uses authentication credentials provided by the network, and also provides credentials to merchants, this enable a communication flow between the three systems.

- System shall enable to setting of network credentials through the graphic user interface.
- System shall be able to provide authentication credentials to merchants connecting to it.
- System shall be able to allow the reset of the authentication credentials.
- System shall enable the ability to disable the credentials.

This component is fully required in the standalone model because key management is required for both merchants and payment networks, but if development is following the integrated model, only the merchant key management is necessary.

## **Card Enrolment**

All qualifying cards with its card management system or payment network connected to the 3W-ADA sentry system can be enrolled in the security program after successful validation from their provider.

- System shall allow the enrolment of card after it has been validated from the card provider using its identification number and a password or Webkey from the 3W ADA sentry public interface.
- System shall allow the manual enrolment of card with only the serial no by an Administrator or Customer Service.
- Card can only be enrolled once and assigned to a unique primary identification number.
- Enrolled card shall be stored in the database as encrypted data.
- Only the card details required for enrolment shall be used.
- System shall allow for re assigning or change of PAC serial no.

- System shall have option to enable SMS communication of PAC details to customer's mobile number held at payment network.

This is a mandatory component for both models.

### **Enrolled Card Directory**

- Successfully enrolled cards are added in enrolment directory.
- Card enrolment directory graphic user interface shall list all enrolled cards in a table showing columns of related card parameters, for instance, unique primary identification, card serial no, date enrolled, PAC serial no, and current status.
- Each row shall have option to disable, delete and re-activate enrolment.
- System shall have separate interface for the listing of disabled and active cards.

This is a mandatory component for both models.

### **Authentication History**

Aim of the authentication history is to store and list a history of all authentication queries, sessions and their status.

- Each time an authentication request is submitted from merchant shop, the system shall store detailed information of the request in session before starting the PAC authentication process, and after the process, it shall also store all information in database including, session id, serial no, date and time, request identification number, merchant identification number and PAC coordinate question, status of the authentication, and number of attempts.
- System shall store and be able to provide as export all relevant trails of authentications.
- System shall store and be able to provide as export or web view all relevant trails of its communications with the payment network.

This is a mandatory component for both models.

## **Merchant application programming interface**

The merchant application programming interface shall interface with merchant shop front and be able to receive and respond to requests from the merchant's application.

- Merchant interface shall be able to post card details to 3W-ADA sentry system matching the correct parameters supplied by the 3W-ADA sentry system operator.
- Merchant interface shall be able to receive and parse the XML response nodes and parameters into the merchant shop's graphic user interface with form fields to enable the collection of card details for authentication.
- Merchant interface shall be able to accept input from customers using form field and be able to convert the data received into the acceptable format of the 3W-ADA sentry system's application programming interface, the data input includes card serial no, card no, expiry date, Webkey, and answers to personal access code questions.

This is a mandatory component for both models.

## **Payment Network application programming interface**

The payment network application programming interface shall be an interface between payment networks or card account management systems and the 3W-ADA sentry, this will be a channel through which the 3W-ADA sentry system can be able to pass authenticated and verified payment message to the payment network to obtain a decision.

- The 3W-ADA sentry system shall be able to authenticate the payment network using its settings and keys.
- The 3W-ADA sentry system shall be able to identify the payment network when it receives verification and authentication request from the merchant.
- The 3W-ADA sentry system shall be able to validate the payment network and route the payment authorisation request.
- The 3W-ADA sentry system shall be able to receive response from the payment network and pass it on to the merchant to enable decision making.
- The 3W-ADA sentry system shall be able to store history of this communication.

This component is required if the development is a standalone model where the payment network is external from the 3W-ADA sentry system.

### **Integrated and Standalone models comparison**

The following table describes the comparison of the components necessary for the development of each model.

<b>Component</b>	<b>Integrated</b>	<b>Standalone</b>
Setup Payment Network and Setting	NO	YES
Setup SMS Gateway	NO/YES	YES
Setup Email Gateway	NO	YES
Authentication Settings and Configurations	Merchant	Merchant/ Payment Network
User Profile Management	NO	YES
Card Enrollment	YES	YES
Enrolled Card Directory	YES	YES
Authentication History	YES	YES
Merchant application programming interface	YES	YES
Payment Network application programming interface	NO	YES

*Table 16: 3W ADA Sentry System Model Components*

### 3.3.4.2 Use Cases

The 3W-ADA Sentry will have three users: the Administrator who will have root access and will configure all payment and card networks using the system; the Customer Service who manages the enrolment of card and; the Cardholder who accesses the system through a public graphic user interface to validate and enrol his personal card.

#### 3W-ADA Sentry Use Case

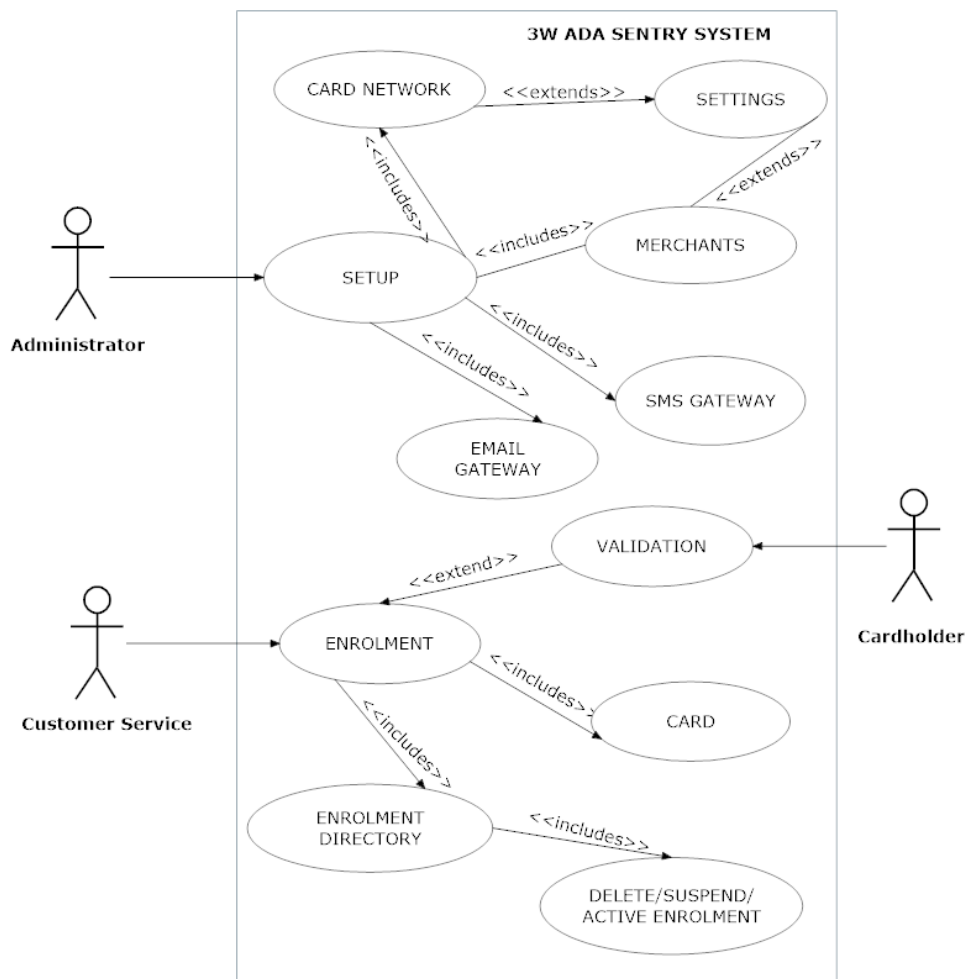


Figure 35: 3W ADA Sentry system Use Case

## Merchant interface Use Case

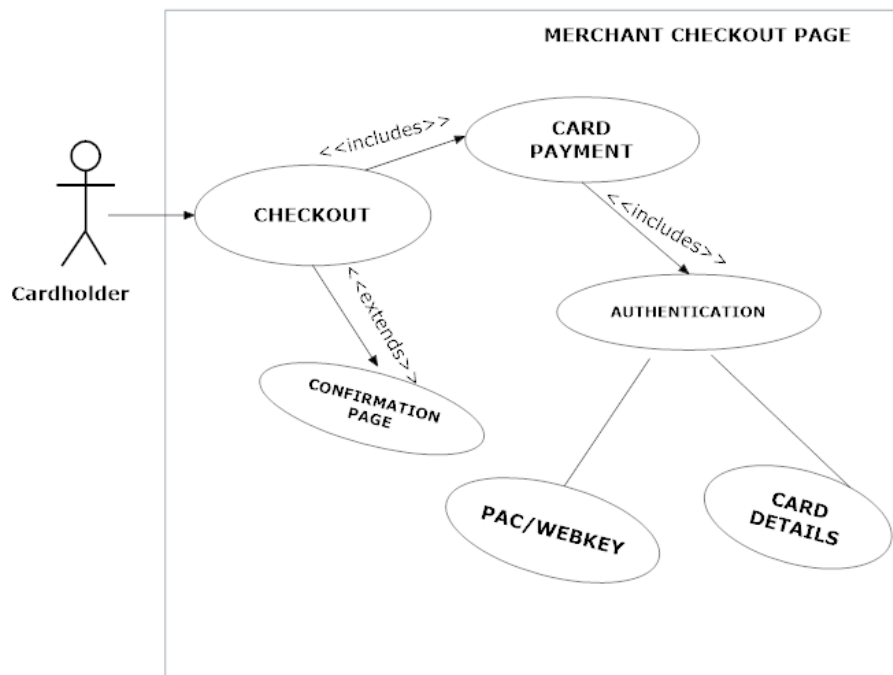


Figure 36: Merchant interface Use Case

### 3.3.4.3 Non-Functional Requirements

#### Usability and Navigability

- The system shall be user-friendly, easy to navigate and find ways around it, intuitive graphic user interface that will be easy to access, and menus positioned in visible locations of the interface.
- Menus shall be relative to the page content or function.
- Font sizes, colours and images shall be structured in the look and feel of the whole system and where necessary cascading style sheet (CSS) shall be used to give a perfect finish.

## **Accessibility**

- The system shall have provision for disabled users.
- The system shall support multi languages.
- The system shall be accessible through common web browsing applications, for instance, Internet Explorer, Firefox, Google Chrome and Safari. The accessibility may be extended to mobile devices using a responsive HTML technology.

## **Performance**

- System shall be compatible with most browsers or mobile sites, running from both web, mobile and application servers.
- System should be able to process over 100 simultaneous requests from merchant's shop and be able to respond within one second in peak time without getting overload.
- System shall be able to deliver response received from card network within 5 seconds or before the set session expires.
- Simultaneous customer service users can be performing enrolment of different accounts.

## **Reliability**

- System shall be able to handle errors and report bug to Administrators.
- System shall be easy to recover with adequate backup plan in place.
- System shall be free from bug, virus, malfunctions and errors.
- System shall maintain redundant servers, failover sites, and load balancer where necessary.

## **Availability**

- The 3W-ADA Sentry system shall maintain at least 99.9% uptime 24 hours a day; this is necessary because it is the gateway to payment.
- The 3W-ADA must be enabled on the Account



## **Safety**

- No safety requirements have been identified between the merchant system and the 3W-ADA sentry system.

## **Security**

- All transaction data and communications between merchant systems to the card network through the 3W-ADA sentry system shall be encrypted using any cryptographic standard, for instance the Advance Encryption Standard (AES) of at least 128 bits and cipher block chaining (CBC) mode.
- System Administrators and Customer Service users with access to enrolment process, or enrollment directory or any interface used to manage enrolled cards requires strong login authentication system.
- System shall be able to kill session and logout user if system is idle for a certain time.
- Cardholder enrolling by himself through the public shall be authenticated with his card credentials before enrolment.
- After receiving three failed authentication attempts from merchant's shops, 3W sentry shall automatically suspend card's enrolment.
- System Administrators shall maintain security policy that covers the 3W-ADA sentry system.
- All access over hypertext transfer protocol (HTTP) shall be secured with Secure Socket Layer (SSL).
- Access to hosting server shall be well managed and controlled to make sure only the authorized users can access the server.
- Database shall be designed with security in mind to prevent unauthorised injection or modification of data.
- System production server shall be PCI compliant and vulnerability scan shall be performed at least once per quarter.
- Personal computers used by system administrators and customer service agents shall be free from virus and spyware, for instance, care shall be taken to scan the personal computers as often as possible.

## **Maintainability**

- System shall not be ambiguous or depend on any specific user, it shall be easy to be managed by any professional in a related field and shall be cross-platform.
- System shall be cost effective to manage and resources can be easily sourced locally.

## **Design Constraint**

- System shall be developed using a software development model and shall observe all standards.
- Coding shall be well commented to support the easy understanding and follow up by future programmers.

### **3.3.4.4 Interface Requirements**

#### **User Interface**

- The system shall support or be compatible with common web and mobile browsing applications, for instance, Internet Explorer, Netscape, Firefox, Google Chrome and Safari.

#### **Hardware Interface**

There is no hardware interface identified for the 3W ADA Sentry system.

#### **Software Interface**

- The System shall be able to communicate with the database system using structured query language (SQL).
- The System shall be able to communicate with the Enrollment Directory
- The System shall be able to communicate with the personal authentication code system.
- The System shall be able to communicate with the active SMS gateway.
- The System shall be able to communicate with the active mail server.

- The System shall be able to communicate with the merchant's systems through the application programming interface.
- The System shall be able to communicate with the payment network system through the application programming interface to request payment authorisation and receive response.
- The System shall be able to communicate with any cryptographic module that will enable it to decrypt or encrypt data.

### **Communication Interface**

The System shall be compatible with HTTP over internet, TCP/IP over intranet or dedicated line communication protocol.

## **3.4 3W-ADA Sentry System Design**

### **3.4.1 Introduction**

This section describes the integrated model of the 3W-ADA sentry system design requirements, environment, system and subsystem architecture of the modules, files and database design, input and out formats, application programming interfaces, processing logic, and external interfaces.

#### **3.4.1.1 Purpose and Scope**

The purpose of this section is to describe the architectural and technical design of the integrated model of the 3W-ADA Sentry to give a blueprint of how to develop software that meets the description of the 3W-ADA sentry system's software requirement specification using any choice of programming language.

The design described in this section is limited to the integrated model of 3W-ADA sentry system because this project aims to solve a problem of existing payment network with card account management system already in place. It serves as a guide to the programmers and software engineers at Paymenex Limited to enable them implement the required add-on on Paymenex TransNET since the researcher is not allowed to access the xTransNET platform.

#### **3.4.1.2 Audience**

This section is intended for administrators, development engineers and program managers at Paymenex Limited and anyone who wants to develop software that meets the software requirement specifications or to understand the system architecture.

#### **3.4.1.3 Project design executive summary**

This document section described the software design of the integrated model of a 3W-ADA Sentry system, a system that act as an enhancement or add-on module to an existing

card management and payment network by enabling a low-cost authentication features using the coordinated geometry.

The card management and payment network assigns a personal authentication code card or plane containing a layout of a coordinated geometry system extending vertically with Alphabets A – J, and horizontally with numbers 1 – 0 forming a 10 x 10 or 100 intersection points represented by randomly generated numbers, and standby to dynamic authenticate the card remotely using a unique randomly selected pair of the vertical and horizontal intersection points before granting access to payment. And the main objective is to prevent remote authentication vulnerabilities caused by using static authentication data.

It illustrates and describes the structural and behavioural components and tools required and provides a programming guideline in such a way that programmers can work with it to build a feasible prototype and main system, the component and guideline covered in this design section includes; system architecture, system database design, human – machine interface design, detailed software design, interface design.

#### **3.4.1.4 3W-ADA Sentry system design overview**

The system design overview described in the following diagram illustrates the design layout of an integrated model of 3W-ADA sentry and the Paymenex xTransNET.

The 3W-ADA sentry system sits between Paymenex TransNET and all third-party systems connecting to it through an application programming interface. However, this design section is limited to a third-party connections for online payment and data that passes the 3W-ADA Sentry to the payment network as illustrated in Fig.3.3-1 below and a connector.

The online payment section represents the merchant’s system connecting over an insecure internet network using the application programming interface.

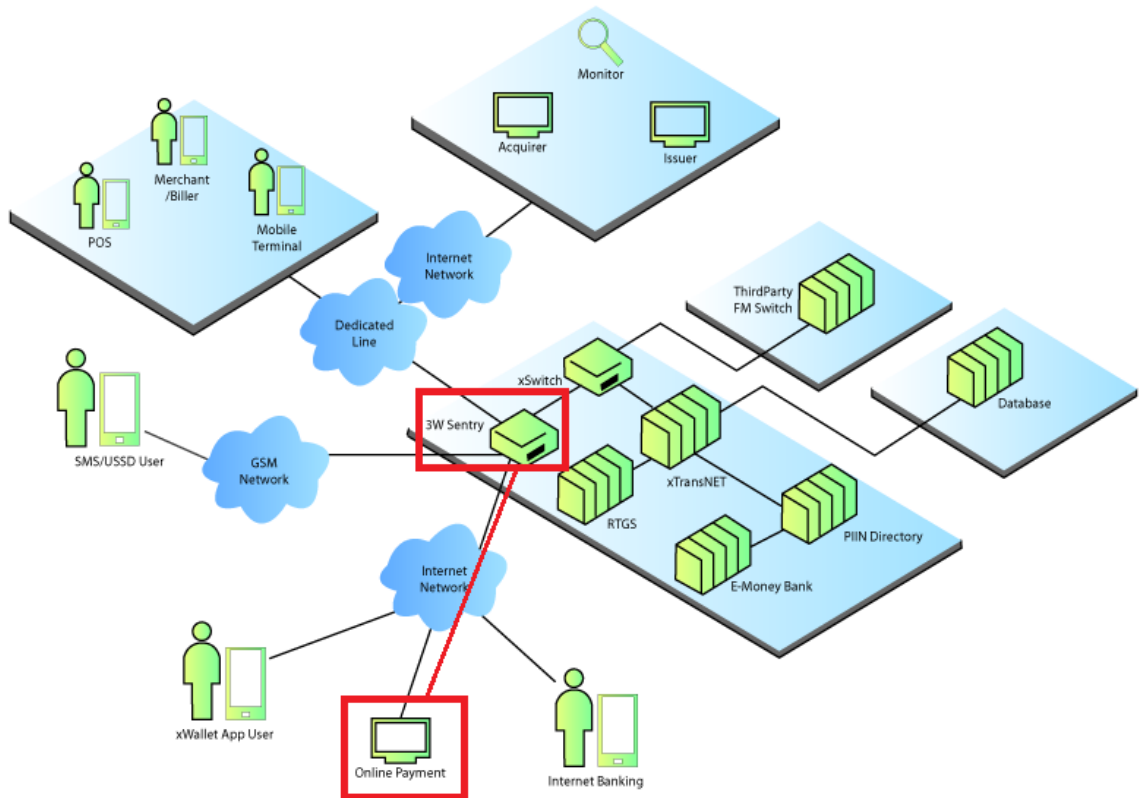


Figure 37: Integrated 3W-ADA Sentry environment in Paymenex TransNET

### 3.4.1.5 3W-ADA Sentry System design constraints

- Limited access to personally inspect the Paymenex TransNET platform.
- Limited access to the Card management system of Paymenex xTransNET.
- No access to the current database structure of Paymenex xTransNET.
- No access to modify codes in Paymenex TransNET.

### 3.4.1.6 Point of Contact

The point of contact for this project is Kingsley Chibuzor Aguoru, ACE Graduate School, University of East London, Docklands. London, United Kingdom.

Email: [kcaguoru@bcs.org](mailto:kcaguoru@bcs.org) Web: [www.kingsley.pro](http://www.kingsley.pro) or [u0840551@uel.ac.uk](mailto:u0840551@uel.ac.uk) .

Alternatively, contact the ACE Graduate School of the University of East London – United Kingdom [www.uel.ac.uk](http://www.uel.ac.uk)

### 3.4.1.7 Project References

Section 3.3 The 3W-ADA Sentry system software requirements specification.

### 3.4.1.8 Project Document Overview

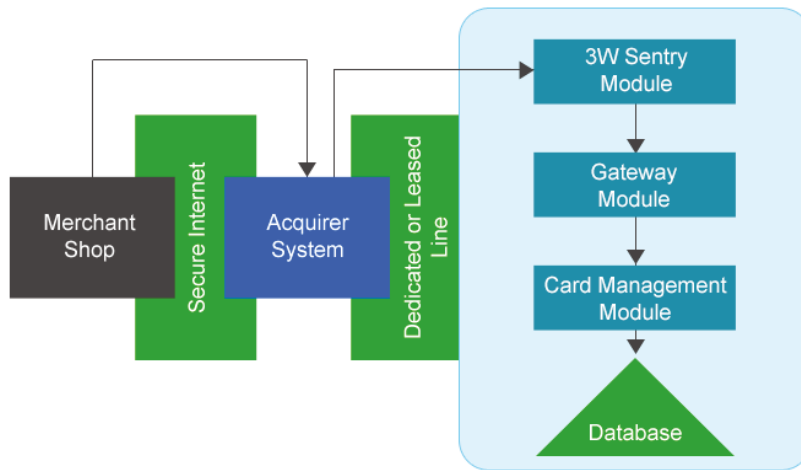
Section	Title	Description
3.3.1	Introduction	The purpose and scope of this project, as well as information about this document.
3.3.2	3W-ADA Sentry system Architecture and design	The system and/or subsystems architecture.
3.3.3	3W-ADA Sentry System Database design	The final design of all database management system (DBMS) files and the non-DBMS files associated with the system.
3.3.4	Detailed software and interface design	The information needed for a system development team to build and integrate the hardware components, to code and integrate the software modules, and to interconnect the hardware and software segments into a functional product.

*Table 17: Project design document overview*

### 3.4.2 3W-ADA Sentry system architecture and design

The software architecture and design is divided into two sections, the Paymenex TransNET section and the Merchant or Third-party section, both sections reside in

different locations and communicate with each other to complete the authentication process. The Paymenex TransNET is the payment processor with integrated 3W-ADA sentry system, while the Merchant or Third-party system is the merchant shopping cart with checkout facilities. Modification will be done at the merchant's checkout facilities to implement the Paymenex 3W-ADA sentry enabled payment authentication system.



*Figure 38: Paymenex TransNET 3W-ADA Sentry System Architecture*



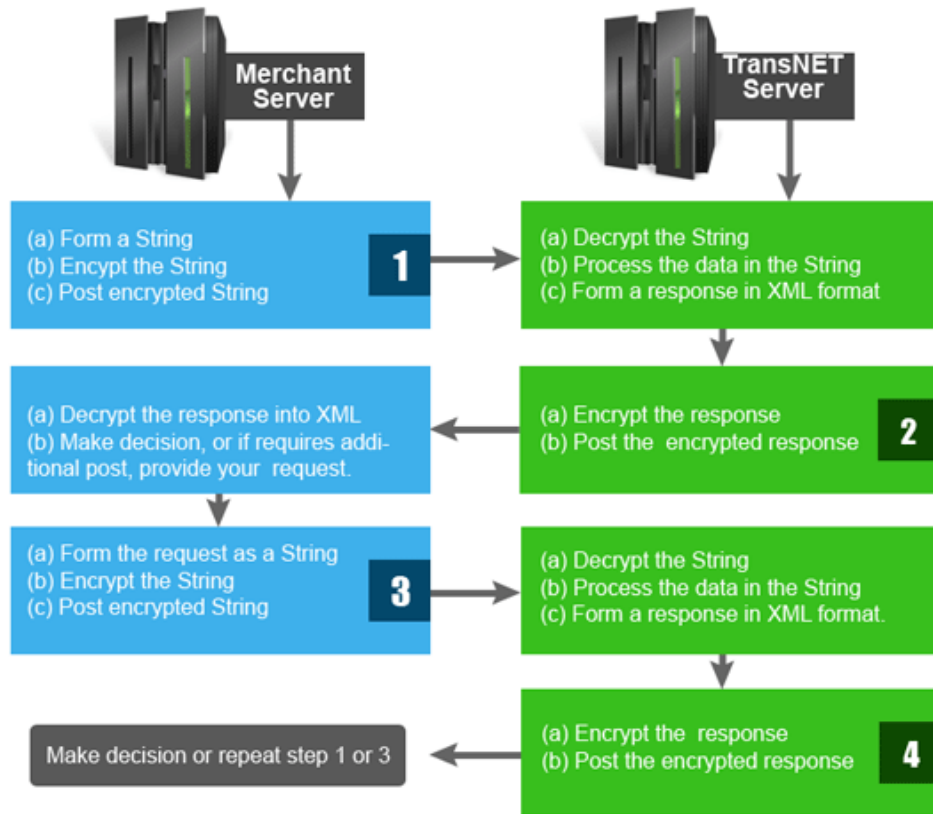


Figure 39: TransNET and Merchant's Systems communication flowchart

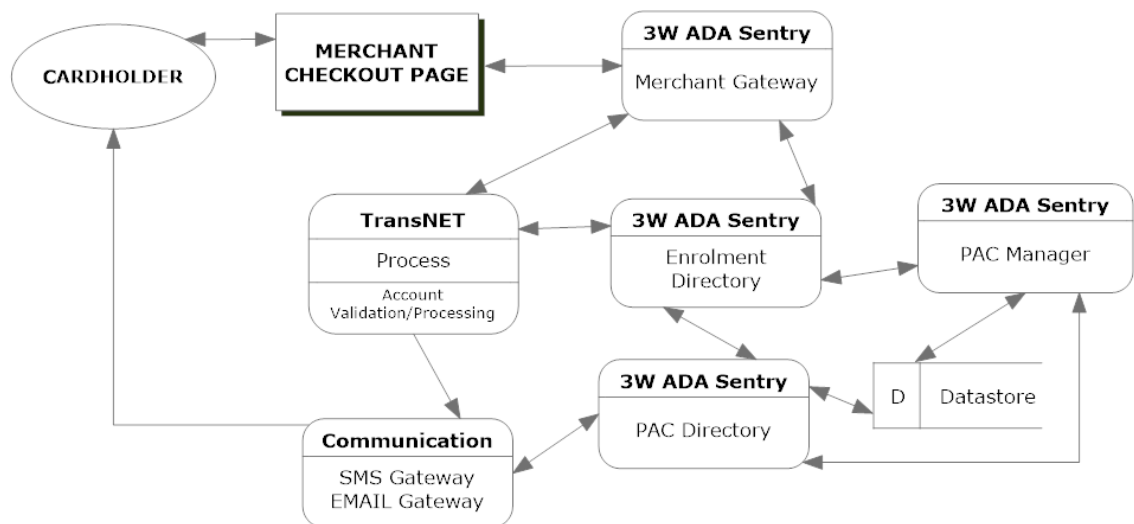


Figure 40: 3W-ADA Sentry dataflow

### 3.4.2.1 Design of 3W-ADA Sentry system on Paymenex TransNET

The description of the 3W-ADA sentry integration to Paymenex TransNET is presented using several unified modelling language (UML) diagrams and sample codes to provide a concept guideline to enable programmers at Paymenex Limited to complete the required update and integration at their end.

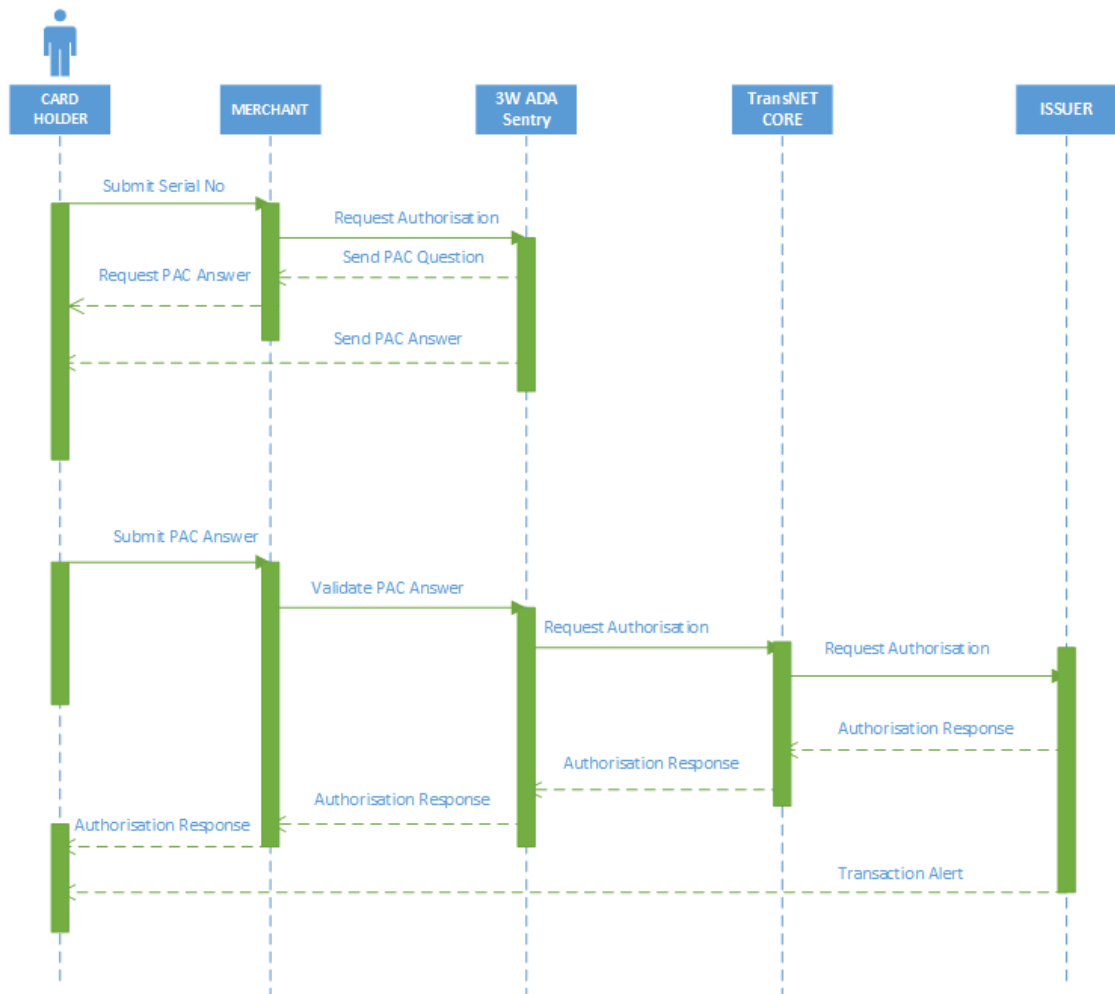


Figure 41: 3W-ADA Sentry Sequence diagram

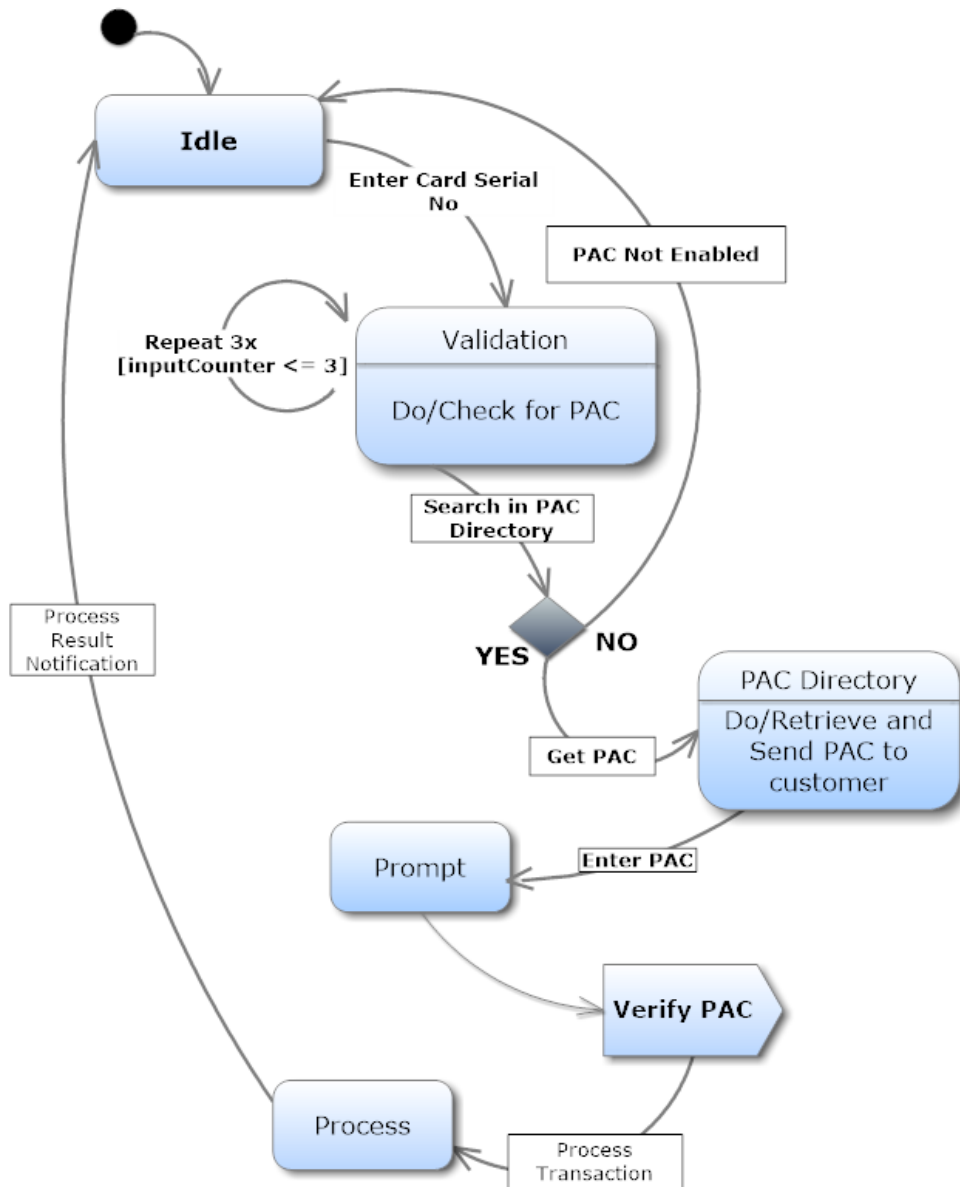


Figure 42: 3W-ADA Sentry Statechart diagram

### 3.4.3 3W-ADA Sentry System database design

The 3W-ADA Sentry integration requires 3 basic database tables.

- a) **Batch Table** (ev\_cord\_batch), this table contains the PAC batch grouping information according to the quantity, group, date, starting and ending, status of download and entire batch history.
- b) **PAC Serial No** (ev\_cord\_serial), this table contains serial numbers of the PAC Cards and their individual status.
- c) **Account Users** (ev-cord\_accuser), this table contains information about Card Accounts and their linked PAC card, including the status of the PAC card on a given card Account.
- d) **PAC Card** (ev\_cordinate), this table contains the information about the PAC coordinated values, including information about used values and active values.

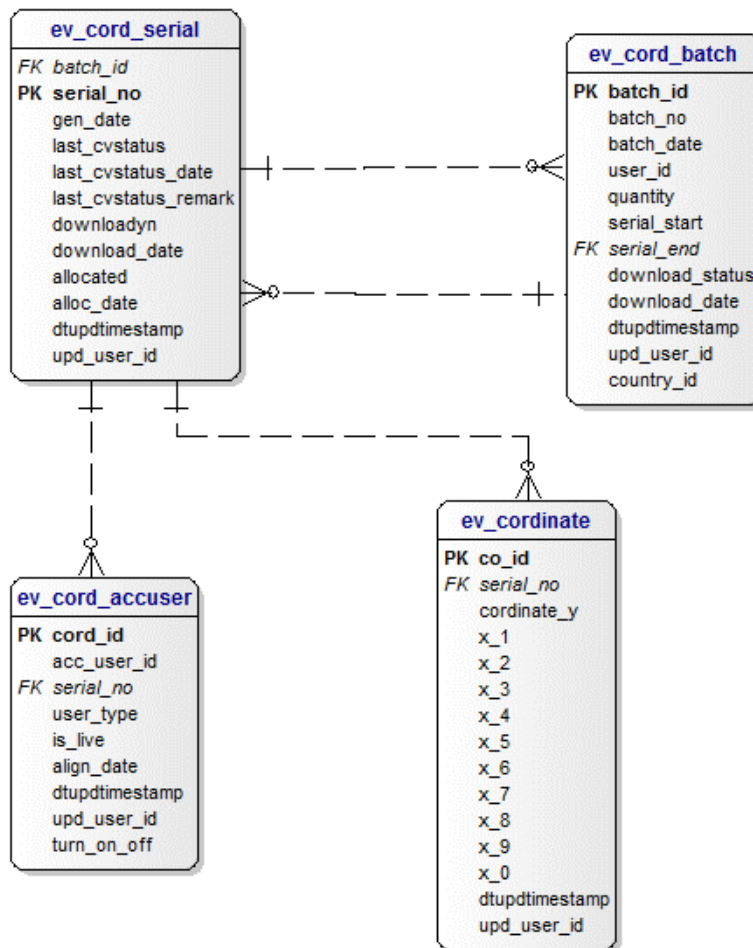


Figure 43: 3W-ADA Paymenex TransNET Entity Relationship Diagram

### **3.4.3.1 Database dictionary**

The database dictionary of the sample entity relationship diagram (ERD) above is presented in appendix A.

### **3.4.4 Detailed Software design**

#### **3.4.4.1 3W-ADA Sentry Paymenex module software design**

The following wireframe, design and the pseudocode described in **Appendix A** presented a blue print of how to integrate the 3W-ADA Sentry system in Paymenex TransNET.

#### **Wireframe UI design for the PAC Card production and initialization**

The following wireframe design illustrates the user interface used for PAC card production and management features.

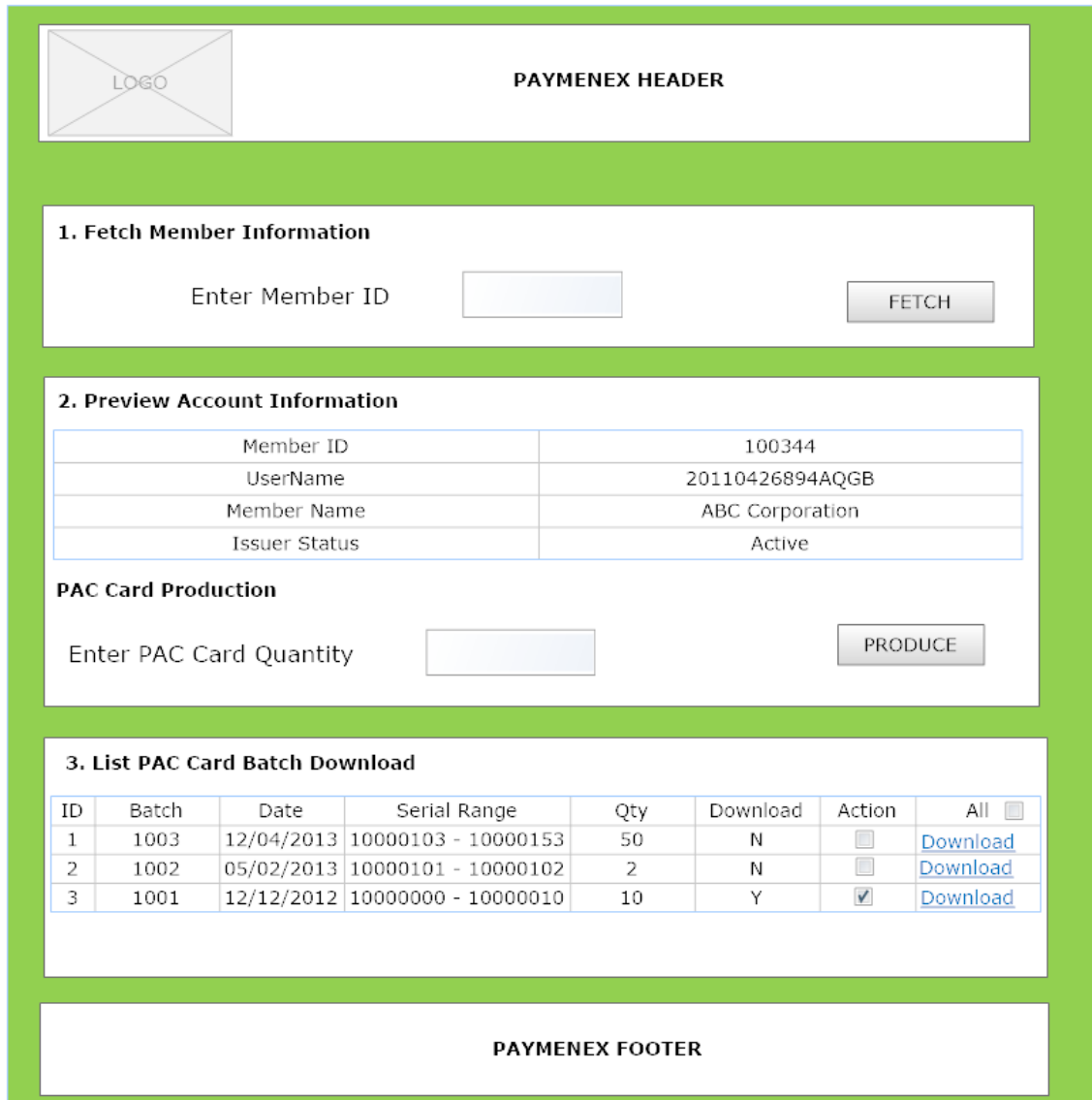


Figure 44: PAC Card Production and Management Wireframe design

### Wireframe UI Design for Link a PAC Card to a Paymenex Account

The following wireframe illustrates how to design the user interface used for linking a PAC card to a Paymenex card or Account.

LOGO

**HEADER**

**1. Fetch Account Information**

Enter Serial No

**2. Preview Account Information**

Serial No	12345678
Email Address	kcaguoru@gmail.com
Mobile No	(+44) 7447028000
Name	Kingsley Aguoru

**Link PAC to Account**

Enter PAC Serial No

**3. PAC Status and Information**

ID	Serial No	Date	Active	Turn On/Off
1	12345678	12/04/2011 14:30	N	
2	11124711	21/12/2011 09:23	N	
3	1002385	02/11/2013 11:34	Y	<input checked="" type="checkbox"/> <input style="width: 40px; height: 15px;" type="button" value="ON/OFF"/>

**FOOTER**

Figure 45: PAC Card Link wireframe design

### 3.4.4.2 3W-ADA Sentry merchant module software design

The implementation at merchant's shopping cart is done using a set of application programming languages as described below.

### 3.4.4.3 Merchant authentication parameter

The following table describes the merchant authentication parameters required to identify the merchant, its encryption keys on Paymenex TransNET, the values used within the parameters are configured and provided by Paymenex TransNET team.

Param Keys	Type	Values	Description
<b>p_merchant_id</b>	Number(10)	8-10 digit value	Paymenex TransNET's Merchant ID
<b>p_local_curr_code</b>	Varchar(3)	ISO Currency Code, i.e. GBP	Merchant Country Local ISO Currency Code
<b>p_country_name</b>	Varchar(30)	United Kingdom	Merchant Country Full Name
<b>izenid</b>	Number(10)	10 digit	Merchant's AES key identifier
<b>enc</b>	Varchar (3)	enc	Encryption data container
<b>Encryption Parameters [ Advanced Encryption Standard – 128 bit Method ]</b>			
<b>cipher</b>	Varchar	rijndael-128	3W-ADA Sentry uses Advanced Encryption Standard (AES – 128 bit) and AES (Rijndael) is new generation symmetric block cipher.
<b>mode</b>	Varchar(3)	cbc	Mode of operation is the procedure of enabling the repeated and secure use of a block cipher under a single key. <b>cipher-block chaining (CBC).</b>



<b>secret_key</b>	Number	16 digit	Encryption Secret Key for merchant issued by Paymenex
<b>iv_key</b>	Number	16 digit	Encryption IV Key or (Initialization Vector Key) issued by Paymenex.

*Table 18: Merchant 3W Sentry authentication parameter and description*

The above data table is used to handle the merchant identification, key identification, encryption and decryption processes.

Sample folder containing an AES decryption and encryption coding in PHP language is provided in **Appendix B**.

#### **3.4.4.4 Requesting transaction session ID**

The following table contains parameters required to initiate the first step of card authentication processing from the merchant's shop.

<b>Parameter</b>	<b>Type</b>	<b>Description</b>
<b>p_merchant_id</b>	Integer(10)	Merchant ID
<b>p_serial_no</b>	Number(10)	Paymenex Card or Account Serial No
<b>p_act_id</b>	VarChar(10)	Action Code, MTCON
<b>p_trans_cur</b>	Char(3)	the transaction currency
<b>p_order_no</b>	VarChar(25)	Order No generated from your system
<b>p_remark</b>	VarChar(25)	Any other remark
<b>p_country_name</b>	Char(20)	Full Name of Merchant's country of location

<b>P_local_curr_code</b>	Char(3)	Merchant Local Currency in ISO standard, i.e. GBP or USD.
--------------------------	---------	---

Table 19: Merchant Interface step one parameter and description

The Serial No parameter will be an input from the customer at merchant’s checkout page.

Product Name	Model	Quantity	Price	Total
<a href="#">MacBook</a>	Product 16	10	\$2.50	\$25.00
<a href="#">Samsung Galaxy Tab 10.1</a>	SAM1	1	\$1.74	\$1.74
			<b>Sub-Total:</b>	\$26.74
			<b>Flat Shipping Rate:</b>	\$1.00
			<b>Total:</b>	\$27.74

**Paymenex Direct**

Serial No:	<input type="text" value="11124711"/>
<input type="button" value="Confirm Order"/>	

Figure 46: Merchant interface – step one wireframe

When “Confirm Order” is clicked, the merchant system should be able to collect required values and parameters relevant to the post and for an NVP string as

shown below in 3.4.4.5.

**3.4.4.5 Parameter string**

*p\_serial\_no=11124711&p\_amount=10.57&p\_trans\_cur=GBP&p\_order\_no=563734&p\_remark=ACEUEL&p\_merchant\_id=100000155&p\_local\_curr\_code=GBP&p\_country\_name=United Kingdom&p\_act\_id=MTCN*

The next step is to encrypt the above string using the AES encryption values, mode, keys, in HEX format. And when encrypted the result will be a mixture of lowercase alphabets and numbers similar to the following;

d9134cba1f2609a8cc85d38eabb01c2c2070c05be8ec3fe4b5b64ae7a69b8ee1f17ec3a5f36233980d07a7a1528239b062de598caaeafe823b3649c4a8b2d73ac9ab6f770ee2bd6ff890112257cc60078e645f6e2b

Now we are ready to post the encrypted data to Paymenex TransNET by forming an NVP string in an URL POST using the “*izenid*” as the identifier and the parameter “*enc*” as the encryption data container.

<https://paymentURLPath/processingfile?izenid=1234567890&enc=9134cba1f2609a8cc85d38eabb01c2c2070c05be8ec3fe4b5b64ae7a69b8ee1f17ec3a5f36233980d07a7a1528239b062de598caaeafe823b3649c4a8b2d73ac9ab6f770ee2bd6ff890112257cc60078e>

#### 3.4.4.6 Response from Paymenex TransNET

Paymenex TransNET will use the “*izenid*” received to search the key directory for matching secret and IV keys, and will attempt to decrypt the encrypted data in the container, if successful, then, it will proceed to read the string for the “*p\_merchant\_id*”, and will again match the value contained in the decrypted file with that stored against the keys in the key directory.

Next is to process the request and return the following sample of XML back to merchant’s system.

```
<?xml version="1.0" encoding="utf-8" ?>
<TRANS_NET>
<REQUEST_ID>13897</REQUEST_ID>
<REQUEST_DATE>2013-09-29 15:08:35.0</REQUEST_DATE>
<RESPONSE_CODE>001</RESPONSE_CODE>
<RESPONSE_REASON>
<SUCCESS>100</SUCCESS>
</RESPONSE_REASON>
```

```

<CATALOG>
<CARDDATA>
<P_MODE>L</P_MODE>
<P_PIN_ONE><![CDATA[First]]></P_PIN_ONE>
<P_PIN_TWO><![CDATA[Fifth]]></P_PIN_TWO>
<P_PAC_CODE_ONE><![CDATA[G7]]></P_PAC_CODE_ONE>
<P_PAC_CODE_TWO><![CDATA[B1]]></P_PAC_CODE_TWO>
<TRANS_SESSION_ID><![CDATA[zlkzwtbcl73XO6nh]]></TRANS_SESSION_ID>
<VAL_CARD_EXP>Y</VAL_CARD_EXP>
<TRANS_AMOUNT>17.820</TRANS_AMOUNT>
<PROCESS_AMOUNT>10.570</PROCESS_AMOUNT>
<TRANS_CURR><![CDATA[GBP]]></TRANS_CURR>
<PROCESS_CURR><![CDATA[GBP]]></PROCESS_CURR>
<CONVER_RATE>1.000</CONVER_RATE>
</CARDDATA>
</CATALOG>
</TRANS_NET>

```

**Table 20:** Merchant interface step one response XML

Merchant system will parse the XML into an html form for the customer, the form will be similar to the following user interface.

Paymenex Direct

Conversion Rate: 1 GBP = USD 1.557



Total Debited Amount: GBP 17.82

Serial No:	<input type="text" value="11124711"/>
Card No:	<input type="text" value="6001110232933158"/>
First Digit of WebKey:	<input type="text" value="8"/>
Fifth Digit of WebKey:	<input type="text" value="5"/>
PAC G7:	<input type="text" value="309"/>
PAC B1:	<input type="text" value="921"/>
Card Expiry Date:	<input type="text" value="December"/> / <input type="text" value="2017"/>

Figure 47: Merchant interface – step two wireframe

The customer is expected to enter his card number, Webkey, PAC answers, expiry date and submit the form to complete his transaction.

When the form is submitted, the merchant system should form the second string as follows using the information submitted by the customer.

```
p_serial_no=11124711&p_card_no=6001110232933158&p_pin_one=8&p_pin_two=5&p_pac_code_one=309&p_pac_code_two=921&p_card_exp_month=12&p_card_exp_year=2017&p_trans_session_id=zlkzwtbcl73XO6nh&p_merchant_id=100000155&p_local_curr_code=GBP&p_country_name=United Kingdom&p_act_id=MTPAY
```

To complete the transaction, the above string should be encrypted and posted to Paymenex URL, this will enable 3W-ADA sentry to validate the card holder for legitimacy, if it went well, the 3W-ADA sentry will pass the payment instruction over to payment network or processor for processing.

#### **3.4.4.7 Database design**

The merchant's module of the 3W-ADA Sentry system requires no database element, however, the existing database of the shop should be used to store payment transaction details, for instance, payment status, amount, time and date paid, and payment method used.

### 3.5 3W-ADA Sentry User Acceptance Test (UAT)

#### 3.5.1 Introduction

This section of this research document presents a descriptive plan of the user acceptance testing of the 3W-ADA Sentry System by the software testers in real world with all business representatives to verify that the system actually solved the problem to an acceptable level in accordance with the business requirement and fit for purpose.

#### 3.5.2 Purpose

The aim of this User Acceptance Test is to ascertain that the 3W-ADA Sentry system meets the owner's business requirement as outlined in the problem statement provided.

The purpose of the user acceptance testing is to measure if the 3W-ADA sentry system can support day-to-day business and prevent card-not-present fraud or abuse and ensure the system is fit for business usage.

#### 3.5.3 Role and Responsibilities

Position	Responsibilities	Name	Company
Project Manager	Communication with user to agree on format and scope of UAT. Agreement of acceptance criteria with the users prior to commencing UAT.	Philip Oscar	Paymenex Limited
Management	Responsible for allocating sufficient resources, experienced personnel, infrastructure, time and budget	Jennifer Ijeoma Vikram Bawne	Paymenex Limited
Administrator	Administration	Alharazi Moe	Paymenex Canada Inc.

Test Lead	<p>Ensure that the full detailed test plan is available for test users.</p> <p>Ensure that any bugs identified during UAT are recorded properly.</p> <p>Ensure testing takes place within agreed timeframes.</p> <p>Administers the deployment of resources to provide the best recommendation to Paymenex management or Board.</p>	<p>Kennedy Richard</p> <p>Jennifer Ijeoma</p> <p>Kingsley Aguoru</p>	<p>Paymenex Limited</p> <p>Paymenex Limited</p> <p>ACE University of East London</p>
Testers	<p>Execute test cases to ensure the application performs at an acceptable level and in line with the SRS. Documentation of all testing results.</p>	<p>Raphael Tawiah</p> <p>Kwaku Ofosuhene</p> <p>Michael Kwablah</p> <p>Tabiri Boakye</p> <p>Sydney Mathabatha</p>	<p>Vodafone Ghana</p> <p>Vodafone Ghana</p> <p>Vodafone Ghana</p> <p>Vodafone Ghana</p> <p>Multichoice South Africa</p>
Developer	<p>Responsible for supporting UAT with resources, infrastructure and correction of errors and fix bug</p>	<p>Kingsley Aguoru</p>	<p>ACE University of East London</p>

*Table 21: UAT role and responsibilities*

### 3.5.4 Testers and Participants

It is fundamental that the testing participants or testers should include representatives from all areas involved in the card-not-present systems at Paymenex Limited and its



member Acquirers or Issuers to validate the system's functions before going live in production, based on this requirements, the best personnel for the UAT testing are:

- Personnel at Paymenex Limited who are directly impacted by the upcoming system and business process changes.
- Proposed frequent users of the 3W-ADA sentry solution.
- Selected individuals with a sound understanding of business processes in the areas they represent.
- Individuals with the necessary time to commit to this endeavour.
- Willing to experiment (to try various methods to see what works and what does not work).
- Patient and have a tolerance for ambiguity.

<b>Participant/Tester Name</b>	<b>Company/Department</b>	<b>Area of testing</b>
Tabiri Boakye	Vodafone Ghana	Merchant's shopping cart implementation, Testing as legitimate Cardholder.
Raphael Tawiah	Vodafone Ghana	Merchant's shopping cart implementation, Testing as legitimate Cardholder.
Kwaku Ofosuhene	Vodafone Ghana	Merchant's shopping cart implementation, Testing as illegitimate Cardholder.
Michael Kwablah	Vodafone Ghana	Merchant's shopping cart implementation, Testing as illegitimate Cardholder.
Sydney Mathabatha	MultiChoice South Africa	Merchant's shopping cart implementation, Testing as both legitimate and illegitimate Cardholder.

Moe Alharazi	Paymenex Canada Inc.	Paymenex TransNET 3W-ADA Sentry Card enrollment and management module
Loius Ruggier	UseMyServices Inc. Canada	Merchant's shopping cart implementation, Testing as both legitimate and illegitimate Cardholder.
Vikram Bawne Mangesh Regundawar	Paymenex Limited	Paymenex TransNET 3W-ADA Sentry Card enrollment and management module.
Della Porbley	Paymenex Ghana Limited	Paymenex TransNET 3W-ADA Sentry Card enrollment and management module.

*Table 22: Testers and Participants*

### 3.5.5 Testing Schedules

Activity /Operation	Lead Responsibility	Date
Testers Identification and Select for UAT.	Kingsley Aguoru	15 /05/ 2012
Establish/Develop test scenarios and script/cases.	Kingsley Aguoru	15/ 05/ 2012
Validates participant's availability for testing.	Kingsley Aguoru	15/05/2012
Review scenarios/scripts for accuracy, completeness and sequence (confirm test data is correct)	Kingsley Aguoru/ Paymenex Technical Team	15/05/ 2012

Ensure all software/hardware and other resources required for UAT environment are configured for testing.	Kingsley Aguoru / Paymenex Technical Team	15/05/2012
UAT Environment validation	Kingsley Aguoru / Paymenex Technical Team	15/05/2012
Testing by UAT Participants	Testing Participants	15/05/2012
Recording and Documentation or reports	Testing Participants	15/05/2012

*Table 23: Testing Schedule*

### **3.5.6 Test Requirements**

- Testing of the 3W-ADA sentry system will initially be carried out at Paymenex head office and Vodafone Ghana head office, alternatively, some testers may choose to perform some testing from their regular personal computers where possible. Test results must still be coordinated with others.
- The date of the User Acceptance Test will be 18/05/2012 and shall be communicated to all parties.
- Identified testing participants shall receive all testing instructions prior to the start of testing.
- Testing materials, for instance, card, mobile phone shall be provided and organizers shall make sure that are in working condition.

#### **3.5.6.1 Types of Testing**

The testing carried out in this research is to show the functionalities and sequential process of the 3W-ADA sentry system on a system prototype, since the prototype is not designed for a production environment, the testing will be a ‘Black-Box’ type of testing

which directs its testing activities on the functionalities of the solution as oppose to ‘White-Box’ testing which looks into the internal structure of the solution.

However, while developing and implementing 3W-ADA sentry system for production the ‘Gray-Box’ testing should be used to make sure both functionalities and codes are securely and adequately implemented, the gray-box testing means testing both the functionalities and codes of the 3W-ADA sentry system.

### **3.5.7 Test Environments**

The testing environment for the 3W-ADA sentry system is online, and the 3W -ADA sentry merchant module.

### **3.5.8 Test Perspectives**

Testers shall also test in both legitimate and illegitimate perspectives. The legitimate perspective will act as a legitimate owner of the payment card, and the mobile no linked to it. The illegitimate perspective will act as fraudsters who will be in possession of the card details only but without the mobile phone and or PAC card of the account.

### **3.5.9 3W-ADA Sentry Test Cases**

#### **3.5.9.1 3W-ADA Sentry Paymenex TransNET Module Test Cases**

##### **I. Paymenex card Enrolment**

<b>TEST CASE</b>	<b>Paymenex Card Enrolment to 3W-ADA Sentry program</b>
<b>Test Case ID</b>	<b>TC-01</b>
<b>Purpose /Feature</b>	Enrolling Paymenex card to the 3W-ADA Sentry system for dynamic authentication during card-not-present transaction.

<b>Pre-Condition</b>	The Paymenex card must be validated, activated, active, and not expired. Mobile phone number is registered with the card.						
<b>Flow of Event/Process</b>	1) Enter the serial number of payment card and fetch account status. 2) Enter PAC serial number and click align to Link PAC to Payment card serial number.						
<b>Expected Result</b>	PAC card is successfully linked to enter payment card serial number.						
<b>Result</b> (Tick as applicable)	Passed	<b>YES</b>	Failed	<b>NO</b>	Incomplete	<b>No</b>	
<b>Remark/Reason / Comment</b> <i>(attach extra sheet if applicable)</i>							

Table 24: Test Case - Paymenex card enrolment

## II. Disable PAC feature on a card

TEST CASE	Disable PAC feature on a card
<b>Test Case ID</b>	<b>TC-02</b>
<b>Purpose /Feature</b>	Disable PAC feature on a Paymenex card.
<b>Pre-Condition</b>	The Paymenex card must be validated, activated, active, and not expired. PAC card is already linked to the payment card's serial number.

<b>Flow of Event/Process</b>	1) Enter serial number of payment card and fetch account status. 2) On the Turn Off/On column, uncheck the checkbox to disable PAC feature. 3) Click on ON/OFF to save changes.					
<b>Expected Result</b>	PAC card features are successfully disabled from payment card.					
<b>Result</b> (Tick as applicable)	Passed	<b>YES</b>	Failed	<b>NO</b>	Incomplete	<b>No</b>
<b>Remark/Reason / Comment</b> <i>(attach extra sheet if applicable)</i>						

Table 25: Test Case – Disable PAC feature on a card

### III. Re-enable PAC feature on a Card

<b>TEST CASE</b>	<b>Re-enable PAC feature on a card</b>
<b>Test Case ID</b>	<b>TC-03</b>
<b>Purpose /Feature</b>	Re-enable PAC feature on a Paymenex card.
<b>Pre-Condition</b>	The Paymenex card must be validated, activated, active, and not expired. PAC card is already linked to the payment card’s serial number.
<b>Flow of Event/Process</b>	1) Enter Serial Number of payment card and fetch account status. 2) On the Turn Off/On Column, Check the checkbox to re-enable PAC feature. 3) Click on ON/OFF to save changes
<b>Expected Result</b>	PAC card features are successfully re-enabled from payment card.

<b>Result</b> (Tick as applicable)	Passed	<b>YES</b>	Failed	<b>NO</b>	Incomplete	<b>No</b>
<b>Remark/Reason / Comment</b> <i>(attach extra sheet if applicable)</i>						

Table 26: Test Case – Re-enable PAC feature on a card

### 3.5.9.2 3W ADA Sentry Merchant interface Test Case

<b>TEST CASE</b>	<b>Payment with a Paymenex card</b>
<b>Test Case ID</b>	<b>TC-02</b>
<b>Purpose /Feature</b>	Using Paymenex card to make payment online on the merchant interface with 3W-ADA Sentry solution.
<b>Pre-Condition</b>	The Paymenex card must be validated, activated, active, with sufficient balance, and not expired. Mobile phone number must be able to receive SMS or customer is holding the corresponding PAC card.
<b>Flow of Event/Process</b>	<ol style="list-style-type: none"> <li>1) Open the merchant payment interface.</li> <li>2) Enter your card's Serial number or mobile number.</li> <li>3) On the next page, enter your card details as asked, including card No, Webkey, Expiry Date, PAC response and submit payment.</li> </ol>
<b>Expected Result</b>	The expected result is divided into two sections.

	<p><b>1) Legitimate Tester Result</b></p> <p>When Serial number is submitted, the 3W-ADA sentry system module installed in Paymenex TransNET will identify the enrolled PAC card and send two random PAC question by SMS to the mobile number registered with the card Serial, And when the cardholder enters the card details and PAC response on step two, if they are valid, the 3W-ADA Sentry module in Paymenex TransNET will validate the account and pass it on to Paymenex TransNET for authorisation.</p> <p><b>2) Illegitimate Tester Result</b></p> <p>When Serial Number is submitted, the 3W-ADA sentry system module installed in Paymenex TransNET will identify the enrolled PAC card and send two random PAC questions by SMS to the mobile number registered with the card serial, and because the illegitimate tester is not in possession of the mobile number or the PAC card registered with the card Serial no, he cannot be able know the PAC response, and he try to guess the PAC response, but the 3W -ADA sentry system module cannot be able to validate the response, and on third attempt, the 3W-ADA sentry will lock the account for suspicion of fraud, Transaction will not be completed.</p>						
<b>Result</b> (Tick as applicable)	Passed	<b>YES</b>	Failed	<b>NO</b>	Incomplete	<b>No</b>	
<b>Remark/Reason / Comment</b> <i>(attach extra sheet if applicable)</i>							

Table 27: Test Case – 3W Sentry Merchant interface



### **3.5.10 Test Assumptions**

- The User Acceptance Test environment will be available.
- Personal Computers with internet access and good browser will also be available.
- Mobile phone number with mobile network connection available in country of testing.
- Paymenex card, duly validated, with expiry date valid until after the testing schedules.
- All Paymenex cards to be used for testing are correctly enrolled in the 3W-ADA sentry system with assigned PAC serial numbers.
- All Paymenex cards have sufficient balance for related testing.
- The business team has reviewed and accepted functionalities identified in the business requirements and software requirements documents.
- Code walkthroughs and reviews will be completed by the development team, though this will serve as guide for production related development.
- Unit testing will be completed by the development team prior to release to the test team.
- Testers will test what is documented in the software requirements specifications.
- All Servers and networks related to the Paymenex TransNET and 3W-ADA sentry systems are running at least 99% uptime.
- All changes to software requirements specifications shall be communicated to the test team.

### **3.5.11 Test Risks**

There is no risk identified for this user acceptance testing, this is because all testing will be carried out on Paymenex TransNET demonstration server.

### **3.5.12 Acceptance and Acknowledgments**

During the testing, recommendations were presented which specifically relates to the incorrectness, or incompleteness of the 3W-ADA Sentry system, but the only concern

with its enhancement and updated responses to this recommendation is presented on **Appendix C**, and the Acceptance Matrix on **Appendix D**.

## **4. PART 4 – 3W-ADA VERIFICATION AND VALIDATION**

### **4.1 Introduction**

This section describes the verification and validation of the 3W-ADA Sentry system.

The verification phase carried out checks to confirm that the system developed fulfils or is in line with the software requirements specification through the evaluation of the development lifecycle drawn from feasibility, specification requirements, design, coding, testing and implementation organized using a checklist or walkthrough document.

The validation phase presents the strategies used to confirm that the project meets user's requirement and accepted by the client as a solution to the reported problem.

#### **4.1.1 Purpose**

The purpose of the verification and validation of this project is to confirm that the system developed and delivered is in line with the software specification requirements and also meets the use's requirements or is fit for purpose.

### **4.2 3W-ADA Sentry System Verification**

#### **4.2.1 System Feasibility**

The appropriateness and feasibility of the 3W-ADA Sentry System was checked through the analysis and evaluation of the problem reported by the stakeholder and compared against the discoveries of this research, this helped to identify the causes of the problem and provided a blueprint of the framework used to produce the solution.

In a follow up, feasibility study was carried out on the proposed solution to confirm the suitability, possibility and relevance of the system and the outcome reveals that, since the problem is majorly caused by using static information for payment in card-not-present environment, and the system proposed to use a known analytical geometry concept to apply dynamism into the process, it is then evidential that this process will remove the causes of the problem.

## 4.2.2 System development cycle

The development process of the 3W-ADA Sentry System was carried out using the waterfall system development model comprising series of sequential development phases and iteration to maintain a check throughout the process, the development process was monitored with the system development checklist.

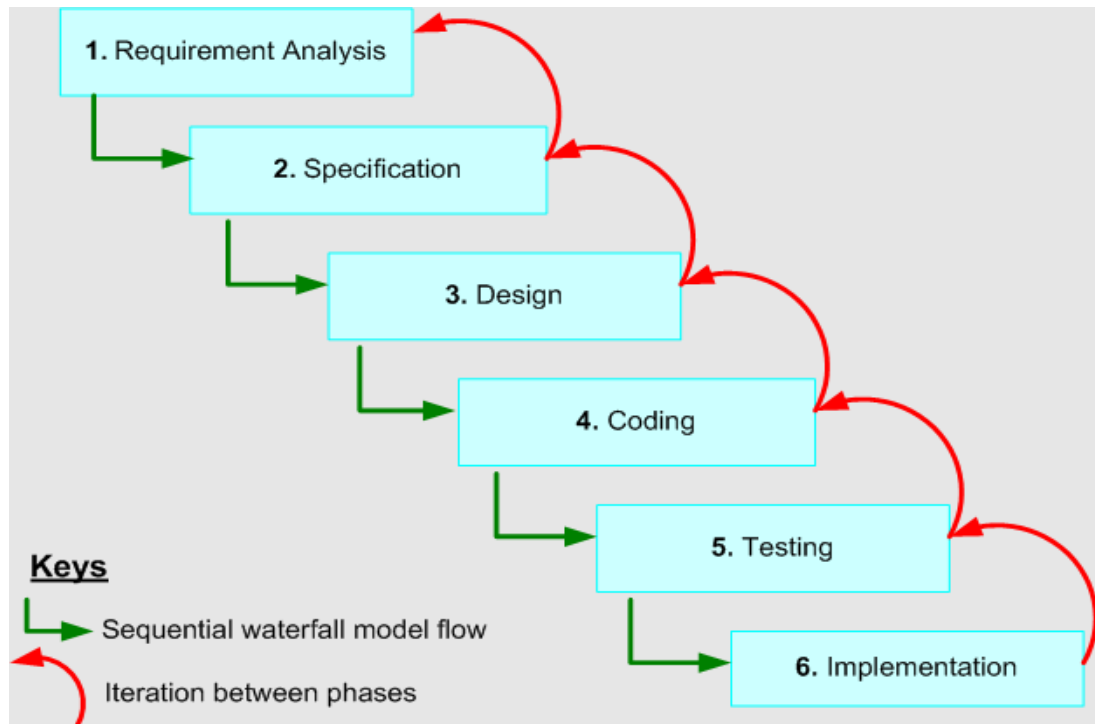


Figure 48: Waterfall Development process with iteration (Aguoru, 2007)

### Requirement Analysis

Analysis of the problem statement and review of literatures, journals, empirical investigation to establish a clear understanding of the problem and requirement.

### Specification

Documentation of the requirements specification including the functional and system requirements, design and relevant information to support development.

## **Design**

Documentation of the architectural design diagrams, including user interfaces, usecase, flowchart and data structure.

## **Coding**

Coding of the merchant module using relevant technologies and environments, and providing a development guideline for the enhancement requirements for the stakeholder's system.

## **Testing**

Testing of the components and application programming interface using functional type of testing.

## **Implementation**

Installation of the 3W-ADA Sentry system enhancement and deployment to live system.

### **4.2.3 System Development Checklist**

The 3W-ADA Sentry system development checklist is a comprehensive list of predefined tasks extracted from the phases of the waterfall model used in system development as a guideline of tasks to be checked, noted, implemented or consulted. The system development milestone and development checklist are predefined guideline to quality because they help in progress monitoring, decision making, prioritization, resources and development efforts management as an important tasks throughout the development phase.

The following table describes the sequential activities carried out to support the system verification and acceptance processes.

Activity	Responsible Personnel
Described the criteria and condition of acceptance.	Paymenex Limited Board and Business Analyst, QA Staffs
Identify and plan for verification and validation activities necessary to support acceptance criteria of the 3W-ADA Sentry System	Paymenex Limited Board and Business Analyst, QA Staffs, Researcher, Selected Paymenex Members.
Complete the 3W-ADA Project's milestone.	Paymenex Technical Team and Researcher.
Certify the completion of any required verification and validation activities for the project deliverables through testing	Researcher.
Schedule and conduct a User acceptance meeting for approvers and testers for a User acceptance testing with respect to their acceptance criteria.	Paymenex Technical Team, Researcher, Administrators

*Table 28: 3W-ADA Sentry System checklist roles*

#### **4.2.4 System Acceptance Criteria**

The 3W-ADA Sentry system is checked through user acceptance testing to confirm that it meets users' requirement. The acceptance criteria presented in this section describes the processes and conditions of reviews carried out to confirm the acceptance of the 3W-ADA Sentry system.

The acceptance criteria described in below table outlined the criteria and conditions under which the approval team, the project owner and the researcher agreed to accept that the project is complete and business requirement fulfilled.

Milestone	Deliverable	Acceptance Criteria
Problem Statement	Problem statement analysis and documentation	The proposal shall seem feasibly possible and within the resources allowance of the company.
Software Requirements Specification Complete	Software Requirements Specification documentation.	<p>The Software Requirements Specification describes the functionalities of the 3W-ADA Sentry System and includes:</p> <ul style="list-style-type: none"> <li>▪ Business requirements and process</li> <li>▪ Use cases</li> <li>▪ Functional requirements</li> <li>▪ Non-functional requirements</li> </ul> <p>The Researcher and the sponsor’s business and technical team has reviewed the specification and its requirements for completeness, feasibility correctness, and consistency with the problem statement.</p> <p>The sponsor’s technical team has reviewed the SRS and its integration requirements to Paymenex TransNET and crosschecks all necessary possible risks involved and analyse the impact of the integration to the existing system.</p>
Software Design Specification Complete	Software Design Specification Documentation	<p>The design documents describes the architectural and technical design of the integrated model of the 3W-ADA sentry to give a blueprint of how to develop software that meets the description of the 3W-ADA sentry system’s software requirement specification using any choice of programming language.</p> <p>The sponsor’s technical team has reviewed the specification design to ensure that all requirements relating the integrated model of the 3W-ADA Sentry system as contained in the SRS documents are represented, well understood and the team has the</p>

Milestone	Deliverable	Acceptance Criteria
		expertise to implement the module necessary for Paymenex TransNET.
Software Ready for Testing and Release	Software User Acceptance Testing and documentation	<p>For user acceptance testing, the completed 3W-ADA Sentry system software was delivered with all recommendations, changes fully completed and it passed through all acceptance testing scenarios with no severity.</p> <p>Acceptance testers agree that the application can move into pilot program and provision made for bug fixing.</p> <p>The 3W-ADA Sentry Paymenex TransNET module has been moved from the test environment to the production environment with all test data removed and is functioning correctly.</p>

*Table 29: 3W-ADA Sentry User Acceptance Criteria*

### 4.3 3W-ADA Sentry System Validation

The validation process of the 3W-ADA Sentry system is divided into three sections of authentication criteria.

#### 4.3.1 Acceptance Validation

The 3W-ADA Sentry acceptance matrix describes the summary of all phases of the acceptance criterion and their results as described in **Table 27**, and details of the Acceptance Matrix document is presented in **Appendix D** of this document.



### 4.3.2 Operational Validation

The operational validation is derived from the user acceptance testing result and the approval of the stakeholder and user acceptance team as shown in the sign off document of the log of system UAT recommended changes provided in **Appendix C**.

### 4.3.3 Performance Validation

Since completion of the user acceptance testing and the acceptance of the solution by Paymenex Limited, the 3W-ADA Sentry system has been their main card-not-present solution recommended for Paymenex members worldwide. Since then, a popular implementation was done for Vodafone Ghana for their Airtime Swipe Card project which enables customers to buy airtime and also shop online with their airtime swipe card.

According to (Vodafone Ghana, 2012) *“All Vodafone Cards are enabled for the 3W Sentry Card security, this means at each authentication session, you will be asked some information from your PAC Card, this information can also be sent to your registered mobile phone no. This security technology increases the chance of protecting your card from un-authorized access. Paymenex strongly recommends all Cardholders to use this FREE service. Fraudulent activities or loss arising in an account that would have been avoided by the use of the 3W Sentry Card security tool will be entirely the responsibility of the cardholder”*. A business case study of Vodafone Ghana which includes how the 3W-ADA Sentry supported their operations is presented in **Appendix E** of this document.

## 5. PART 5 – CONCLUSION

### 5.1 Thesis Summary

This research project described the process and scenarios of an investigation and research carried out to establish the causes and consequences of card-not-present fraud, its impact and a solution. Systematically organized in five principal parts as follows:

**Part One:** This part covers the introduction of the research context. After reading this chapter, reader will be equipped with the research question, purpose scope and approach, including the overview of the research motivation, what others has done in this research area, and what this research will contribute to the knowledge.

**Part Two:** This part described the background of this research and information from the literature review concerning what people have written about this research area. It further explored the e-commerce technologies and their factors with much focus on card payment. After reading this chapter, reader will be able to understand the background of the problem this research relied on, the current situation of the problem including the causes and consequences, the e-commerce technologies, how they work, their benefits, their problems and overview of its development. It further analyzed the context of related card fraud, the infiltration processes and their consequences.

**Part Three:** This chapter presents the 3W-ADA Sentry system as a low-cost and non-electronic solution built using the framework of the Cartesian coordinate system to add additional dynamic authentication method during card-not-present transaction. After reading this chapter, reader will be able to understand what 3W-ADA Sentry system is all about, its concepts, process and benefits, it further covers the development process and cycle, design and user acceptance test.

**Part Four:** This chapter validates and evaluates the 3W-ADA Sentry system for its suitability and fit for the purpose. After reading this chapter, reader will be able to understand the validation process and acceptance criteria used to validated the 3W-ADA Sentry system before acceptance.

**Part Five:** This chapter refreshes the reader's memory about the content and limitation of this research. After reading this chapter, reader will be able to understand the content of this thesis and its limitations, solution provided, its justifications, strength and weaknesses, and direction for future research on this domain.

## **5.2 Limitations**

This thesis described the analysis of the card-not-present transaction process, method, fraud infiltration processes and the vulnerabilities in existing fraud solutions for card-not-present transactions, as a means to understand the nature of the business case of Paymenex Limited. This also guided the literature review process and area of research, in order to understand the causes and consequences of card-not-present fraud, which remains the principal and focal topic of this thesis. To provide a comprehensive and sound analysis, other types of card frauds or payment methods are used as reference in this research.

The research outcome provided a blueprint for a feasible solution proposed to solve the problem of Paymenex Limited. The solution developed comprises of a pair of system modules, one residing on the merchant shopping cart and the other integrated with Paymenex TransNET, and both communicate through the application programming interface. The researcher designed and implemented the merchant module and the API.

Because of access restrictions, the researcher could only provide guided descriptions and illustrations to enable the technical team at Paymenex to implement the 3W-ADA Sentry system functionality on their platform.

## **5.3 Contribution summary of this thesis**

Throughout the concept of this thesis, the author identified the following main contributions to knowledge as follows:

### **5.3.1 Philosophy of identity theft and card-not-present fraud**

This research project examines the trace of identity theft as the major cause of card-not-present fraud from a biblical version when physical stealing was virtually the only method of identity theft, and how the development of information and communication technology and the trend of electronic commerce introduced additional anonymous and low-risk routes to identity theft which inspired and led to a significant exploitation of technologies. And as the development continues to strengthen, the social engineering technologies used to support this crime transforms equally into a sophisticated and flexible tool.

### **5.3.2 A framework work for academic scrutiny and future research**

E-commerce technologies is largely software and internet based, and the quality assurance of every piece of software developed requires a continuous process of monitoring, maintenance and validation throughout its life cycle to remain in compliance and fit, additionally, the evolution of e-commerce technologies and its phenomenon is becoming more dynamic, complex, and sophisticated, therefore e-commerce technologies requires continuous research, evaluation and innovation to update or upgrade previous knowledge, results and solutions that may no longer be valid so that they can be current and fit for purpose. This piece of research validated the card-not-present fraud causes, consequences, and solutions in line with the current technology trend.

Previous research also showed that card-not-present transaction fraud and its solutions escaped academic scrutiny, while it is understood that solutions or clues to solutions to a problem is usually the result of an academic research investigation, the card-not-present transaction, related fraud and solutions lacks satisfactory knowledge in the academic domain and hence stands as a huge problem for new researchers working on this area. However, this research incorporated business profession and academic environment into its research development and produced a piece of academic research which will serve as a background for future academic research on card-not-present transactions fraud, causes, and consequences.

### **5.3.3 Introduction of a non-electronic and low-cost CNP Fraud solution**

This research recognised the present of existing solutions, though with significant indications why the existing solution could not adequately solve the problem, while some of these solutions are effective to certain level, some are also very expensive to implement, manage, and cause dissatisfaction to users, but this research proposed the 3W-ADA Sentry system, a new non-electronic and low-cost account dynamic authentication system using the Cartesian two-dimensional coordinate logic to solve the problem of card-not-present fraud and it is accepted by the sponsor.

## **5.4 Conclusion**

Card-not-present fraud continues to be a serious threat to online merchants and a leading security issue among card association, issuers and acquirers. Several solutions have been introduced and tested by card associations and different organisations both in and outside the card payment industry, however, all approaches could not effectively tackle the fraud arising from card-not-present transactions.

The more solutions that are developed and introduced, the more technologies to thwart and exploit the solutions emerges. Many online merchants have disappeared from e-commerce business or turned to accept alternative payment methods that eliminates traces of card payment because they could no longer tolerate the losses arising from card-not-present fraud. The issuers and acquirers could not provide a reliable and trusted solution that could guarantee and reassure the online merchant's safety, instead they continue to promote and campaign for weak solutions which tends to pass a wrong signal to businesses who are planning to introduce electronic commerce in their business offerings.

Existing merchants are greatly encouraged by leading card association to continue to use a weak solution such as 3D secure at the consequences of the merchants.

Developers of technologies used to thwart or exploit card-not-present fraud prevention solutions are as experienced and strong as the developers of the solution and this has led to the establishment of a sort of technology competition between both sides.

Alternative payment methods are fast growing and substantively competing with card payments in the online environment because the merchants have adopted alternative payment methods for its assurance of not having any sort of chargeback, while customers are happy with alternative payment method because it conceals and protects their personal information from online identity theft threats.

Law enforcement agencies are concentrating more on the drive for arrests and prosecution of card-not-present fraud offenders, wide publicity of the fraud threat, education about related measures to protect parties online, but they failed to concentrate on the research and development of reliable solutions.

The card association has been happy with a recent reduction in card-not-present losses in the last years as they experienced a three consecutive years of fraud reduction in United Kingdom which made all involved to relax and believe that finally a solution has been discovered, but the fight is still on and getting stronger. However, the recent increase in card-not-present fraud report for the year 2012 disappointed all the stakeholders and renewed the fear of card-not-present fraud because many now believe that the previous information about a solution solved is simply a camouflaged of a weak solution.

## **5.5 Future research direction**

This research presented a series of findings about the causes of card-not-present transaction fraud and the related consequences to the parties involved as a guide to future research in this domain, it also added to current academic knowledge of this problem and attempted to solve the problem with a low cost solution.

The major cause of card-not-present transaction fraud is attributed to identity theft, including all motivations of identity theft, because if there is no avenue or method to steal personal and card details belonging to others and impersonating them in the card-not-present environment, there will definitely be no card-not-present transaction fraud, therefore, future research in this area will continue to concentrate on more tackling identity theft.

### **5.5.1 Trend and causes of card-not-present fraud**

Future research at any point in time should consider the evolution of electronic commerce technologies, the complexity, the exploitation and its techniques, this is because technology is a dynamic innovative tool that changes with the time and human ideas, and it is likely that every piece of well researched work will contribute to knowledge and help to well inform the stakeholders of the current trend at the time of research.

### **5.5.2 Concealing Sensitive information**

Researchers should find more feasible and reputable methods or advance existing methods of identifying ourselves online which at the same time will conceal our personal and card information.

### **5.5.3 More research on dynamic authentication method**

For any future card-not-present transaction fraud solution to be effective and reliable, it should continue to prevent the use of only static information for its authentication model, because identity theft techniques used on card-not-present transaction environment rely on capturing personal and card details as static data and using them to commit card-not-present fraud since these data can be replicated without losing its reliability.

It is believed that using a new dynamic keyword for each online transaction will prevent the effects of identity theft and will positively disable and renders all methods and systems used to steal sensitive information worthless, hence researchers should find more effective and universal ways to design unique authentication model for online card payment. This research used a non-electronic and low-cost method to determine its unique token for each authentication through the implementation of the Cartesian two-dimensional coordinate system.

### **5.5.4 Additional Research Recommendation**

There has been a widespread of tokenization usage in accessing online banking especially by financial institutions in United Kingdom, where electronic devices are used to generate a one-time token to authorize an online payment or login to an account. Because every

bank use and promote their own device, a customer with multiple accounts from different bank will have multiple devices to carry along, which makes the concept to be ambiguous, dissatisfactory and expensive.

This research therefore recommends the adoption of the 3W ADA Sentry System and moving it to a further research scrutiny and developing it as a membership authentication framework allowing financial institutions, card association and payment companies to join the network to enable them offer a universal, cross-platform, and low-cost dynamic authentication system that will enable customers to maintain only one authentication system for all types of payment cards or financial accounts irrespective of number of providers.



## 6. BIBLIOGRAPHY

- Abdelhamid, N., Ayes, A. & Thabtah, F., 2014. Phishing detection based Associative Classification data mining. *Expert Systems with Applications*, 41(13), pp. 5948-5959.
- Abraham, S. & Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), pp. 183 -196.
- Abrazhevich, D., 2004. *Electronic Payment Systems: a User-Centred Perspective and Interaction Design*. Eindhoven: Technische Universiteit.
- Aguoru, K. C., 2007. *Information Security flaws in e-commerce payment authentication: The impact on card-not-present transaction in United Kingdom*, Liverpool, UK: s.n.
- Ahmad, W., 2008. 'Is Credit Card Fraud a Real Crime? Does it Really Cripple the E-Commerce Sector of E-Business?'. s.l., s.n., pp. 364-370.
- Aljawarneh, S., Dababneh, M., Hossey, H. & Alwadi, E., 2010. *A Web Client Authentication System Using Smart Card for e-Systems: Initial Testing and Evaluation*. St. Maarten, IEEE, pp. 192-197.
- Altinkemer, K. & Wang, T., 2011. Cost and benefit analysis of authentication systems. *Decision Support Systems*, 51(3), pp. 394 - 404.
- Anderson, J. B. & Johansson, R., 2006. *Understanding Information Transmission*. Hoboken(NJ): John Wiley & Sons.
- Anderson, K. B., Durbin, E. & Salinger, M. A., 2008. 'Identity Theft'. *Journal of Economics Perspectives*, 22(2), pp. 171-192.
- Anderson, R., 2008. *Security Engineering, A Guide to Building a Dependable Distributed*. Indiana(Indianapolis): Wiley Publishing Inc..
- Andress, J., 2011. *The basis of Information Security: Understanding the fundamentals of InfoSec in theory and Practice*. Waltham(MA): Elsevier Inc.

Anumba, C. J. & Ruikar, K., 2002. Electronic commerce in construction—trends and prospects. *Automation in Construction*, 11(3), pp. 265 - 275.

APACS, 2005. 'The definitive overview of plastic card, cheque and online banking fraud – and measures to prevent them'. *Fraud The Facts 2005*, Issue 2006, pp. 6-9.

APACS, 2010. 'The definitive overview of plastic card, cheque and online banking fraud – and measures to prevent them'. *Fraud The Facts 2010*, pp. 5-10.

APACS, 2012. 'The definitive overview of plastic card, cheque and online banking fraud – and measures to prevent them'. *Fraud The Facts 2007*, pp. 6-10.

Archer, N. et al., 2012. *Identity Theft and Fraud: Evaluating and Managing Risk*. 2012 ed. Ottawa(ON): University of Ottawa Press.

Asokan, N., Janson, P. A., Steiner, M. & Waidner, M., 1997. The state of the art in electronic payment systems. *Computer*, 30(9), pp. 28 - 35.

Australian Competition & Consumer Commission, 2013. *ScamWatch*. [Online] Available at: <http://www.scamwatch.gov.au/content/index.phtml/tag/CardSkimming> [Accessed 21 August 2013].

Australian Institute of Criminology, 2011. *Australian crime: Facts & Figures*, Canberra: Australian Institute of Criminology.

Australian Payments Clearing Association, 2013. *Payments fraud in Australia declines in 2012*, Sydney: APCA.

Awasthi, A. K., 2004. Comment on A dynamic ID-based Remote User Authentication Scheme. *Transaction on Cryptology*, September, 01(02), pp. 15-17.

Baxter, W. F., 1983. 'Bank Interchange of Transactional Paper: Legal and Economic Perspectives'. *Journal of Law and Economics*, 26(3), pp. 541-588.

Beatty, P., Reay, I., Dick, S. & Miller, J., 2011. Consumer trust in e-commerce web sites. *ACM Computing Surveys*, 43(3)(Fall 2011), p. 14.

Bella, G., Paulson, L. C. & Massacci, F., 2002. *'The verification of an industrial payment protocol: the SET purchase phase'*. New York, NY, USA, ACM, pp. 12-20.

Bharat, B., 2013. *Electronic Commerce: Framework, Technologies and Applications*. 4 ed. New Delhi(Delhi): McGraw Hill Education (India) Private Limited.

Bhasker, B., 2006. *Electronic Commerce: Framework, Technologies' and Applications*. Second Edition ed. New Delhi: McGraw-Hill Publishing Company Limited.

Bhattacharyya, S., Jha, . S., Tharakunnel, K. & Westland, C. J., 2011. Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50(3), pp. 602-613.

Bidgoli, H., 2006. *Handbook of Infromation, Security, Threats, Vulnerabilities, Prevention, Detection, and Management*. 3 ed. Hoboken(New Jersey): John Wiley & Sons.

Biegelman, M. T., 2009. *Identity Theft Handbook: Detection, Prevention, and Security*. 2009 ed. Hoboken(New Jersey): John Wiley & Sons.

Bohn, N. & Mason, S., 2010. 'Identity and its verification'. *Computer Law & Security Review*, 26(1), pp. 43-51.

Botha, J., Geldenhuys, P. & Bothma, C. H., 2008. *Managing E-commerce in Business*. Wetton(Cape Town): Juta and Company Ltd.

Bowonder, B. & Miyake, T., 1992. Creating and sustaining competitiveness: Information management strategies of Nippon Steel Corporation. *International Journal of Information Management*, March, 12(1), pp. 39-56.

Bryan-Low, C., 2011. 'Cybercrime Costs Mount in U.K.'. *Wall Street Journal*, 17 February.

Buckland, M. K., 1991. *Information and Information Systems*. Westport(CT): Greenwood Publishing Press.

Bushry, M., 2005. *E-Commerce*. New Delhi: Firewall Media (Laxmi Publications).

Canadian Anti-Fraud Centre, 2013. *Financial Crime Trend Bulletin: Payment Card Fraud* 2013-03-08. [Online]

Available at: [http://www.antifraudcentre-centreantifraude.ca/english/Bulletin%202012-03\\_Payment%20Card%20Fraud.html](http://www.antifraudcentre-centreantifraude.ca/english/Bulletin%202012-03_Payment%20Card%20Fraud.html)

[Accessed 17 August 2013].

Card Technology Today, 2002. 'Card not present fraud'. *Card Technology Today*, 14(7-8), pp. 11-13.

Cheswick, W. R., Bellovin, S. M. & Rublin, A. D., 2003. *Firewalls and Internet Security: Repelling the Wiley Hacker*. Boston(MA): Addison Wesley.

Computer Fraud & Security, 1999. Hackers, crackers and phreakers oh my!. *Computer Fraud & Security*, December, 6(6), pp. 16 - 19.

Computer Fraud & Security, 2005. Forty million credit card numbers hacked: Could be biggest breach of financial data ever. *Computer Fraud & Security*, 2005(1), pp. 1 -2.

Cresson Wood, C., 2003. Effective information system security with password controls. *Computers & Security*, January, 2(1), pp. 5 - 10.

Crossley, J., 2009. 'Credit Card Fraud'. *Credit Management*, pp. 26-27.

Das, M. L., Saxena , A. & Gulati, V. P., 2004. A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*, May, 50(2), pp. 629-631.

Davenport, L. & Cronin, B., 1988. Strategic information management: Forging the value chain. *The Journal for Information Professionals*, March, 8(1), pp. 25-34.

Donnelly, A., 2000. 'Online credit card fraud outpaces physical world'. *Computer Fraud & Security*, 2000(10), p. 9.

Drake, P. & Heath, L., 2011. *Practitioner Research at Doctoral Level: Developing Coherent Research Methodologies*. Abingdon(Oxon): Routledge.

E-finance & payments, Law & Policy, 2012. Pat Carroll CEO at ValidSoft on UK Card fraud figures and security challenge. *The Newsletter for the Financial Services Industry*, March, 06(03), p. 07.

Eisenstein, E. M., 2008. Identity theft: An exploratory study with implications for marketers. *Journal of Business Research*, November, 61(11), pp. 1160-1172.

Elderawy, M. H. et al., 2012. Mobile one-time passwords: two-factor authentication using mobile phones. *Security and Communication Networks*, 5(5), pp. 508-516.

Erbschloe, M., 2004. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. 2005 ed. Burlington(MA): Elsevier Butterworth-Heinemann.

Europol, 2012. *Situation Report: Payment Card Fraud in the European Union*. [Online] Available at: [https://www.europol.europa.eu/sites/default/files/publications/1public\\_full\\_20\\_sept.pdf](https://www.europol.europa.eu/sites/default/files/publications/1public_full_20_sept.pdf) [Accessed 17 August 2013].

Fengtong, W. & Xuelei, L., 2012. An improved dynamic ID-based remote user authentication with key agreement scheme. *Computers & Electrical Engineering*, March, 38(2), pp. 381-387.

Financial Fraud Action UK, 2009. 'The definitive overview of payment industry fraud'. *Fraud The Facts 2009*.

Financial Fraud Action UK, 2013. *Fraud the Facts 2013*, London: The UK Cards Association.

Financial Fraud Action UK, 2014. *Fraud the Facts 2014*, London: The UK Card Association.

Furnell, S., 2006. 'Safety in numbers? Early experiences in the age of chip and PIN'. *Computer Fraud & Security*, 2006(4), pp. 4-7.

Gamal, T. E., 1985. '*A public key cryptosystem and a signature scheme based on discrete logarithms*'. New York, Springer-Verlag, pp. 468-472.

- Ghosh, S. & Reilly, D. L., 1994. *Credit card fraud detection with a neural-network*. Wailea, Proceedings of the Twenty-Seventh Hawaii International Conference on, pp. 621 - 630.
- Gifford, N., 2009. *Information Security: Managing the legal risks*. s.l.:CCH Australian Limited.
- Giot, R., El-Abed, M., Hemery, B. & Rosenberger, C., 2011. Unconstrained keystroke dynamics authentication with shared secret. *Computers & Security*, 30(6), pp. 427-445.
- Giot, R., EL-Abed, M. & Rosenberger, C., 2009. *Keystroke Dynamics Authentication For Collaborative Systems*. Baltimore, IEEE, pp. 172-179.
- Glazer, R., 1993. Measuring the Value of Information: The Information intensive organisation. *IBM System Journal*, 32(1).
- Gold, S., 2014. The evolution of payment card fraud. *Computer Fraud & Security*, 2014(3)(2014), pp. 12-17.
- Gonzales, A. R. & Majoras, D. P., 2007. Combating identity theft: A Strategic Plan. *The President's Identity Theft Task Force*, pp. 9-10.
- Grance, T., Stevens, M. & Myers, M., 2010. *Guide to Selecting Information: Recommendations of the National Institute of Standards and Technology*, Gaithersburg: NIST Special Publication.
- Gunasekaran, A., Marri, H. B., McGuaghey, R. E. & Nebhwani, M. D., 2002. E-commerce and its impact on operations management. *International Journal of Production Economics*, 75(1-2), pp. 185 - 197.
- Hamid, I. R. A. & Abawajy, J. H., 2014. An approach for profiling phishing activities. *Computers & Security*, 45(September), pp. 27-41.
- Herreweghen, E. V., 2000. *'Non-repudiation in SET: Open Issues'*. London, UK, Springer-Verlag, pp. 140-156.

- Hinde, S., 2005. 'Identity theft & fraud'. *Computer Fraud & Security*, 2005(6), pp. 18-20.
- Hoffman, S. K. & McGinley, G. T., 2010. *Identity Theft: A Reference Handbook*. Santa Barbara(California): ABC-CLIO.
- Holzmuller, H. H. & Schluchter, J., 2002. Delphi study about the future of B2B marketplaces in Germany. *Electronic Commerce Research and Applications*, 1(1), pp. 2 - 19.
- HSN Consultants Inc., 2013. The Nilson Report. August.2013(1023).
- Hu, J. et al., 2004. An empirical study of audience impressions of B2C web pages in Japan, China and the UK. *Electronic Commerce Research and Applications*, 3(2), pp. 176 - 189.
- Hunter, P., 2004. 'Chip and PIN – biggest UK retail project since decimalisation, but not enough on its own to defeat card fraud'. *Computer Fraud & Security*, 2004(5), pp. 4-5.
- Hunter, P., 2006. 'Relentless pace of Internet trade in stolen credit card details continues'. pp. 14-16.
- Huston, B., 2009. 'Identity Theft on Campus'. *Black Enterprises*, 40(5), p. 39.
- Hwang, J.-J., Yeh, T.-C. & Li, J.-B., 2003. Securing on-line credit card payments without disclosing privacy information. *Computer Standards & Interfaces*, 25(2), pp. 119 - 129.
- I-En, L., Cheng-Chi, L. & Min-Shiang, H., 2005. *Security enhancement for a dynamic ID-based remote user authentication scheme*. s.l., IEEE, p. 4.
- Jansen, W., Steenbakkens, W. & Jaegers, H., 2007. *New Business Models for the Knowledge Economy*. 2007 ed. Aldershot(Hampshire): Gower Publishing Limited.
- Joyce, R. & Gupta, G., 1990. Identity authentication based on keystroke latencies. (stream of latency periods between keystrokes). *Communications of the ACM*, Feb, 33(2), p. 168.

- Juang, W. & Wu, J., 2009. Two efficient two-factor authenticated key exchange protocols in public wireless LANs. *Computers and Electrical Engineering*, 35(1), pp. 33-40.
- Kahate, A., 2003. *Cryptography and Network Security*. New Delhi: Tata McGraw-Hill.
- Kaminsky, J. S., 2000. Humor and the Theology of Hope: Isaac as a Humorous Figure. *Interpretation*, 54(4), pp. 363 - 375.
- Kim, C., Tao, W., Shin, N. & Kim, K.-S., 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9(1)(2010), pp. 84-95.
- Kruegel, C. & Kirda, E., 2006. Protecting Users against Phishing Attacks. *The Computer Journal*, 30 January, 49(5), pp. 554-561.
- Kuo, P.-J., Hsi, K.-H. & Yu, H.-C., 2002. 'Electronic payment systems: an analysis and comparison of types'. *Technology in Society*, 24(3), pp. 331-347.
- Lamport, L. & Ashenurt, R., 1981. Password authentication with insecure communication. *Communications of the ACM*, November, 24(11), pp. 770-772.
- Laudon, K. C. & Traver, C. G., 2004. *E-Commerce: Business Technology, Society*. Boston(MA): Addison-Wesley.
- Liao, I.-E., Lee, C. & Hwang, M., 2006. A password authentication scheme over insecure networks. *Journal of Computer and System Sciences*, 72(4), pp. 727-740.
- Li, X. et al., 2013. A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. *Mathematical and Computer Modelling*, 58(1-2), pp. 85-95.
- Li, Y. & Zhou, J., 2010. *Radio Frequency Identification System Security: RFIDsec'10 Asia Workshop Proceedings*. 2010 ed. Amsterdam: IOS Press BV.
- Lomax, S., 2006. 'Securing the eCommerce revolution: safeguarding Internet transactions. *Card Technology Today*, 18(6), pp. 9-10.



- Maconachy, V. W., Schou, C. D., Ragsdale, D. & Welch, D., 2001. *A Model for Information Assurance: An Integrated Approach*. West Point New York, IEEE, pp. 306 - 310.
- Manzoor, S. A., 2008. *E-Commerce Technology and Management*, Chennai: Centre for Distance Education.
- Masters, B. & Boxell, J., 2011. 'Bill for 'rising tide' of economic crime soars to pound(s)38bn'. *Financial Times*, Issue 3, p. 2.
- Matejkovic, J. E. & Lahey, K. E., 2001. 'Identity theft: no help for consumers'. *Financial Services Review*, 10(1-4), pp. 221-235.
- Maxwell, M. J., 1972. Skimming and Scanning improvement: the needs, assumptions and knowledge base. *Journal of Literacy Research*, March, 5(1), pp. 47 - 59.
- McKay, S. C. & Piazza, C. J., 1992. EDI and X12: What, why, who?. *Serials Review*, 18(4), pp. 7-10.
- Mohapatra, S., 2012. *E-Commerce Strategy: Text and Cases*. New York(New York): Springer.
- Molla, A. & Licker, P. S., 2005. 'eCommerce adoption in developing countries: a model and instrument'. *Information and Management*, 42(6), pp. 877-899.
- Montague, D. A., 2011. *Essentials of online payment security and fraud prevention*. Hoboken(New Jersey): John Wiley and Sons Inc..
- Murdoch, S. J. & Anderson, R., 2010. *Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication*. Tenerife, Spain, IFCA, pp. 337-340.
- NCSA, 2009. *A long way in all directions; National Center for Supercomputing Application*, Illinois: NCSA.
- Network Security, 2000. 43% of credit card fraud not reported. *Network and Security*, 2000(10), p. 4.

- Nieschwietz, R. J. & Kaplan, S. E., 2003. 'A Web assurance services model of trust for B2C e-commerce '. *International Journal of Accounting Information Systems*, 4(2), pp. 95-114.
- Nirshan, P., 2000. 'Fighting fraud'. *Risk Management*, 47(3), p. 9.
- Ofcom, 2011. *Communications Market Report: UK*, s.l.: Ofcom.
- Office for National Statistics, 2010. 'Internet Access - Households and Individuals'. *Statistical Bulletin*, pp. 13-18.
- Omer, A. A., 2007. *Mutual Authentication Protocols for RFID Systems*, Tulsa: ProQuest.
- Palvia, P., 2009. 'The role of trust in e-commerce relational exchange: A unified model'. *Information & Management*, 46(4), pp. 213-220.
- Patidar, R. & Sharma, L., 2011. Credit Card Fraud Detection Using Neural Network. *International Journal of Soft Computing and Engineering*, 1(NCAI2011), p. 34.
- Paymenex Limited, 2012. *About Paymenex*. [Online] Available at: <http://www.paymenex.com/about-paymenex-united-kingdom> [Accessed 01 July 2012].
- Paymenex Panama LLC., 2013. *Account Security and Protection*. [Online] Available at: <http://www.paymenex.com/pa/accountsecurityandprotection> [Accessed 19 August 2013].
- Philippsohn, S. & Thomas, S., 2003. E-Fraud - What Companies Face Today. *Computer Fraud & Security*, January, 2003(1), pp. 7 -9.
- Porters, M. E. & Millar, V. E., 1985. How Information Gives you Competitive Advantage. *Harvard Business Review*, Jul-Aug.
- Quigley, M., 2005. *Information Security & Ethics: Social & Oragnizational issues*. London(England): IRM Press.

- Rainer, K. R. & Cegielski, C. G., 2011. *Introduction to Information System*. Danvers(MA): John Wiley & Sons Inc..
- Rocco, E., 1998. *Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact*. New York, ACM Press/Addison-Wesley Publishing Co, pp. 496 - 502.
- Rodriguez, B., 2009. 'The cyber-crime threat to online transactions'. *Network Security*, 2009(5), pp. 7-8.
- Scarrott, G. G., 1985. Information, the life blood of organisaton. *The Computer Journal*, 28(3), pp. 203 - 205.
- Schultz, C., Kaplan & Jeremko, C., 2007. *Shortcut Geometry*. New York: Kaplan Publishing.
- Semmens, N., 2002. *The fear of plastic card fraud*, Sheffield, UK: British Library.
- Sharma, A. K., 2005. *Co-Ordinate Geometry*. New Delhi: Discovery Publishing House.
- Shaw, M. J., Blanning, R. W., Whinston, A. B. & Strader, T. J. eds., 2000. *Handbook on Electronic Commerce*. s.l.:Springer Verlag.
- Smith, R. G., 1997. *Plastic Card Fraud*, Canberra: Australian Institute of Criminology.
- Smith, R. G., n.d. *Cyber Crime Research*, Cranberra: Australian Institute of Criminology.
- Song, R., Korba, L. & Yee, G., 2007. *Trust in E-Services: Technologies, Practices, and Challenges*. Ronggong Song ed. Hershey(PA): Idea Group Publishing.
- Strebe, M., 2002. *Network Security JumpStart: Computer and Network Security Basics*. 2002 ed. Alameda(CA): Sybex Inc.
- Suh, B. & Han, I., 2003. The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce*, 7(3), pp. 135 - 161.

Sullivan, R. J., 2010. The changing nature of U.S. card payment fraud: industry and public policy options. *Economic Review (Kansas City)*, 95(2)(Spring 2010), p. 101.

Systems and software engineering, 2011. Content of life-cycle information products (documentation)," ISO/IEC/IEEE 15289:2011(E). *IEEE Xplore*, 94(November), p. 1.

Trupti, H. G. & Manisha, D., 2012. Remote Client Authentication using Mobile phone generated OTP. *International Journal of Scientific and Research Publications*, 2(5), p. 2.

UK Border Agency, 2013. *Three jailed for immigration offences*. [Online] Available at: <http://www.ukba.homeoffice.gov.uk/sitecontent/newsarticles/2013/june/16-three-jailed> [Accessed 19 August 2013].

Van der Aalst, W. & Van Hee, K., 2006. *Workflow Management*. Cambridge(MA): MIT Press.

Voas, J. & Wilbanks, L., 2008. Information and Quality Assurance: An Unsolved, Perpetual Problem for Past and Future Generations. *IT Professional*, 10(3), pp. 10 - 18.

Vodafone Ghana, 2012. *Vodafone Swipe Card Terms and Conditions*. [Online] Available at: <http://www.vodafoneswipe.com/terms-and-conditions> [Accessed 02 October 2013].

Vu, K.-P.L. et al., 2007. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, August, 65(8), pp. 744 - 757.

Wales, E., 2003. 'E-commerce Counts Cost of Online Card Fraud'. *Computer Fraud & Security*, 2003(1), pp. 9-11.

Walton, R., 2005. 'Low-cost assurance for B2C E-commerce'. *Computer Fraud & Security*, 2005(10), pp. 4-6.

Wang, Y., Liu, J., Xiao, F. & Dan, J., 2009. A more efficient and secure dynamic ID-based remote user authentication scheme. *Computer Communications*, 4 March, 32(4), pp. 583-585.

Wilson, S. G. & Abel, I., 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, January - February, 31(2), pp. 84-95.

Xu, Y., Huang, L. & Yang, Q., 2008. 'Role of Trust Transfer in E-Commerce Acceptance'. *Tsinghua Science & Technology*, 13(3), pp. 279-286.

Yu-Hui, C. & Stuart, B., 2007. Initial trust and online buyer behaviour. *Industrial Management & Data Systems*, 107(1), pp. 21 - 36.

Zhang, X. & Li, Y., 2005. 'Securing credit card transactions with one-time payment scheme'. *Electronic Commerce Research and Applications*, 4(4), pp. 413-426.

Zheng, Q. et al., 2009. *E-commerce Architecture and System Design*. Berlin: Springer Berlin Heidelberg.

Zhou, Z., 2004. *E-Commerce and Information Technology in Hospitality and Tourism*. Clifton Park(New York): Thomson Delmar Learning.

## 7. APPENDICES

### 7.1 Appendix A: TransNET module PseudoCode and Database

#### 7.1.1 PAC Card Production Pseudocode

##### Initialize form

- a) Input Member ID
- b) If Member do not exist or invalid, output error message,
- c) Else, Fetch and display member profile
- d) Input Quantity of PAC Card to be generated
- e) If Quantity is more than permitted integer, output error message,
- f) Else, generate PAC according to input number.
- g) Then, Display summary if generated PAC Card by batch ID

#### 7.1.2 Link PAC Card to Account Pseudocode

##### Initialize form

- a) Input Serial No
- b) If Serial No does not exist
- c) Output error “Account does not exist or Account is Invalid”
- d) Else – fetch and display Account information and position PAC Card form.
  
- e) Input PAC Serial No
- f) If PAC Serial No does not exist or is already in use
- g) Output error “ PAC Serial No is invalid or already linked to another Account”
- h) Else check if Account has existing PAC Card linked.
- i) If Account has an existing PAC Card,
- j) Change the existing PAC Card Status to inactive.
- k) While existing PAC Card status is changed to inactive.

- l) Link the new PAC Card and set it as the Active PAC Card.
- m) And Add entry in DB in descending order
- n) If all OK
- o) Display PAC Status and Information
- p) Else output error

### 7.1.3 Database Dictionary

## ev\_cordinate

Column	Type	Null	Default	Comments
co_id	bigint(20)	No		
serial_no	bigint(20)	No	0	
cordinate_y	char(1)	No		
x_1	int(3)	No	0	
x_2	int(3)	No	0	
x_3	int(3)	No	0	
x_4	int(3)	No	0	
x_5	int(3)	No	0	
x_6	int(3)	No	0	
x_7	int(3)	No	0	
x_8	int(3)	No	0	
x_9	int(3)	No	0	
x_0	int(3)	No	0	
dtupdatetime	datetime	No	0000-00-00 00:00:00	
upd_user_id	bigint(20)	No	0	

## ev\_cord\_accuser

Column	Type	Null	Default	Comments
cord_id	bigint(20)	No		
acc_user_id	bigint(20)	No	0	
serial_no	bigint(20)	No	0	
user_type	char(1)	No	N	
is_live	char(1)	No	N	
align_date	datetime	Yes	NULL	
dtupdtimestamp	datetime	Yes	NULL	
upd_user_id	bigint(20)	No	0	
turn_on_off	char(1)	No	Y	

## ev\_cord\_batch

Column	Type	Null	Default	Comments
batch_id	bigint(20)	No		
batch_no	bigint(20)	No	0	
batch_date	datetime	Yes	NULL	
user_id	bigint(20)	No	0	
quantity	int(10)	Yes	NULL	
serial_start	bigint(20)	No	0	
serial_end	bigint(20)	No	0	
download_status	char(1)	No	N	
download_date	datetime	Yes	NULL	
dtupdtimestamp	datetime	No	0000-00-00 00:00:00	
upd_user_id	bigint(20)	No	0	
country_id	int(5)	No	0	



## 7.2 Appendix B: AES Encryption/Decryption in PHP Language

```
function GetUrlData($strVariables){

global $arrParam;

$scipher = $arrParam["merchant"]["cipher"];

$smode = $arrParam["merchant"]["mode"];

$sizeid = $arrParam["merchant"]["izenid"];

$shiv= $arrParam["merchant"]["iv_key"];

$secret_key = $arrParam["merchant"]["secret_key"];

$strUrl = $arrParam["merchant"]["urlPath"];

$std = mcrypt_module_open($scipher, "", $smode, $shiv);

mcrypt_generic_init($std, trim($secret_key), $shiv);

$scyper_text = mcrypt_generic($std, $strVariables);

$szReturn = bin2hex($scyper_text);

mcrypt_generic_deinit($std);

mcrypt_module_close($std);

echo "<br>";

echo $encRequest="izenid=".$sizeid."&enc=".$szReturn;

echo "<br>";

$schObject =curl_init();
```

```

curl_setopt($schObject, CURLOPT_URL, $strUrl);

curl_setopt($schObject, CURLOPT_POST, 1);

curl_setopt($schObject, CURLOPT_POSTFIELDS,$encRequest);

curl_setopt($schObject, CURLOPT_VERBOSE, 1);

curl_setopt ($schObject, CURLOPT_SSL_VERIFYPEER, FALSE);

curl_setopt($schObject, CURLOPT_RETURNTRANSFER , 1);

curl_setopt($schObject, CURLOPT_TIMEOUT, 500);

$rsOutPut=curl_exec($schObject);

$rsOutPut=trim($rsOutPut);

/* Output Decryption */

$rsOutPut=decryptXmlResult($rsOutPut);

$rsOutPut=trim($rsOutPut);

/* Ends Here */

$objXML = xml_parser_create();

xml_parse_into_struct($objXML,$rsOutPut, $vals, $index);

xml_parser_free($objXML);

return $vals;

}

```

```
/* GetTreeValues :: This method Retrieve Childs[Keys and values ] of a specific node
into array From the Return XML */
```

```
function GetTreeValues($szkey,$arrXML){

$arrReturn = array();

$x=0;

$blnIsPresent =false;

$isSkip= false;

for($p=0;$p<count($arrXML);$p++){

if(strtoupper($arrXML[$p]["tag"])==$szkey &&
strtolower($arrXML[$p]["type"]=="open"){

$blnIsPresent=true;

$isSkip=true;

}else if(strtoupper($arrXML[$p]["tag"])==$szkey &&
strtolower($arrXML[$p]["type"]=="close"){

$blnIsPresent=false;

$isSkip=false;

if($szkey!="ERROR")

$x++;

}

if($blnIsPresent && !$isSkip){
```

```

    $arrReturn[$x][strtoupper($arrXML[$p]["tag"])]=$arrXML[$p]["value"];

        if($szkey=="ERROR")

            $x++;

    }

    $isSkip=false;

}

return $arrReturn;

}

function isValidDate($dt,$dtFormat){

$isDateFlag =false;

$arr=split("/", $dt); // splitting the array

    if($dtFormat=="MM/DD/YYYY"){

        $mm=$arr[0];

        $dd=$arr[1];

        $yy=$arr[2];

    }else if($dtFormat=="DD/MM/YYYY"){

        $mm=$arr[1];

        $dd=$arr[0];

        $yy=$arr[2];

```

```

    }else if($dtFormat=="YYYY/MM/DD"){

        $mm=$arr[1];

        $dd=$arr[2];

        $yy=$arr[0];

    }

    If(checkdate($mm,$dd,$yy))

        $isDateFlag=true;

    return $isDateFlag;

}

function decryptXmlResult($strEncXMLOutPut){

global $arrParam;

$cipher = $arrParam["merchant"]["cipher"];

$mode = $arrParam["merchant"]["mode"];

$iv= $arrParam["merchant"]["iv_key"];

$secret_key = $arrParam["merchant"]["secret_key"];

$strEncXMLOutPut = hex2bin($strEncXMLOutPut);

$td = mcrypt_module_open($cipher, "", $mode, $iv);

mcrypt_generic_init($td, trim($secret_key), $iv);

```

```
$decrypted_data = mdecrypt_generic($td, trim($strEncXMLOutPut));

mdecrypt_generic_deinit($td);

mdecrypt_module_close($td);

echo $decrypted_data;

return $decrypted_data;

    }

function hex2bin($hexdata) {

$bindata = "";

for ($i = 0; $i < strlen($hexdata); $i += 2) {

$bindata .= chr(hexdec(substr($hexdata, $i, 2)));

    }

    return $bindata;

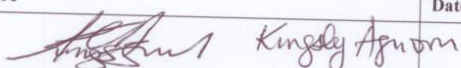
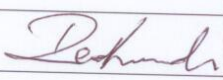
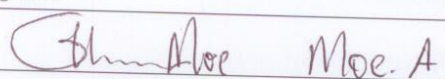
}

?>
```




## 7.4 Appendix D: 3W-ADA Sentry Acceptance Matrix

PROJECT ACCEPTANCE SUMMARY						
Project Name		Project Ref		Date Created		
3W ADA Sentry System		UEL Thesis		17 October, 2012		
Project Sponsor			Project Owner			
Paymenex Limited			Paymenex Limited			
Researcher/Program Manager			Project Manager			
Kingsley Aguoru			Kennedy Richard			
Completed by						
Kingsley Aguoru						
No	Acceptance Criterion	Critical		Test Result		Comments
		Yes	No	Accept	Reject	
1	Problem statement analysis and documentation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Software Requirements Specification documentation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The project will follow the integrated model of 3W ADA Sentry system
3	Software Design Specification Documentation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Paymenex TransNET module is presented high level description
4	Software User Acceptance Testing and documentation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

OTHER CONSIDERATIONS			
<b>Business Objectives – Did the software system meet the business requirements and objectives?</b>			
Yes	No	The 3W ADA Sentry system was tested on both legitimate and fraudulent perspectives, and it is feasibly seen to have solved the problem of card not present reported by the sponsor.	
<input checked="" type="checkbox"/>	<input type="checkbox"/>		
<b>Does the software application/system require any changes prior to installation? If so, please describe.</b>			
Yes	No	The software does not require any additional changes	
<input type="checkbox"/>	<input checked="" type="checkbox"/>		
APPROVAL			
Researcher		Signature	Date: 17/11/2012
Yes	No	 Kingsley Aguoru	
<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Project Owner		Signature	Date: 17/11/2012
Yes	No	Kennedy Richard 	
<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Project Sponsor		Signature	Date: 17/11/2012
Yes	No	 Moe. A.	
<input checked="" type="checkbox"/>	<input type="checkbox"/>		



## 7.5 Appendix E: Case Study of Vodafone Ghana




### MOBILE AIRTIME SWIPE CARD

**Leveraging Paymenex MultiCard technology enables an innovative and efficient electronic airtime swipe card solution for customers of Vodafone Ghana.**

“The Vodafone Swipe Card is an amazing and innovative product in the history of Telecommunication in Ghana and the first of its kind in Africa.

We are most delighted with inCharge Global Ltd for leveraging the Paymenex MultiCard technology in the provision of airtime e-top-up solution for Vodafone Ghana, moreover this will be invaluable for all mobile operators worldwide.”

Della Porbley - Administrator Paymenex Ghana



**vodafone**

### Background Information

- **Client:** Vodafone Ghana
- **Industry:** Telecommunications
- **Geography:** Ghana
- **Paymenex Product:** Paymenex MultiCard
- **Administrator:** Paymenex Ghana Limited
- **Issuing Member:** inCharge Global Limited Ghana
- **Member Background:** inCharge Global Limited, is a payment service provider and an authorised Paymenex Acquiring and Issuing member in Ghana, licensed to acquire and issue range of Paymenex payment and utility cards and D-Vouchers.



### Business Challenge

Method of buying and loading airtime credit to mobile prepaid subscriber's account pose great challenge to mobile phone operators around the world and lot more frustration to the customers because the widely used method do not offer the privilege and convenience of buying airtime when and where it is needed.

Despite the scratch card method virtually denies these privileges and convenience to the customer, the mobile operator also carries the burden of a clumsy and ambiguous logistics in managing scratch card products.

#### Airtime Scratch Card Process





**Some of the disadvantages includes:**

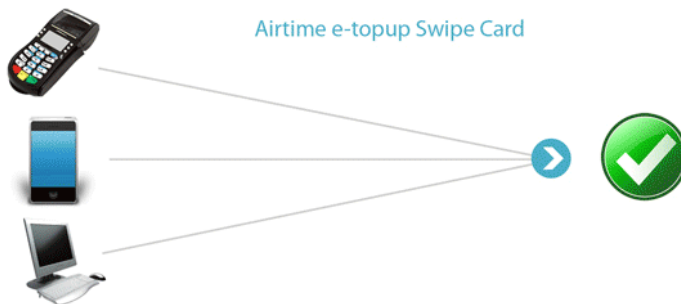
- High cost of scratch cards production
- Cost of producing each scratch card makes it not effective to sell low value airtime.
- Risk in distribution, storage and logistics.
- Inelegant and unreliable loading process.
- Low Profit margin
- Not eco friendly

## OBJECTIVES

- Reducing the cost of airtime top-up solution, eliminating the ambiguity in the use of scratch card solution and implementation of a cost-effective solution that will increase customer convenience and return on investment for Vodafone.
- Implementation of a solution that will be cost effective to sell airtime value of any low or high denomination, provide subscribers with greater flexibility and offer innovative way to top-up.
- A solution that will eliminate the risk involve in airtime distribution, storage, and logistics meanwhile remaining eco friendly.
- A solution that provides loyalty program possibilities and transparency.

## SOLUTION

For any mobile operator to remain reasonably competitive with the trend of technology innovation they need to strategize their marketing and airtime distribution processes, adapting to the electronic top-up method enables mobile operators to optimize their airtime distribution potentials covering all channels and improve customer's accessibility, satisfactions, and saves high production cost.



**Paymenex Limited**  
143 Kingston Road,  
Suite 132, Wimbledon,  
London - SW19 1LJ  
United Kingdom.

Tel: +44 20 8133 6065  
Fax: +44 20 8181 6899  
[www.paymenex.com](http://www.paymenex.com)

# Enjoy real convenience with the Vodafone Swipe Card

- Top up airtime, anytime, anywhere
- Top up airtime for family & friends instantly
- Enjoy online access to your swipe account



## APPROACH

- Establishing a secure connection between Vodafone's billing system and Paymenex TransNET.
- Configuration of a Vodafone USSD Shortcode to a Paymenex gateway specific.
- Issuance of Vodafone Swipe brand on PaymenexTransNET and linking of a Paymenex PAC card powered by 3W-ADA Sentry technology.

## RESULT

The result exceeds Vodafone's imagination. No more scratching, top-up conveniently anytime, anywhere through varieties of channels making Vodafone Ghana the first to offer airtime e-top-up swipe card in Ghana.

**Paymenex Limited**  
143 Kingston Road,  
Suite 132, Wimbledon,  
London - SW19 1LJ  
United Kingdom.

Tel: +44 20 8133 6065  
Fax: +44 20 8181 6899  
[www.paymenex.com](http://www.paymenex.com)



**END**