

**FACTORS INFLUENCING CREDIT CARD FRAUD IN THE
BANKING SECTOR:
THE CASE OF KENYA COMMERCIAL BANK MOMBASA
COUNTY, KENYA**

**BY
HARON ALEX KIBIWOT SITIENEI**

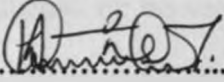
UNIVERSITY OF NAIROBI
KIKUYU LIBRARY
P. O. Box 30197
NAIROBI

**A RESEARCH PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE AWARD OF MASTER OF ARTS DEGREE
IN PROJECT PLANNING AND MANAGEMENT OF THE UNIVERSITY OF
NAIROBI**

2012

DECLARATION

I hereby declare that this research project report is my original work and has not been presented for a degree at any other university.

Signature: .....

Date:10/08/2012.....

HARON ALEX K. SITIENEI

L50/61248/2011

This research project has been submitted for examination with my approval as the candidate's University Supervisor.

Signature: ..... Date:10.08.2012.....

Johnbosco Kisimbii

Lecturer, Department of Extra-Mural studies,

University of Nairobi

ACKNOWLEDGEMENTS

I would like to acknowledge the University of Nairobi fraternity for opportunity accorded to me and the support I got from various offices during the process of writing my project.

I would also like to acknowledge the individual support provided by my Supervisors Mr. Johnbosco Kisimbii for his support and guidance throughout the whole project.

I would also like to thank Mr. Kirui Kenya Commercial Bank Treasury Square Branch Manager who encouraged me very much and gave me some of the information I needed concerning the Bank.

I would also like to thank Purity and Caro of University of Nairobi Mombasa campus for their administrative support accorded to me during my research.

I acknowledge your inputs and your participation. Thank you very much and God bless you abundantly.

DEDICATION

I dedicate this work to my lovely wife Viola Sitienei for her tireless efforts and supports in ensuring I finish the project on time. my beautiful girl Harriet and Son Trevor for their love and continued support throughout the process of writing this project.

May the almighty God bless you abundantly.

TABLE OF CONTENTS

	Page
DECLARATION	ii
ACKNOWLEDGEMENTS	iii
DEDICATION	iv
TABLE OF CONTENTS	v
LIST OF FIGURES.....	ix
LIST OF TABLES.....	x
ABBREVIATIONS AND ACRONYMS	xi
ABSTRACT.....	xii
CHAPTER ONE: INTRODUCTION.....	1
1.1 Background of the Study	1
1.2 Statement of the Problem.....	4
1.3 Purpose of the Study	5
1.4 Objectives of the Study.....	5
1.5 Research Questions.....	6
1.6 Research Hypothesis.....	6
1.7 Significance of the Study	7
1.8 Delimitations of the Study	7
1.9 Limitations of the Study	7
1.10 Basic Assumptions of the Study	8

1.11	Definition of Significant Terms used in the study	8
1.12	Organization of the Study.....	9
CHAPTER TWO: LITERATURE REVIEW.....		10
2.1	Introduction.....	10
2.2	Skimming and Credit Card Fraud.....	10
2.3	Proper Card Management and Credit Card Fraud	12
2.4	Technology and Credit Card Fraud	16
2.5	System Security and Credit Card Fraud	18
2.6	Systems integration and Credit Card Fraud.....	26
2.7	Conceptual Framework.....	30
2.8	Summary of Literature.....	32
CHAPTER THREE: RESEARCH METHODOLOGY		36
3.1	Introduction.....	36
3.2	Research Design	36
3.3	Target Population.....	36
3.4	Sample Size and Sampling Procedure	37
3.5	Data Collection Methods	38
3.6	Data Collection Procedure.....	39
3.7	Validity and Reliability of Research Instruments.....	39
3.7.1	Validity of Research instrument	39
3.7.2	Reliability of the Research Instruments.....	39

3.8	Data Analysis Techniques	40
3.9	Ethical Considerations	41
3.10	Operational Definition of Variables	41
CHAPTER FOUR: DATA PRESENTATION, ANALYSIS AND INTERPRETATION.....		45
4.1	Introduction.....	45
4.2	Response rate	45
4.3	Demographic Characteristics of the Respondents	46
4.4	Skimming and Credit Card Fraud in the Banking Sector	48
4.5	Proper card Management and Credit Card Fraud in the Banking Sector	50
4.6	System integration and credit card fraud in the banking sector.....	52
4.7	System Security and Credit Card Fraud in the Banking Sector.....	55
CHAPTER FIVE: SUMMARY OF FINDINGS, DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS.....		57
5.1	Introduction.....	57
5.2	Summary of Findings	57
5.3	Discussions	59
5.4	Conclusions.....	63
5.5	Recommendations.....	63
5.6	Suggestion for Further Study.....	64
REFERENCES		65

APPENDICES.....69

APPENDIX I: Transmittal Letter.....68

APPENDIX II: Employees Questionnair70

APPENDIX III: Customers Questionnair.....75

LIST OF FIGURES

	Page
Figure 1: Initial Server-Customer Communication Flow Diagram	14
Figure 2: Client Handler Software Architecture.....	15
Figure 3: System Diagram	22
Figure 4: Full System Architecture.....	24
Figure 5: Bank Server Architecture	25
Figure 6: Authentication Round 1	27
Figure 7: Authentication Round 2	28
Figure 8: Bank server vs. Customer E-card.....	29
Figure 9: Conceptual Framework.....	32

LIST OF TABLES

	Page
Table 3.1: Sample size.....	38
Table 3.2: Operational Definition of variables.....	43
Table 4.1: Response Rate.....	45
Table 4.2: Summary of respondents on Level of Management.....	46
Table 4.3: Age of respondents.....	47
Table 4.4: Profile of respondents on years of Experience.....	47
Table 4.5: Respondents knowledge on Credit Card Skimming.....	48
Table 4.6: Respondents training on credit card skimming.....	49
Table 4.7: Summary of chi-square statistic on knowledge in skimming.....	49
Table 4.8: Respondents on card management systems responsibility.....	50
Table 4.9: Summary of chi-square analysis on card management.....	51
Table 4.10: Percentage respondents on system Integration.....	52
Table 4.11: Summary of chi-square analysis on system integration.....	53
Table 4.12: Percentage respondents on training of customers.....	54

ABBREVIATIONS AND ACRONYMS

USA	United States of America
UK	United Kingdom
ATM	Automated Teller Machine
POS	Point of Sale
APACS	Association for payment clearing services
MOTO	Mail Order/Telephone Order
CNP	Cardholder Not Present
UN	United Nations
KCB	Kenya Commercial Bank
ICT	Information and Communication Technology
ACH	Automated Clearing House
AI	Artificial Intelligence

UNIVERSITY OF NAIROBI
KIKUYU LIBRARY
P.O. Box 20197
NAIROBI

ABSTRACT

Electronic commerce has gained a rapid growth and it has a significant impact on market of all the countries. Credit Card has become a de facto standard for online payments. This increase use of credit card has raised fraudulent practices across the world. There are no secure well defined ways to deal with credit card frauds in developing countries. By mid 1990s, credit card fraud was a rapidly growing problem for consumers and law enforcement agencies. As per the FBI report of 1997, United States had suffered the bulk of credit card losses-approximately \$875 million for 1996 alone. This is not surprising because 71% of all worldwide revolving credit cards in circulation were issued in United States. Law enforcement authorities continually confronted new and complex schemes involving credit card frauds committed against financial institutions and credit card holders. In 2009, MasterCard reported that the percentage of fraud in all Kenya Commercial banks within the country was approximately 0.07% of card holder expenditure while in Mombasa this figure was 0.05%. The Association for Payment Clearing Services (APACS, 2009) reported that at a worldwide level Kenya is one of the top five countries to have had an increase in the use of fraudulent credit cards. The report further stated that fraud on cards being used in Kenya had increased by 7.9% in 2005, to 18.3% in 2010. The purpose of this study was to determine the factors influencing credit card fraud in the banking sector. The literature review of the study revealed that skimming, technology, system security and proper card management are factors influencing credit card fraud, however other studies reviewed didn't identify system authentication as a factor apart from a study by World Bank in 2009. The Descriptive survey research design was employed in the study because it enabled the researcher to generalize its findings to the larger population of Kenya commercial bank. Data was collected from various Kenya Commercial Bank branches within Mombasa County and some customers who were sampled randomly as they visit the Bank. The target population for the study was senior staff members, junior staff members and some few customers who were sampled randomly. The study applied both quantitative and qualitative techniques to collect data. Various techniques and methods were used in data analysis and presentation. They include descriptive statistics and qualitative techniques. In descriptive analysis this included measures of central tendency for instance mean, mode and media. Statistical analysis frequency distribution was also used. The study established factors that were considered important in influencing credit card fraud in the banking sector. This included credit card skimming, technology, system security, proper card management and systems integration. The study found out that in terms of factors that influence credit card fraud all the five factors were found to be significant and contribute to the credit card frauds. The study recommended that all banks adopt smart credit cards as their main mode of operation, smart credit cards operate in the same way as their magnetic counterparts, the only difference being that an electronic chip is embedded in the card which can be loaded with customer's biometric details. A similar study may be undertaken in the entire Kenya commercial bank branch network in the country and also in the entire banking sector and other sectors that use credit and debit cards.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The current global recession is highlighting the fragility of the global banking and finance system that is subject to greater risk and acts of fraud. There are new challenges in tackling fraud stemming from a fast changing information technology environment, where the internet has become one of the most important channels for the retail sector. Kageyama (2009) reports that in the past three years more than 900 companies surveyed at a worldwide level have lost an average of 8.2 billion dollars a year, a 22% increase with respect to the previously published research. Moreover, the percentage of firms that registered at least one fraud in 2008 has reached 85%, an 80% increase on the previous year. While these figures hide the motivation for fraud, the rates of growth are significant and in a time of recession this rate is more likely to increase as higher numbers of individuals commit fraud (Abbey, 2009).

In 1958 Credit Card use rose and, unsurprisingly, credit card fraud was rampant. Mail theft also became widespread as unscrupulous individuals discovered that envelopes containing credit cards were just like envelopes full of cash and there was little to stop card companies from sending out cards which customers had never asked for, were not expecting, and could not have known had been stolen until the issuing company began demanding payment for the charges which had been run up. These crimes and other problems stemming from the relentless card-pushing by banks led directly to the passage of the Fair Credit Billing Act of 1974 as well as many other laws designed to protect the consumer. (Fox, 2005)

A 1997 FBI report stated that, around the world, The Bank card fraud losses to Visa and Master-Card alone had increased from \$110 million in 1980 to an estimated \$1.63 billion in 1995. The United States had suffered the bulk of these losses-approximately \$875 million for 1995 alone. This is not surprising because 71% of all worldwide revolving credit cards in circulation were issued in United States.

Law enforcement authorities continually confronted new and complex schemes involving credit card frauds committed against financial institutions and bank card companies. Perpetrators run the gamut from individuals with easy access to credit card information such as credit agency officials, airline baggage handlers, and mail carriers, both public and private-to organized groups, usually from similar ethnic backgrounds, involved in large-scale card theft, manipulation, and counterfeiting activities. Although current bank card fraud operations are numerous and varied, several schemes account for the majority of the industry's losses by taking advantage of dated technology, customer negligence, and laws peculiar to the industry. (Hutchins, 2002).

In early 2010 the world's two largest credit card circuits, Visa and MasterCard, reported 1.14 billion dollars of fraud losses that represented a 62.9% increase with respect to 2005. In the United Kingdom for example credit card fraud is one of the fastest growing crimes and in 2009 total card fraud losses amounted to more than 609 million pounds, of which 52.5 million was attributed specifically to online banking fraud (Association for Payment Clearing Services, 2009). Visa (2009) calculates a 10% year on year compound growth since cards were first issued. The USA for instance denotes the highest number of issued cards (more than 1.5 billion) and each inhabitant owns on average more than 5 payment instruments. In Europe however, the average card holder owns 1.3 cards and the UK confirms its predominance with fraud losses are driving increasing efforts in both the detection and prevention of fraud and the implementation of robust risk management practices in the credit card industry (Affari and Finanza, 2009).

Credit card fraud has been defined as the misuse of a card without authorization or unapproved purchases or the counterfeiting of cards (Wells, 2010). The motivation and opportunity behind credit card fraud are many and varied. Traditional types of fraudulent behavior such as identity theft relate to family members or people that can easily access individual's mail and personal information and committing fraud either by applying for a card or taking over the existing account. Dumpster diving or trashing, where criminals raid rubbish bins to search for credit card details and other sensitive information is becoming more widespread. Lost or stolen credit cards may also be used fraudulently. Skimming of the magnetic stripe is also still practiced either using highly sophisticated

devices embedded in ATM's or POS or using simple hand held skimmers capable of storing magnetic stripe data (Wells, 2010).

Internet enabled fraud is also growing; phishing attacks continue to harvest credit card users' details and compromised computer with key loggers provide organized criminals with the card details. As the vast majority of all credit card transactions are now authorized and cleared on-line, hacking into the e-payment chain to intercept data can harvest many millions of card details. The e-fraud market has grown, criminals are now provided with various internet resources to counterfeit credit cards, examples are tipping, custom embossing, decoding machines as well as software such as Credit master. A common practice is also that of phishing where fraudulent emails hijacking brand name of banks and credit cards companies are sent aimed at acquiring tricky financial data, account usernames and passwords. National picture on credit card fraud: Organized crime is normally composed by professional criminals that are setting "carding forums" where it is possible to buy wide-scale global stolen personal and financial information. This practice that leads to the unauthorized use of sensitive information to purchase goods and services often involves thousands and even millions of victims. Indeed credit card fraud is subject to technological enhancement and it is in a continuous evolution (Peretti and Onyarie, 2008).

However, due the lack of statistical information on fraud - MasterCard for example is the only international circuit that provides statistical information on credit card fraud. In 2009, MasterCard reported that the percentage of fraud in all Kenya Commercial banks within the country was approximately 0.07% of card holder expenditure while in Mombasa this figure was 0.05% (Affari and Finanza, 2009). The Association for Payment Clearing Services (APACS, 2009) reports that at a worldwide level Kenya is one of the top five countries to have seen an increase in the use of fraudulent credit cards. Fraud on cards being used in Kenya has increased by 72.9% since 2005, to £8.3 million in 2010.

1.2 Statement of the Problem

Kageyama (2009) reports that in the past three years more than 900 companies surveyed at a worldwide level have lost an average of 8.2 billion dollars a year, a 22% increase with respect to the previously published research. Moreover, the percentage of firms that registered at least one fraud in 2008 has reached 85%, an 80% increase on the previous year. While these figures hide the motivation for fraud, the rates of growth are significant and in a time of recession this rate is more likely to increase as higher numbers of individuals commit fraud.

In early 2010 the world's two largest credit card circuits, Visa and MasterCard, reported 1.14 billion dollars of fraud losses that represented a 62.9% increase with respect to 2005. In the United Kingdom for example credit card fraud is one of the fastest growing crimes and in 2009 total card fraud losses amounted to more than 609 million pounds, of which 52.5 million was attributed specifically to online banking fraud (Association for Payment Clearing Services, 2009). Arguably, these high amounts can be partially explained by the high volume of transactions and remarkable growth in credit cards ownership over the past three decades. Visa (2009) calculates a 10% year on year compound growth since cards were first issued. The USA for instance denotes the highest number of issued cards (more than 1.5 billion) and each inhabitant owns on average more than 5 payment instruments. In Europe however, the average card holder owns 1.3 cards and the UK confirms its predominance with fraud losses are driving increasing efforts in both the detection and prevention of fraud and the implementation of robust risk management practices in the credit card industry (Affari and Finanza, 2009).

In 2009, MasterCard reported that the percentage of fraud in all Kenya Commercial banks within the country was approximately 0.07% of card holder expenditure while in Mombasa this figure was 0.05% (Affari and Finanza, 2009). The Association for Payment Clearing Services (APACS, 2009) reports that at a worldwide level Kenya is one of the top five countries to have seen an increase in the use of fraudulent credit cards. Fraud on cards being used in Kenya has increased by 72.9% since 2005, to £8.3 million in 2010.

Credit card Fraud is the number one enemy of business, no bank is immune to it and it is in all works of life. The fear is now rife that the increasing wave of fraud in the financial institutions in recent years, if not arrested might pose certain threats to stability and the survival of individual financial institution and the performance of the industry as a whole and no area of the economy is immune from fraudsters and even the banking system. Fraud if not checked might cause run on in the banking sector (Affari and Finanza, 2009). The losses associated with these attacks has risen drastically over the past couple of years, and counterfeit fraud has now been overtaken as the most costly type of card fraud by a newer method, that of Cardholder-Not-Present (CNP) fraud. In Kenya year 2009 alone, CNP fraud was responsible for losses of USD 116.4m more than any other type of card fraud, in the KCB, over the period (Financial times, January 2010; UN World Report on electronic fraud-December 2004). The essence of this study was to examine those factors that have influenced credit card fraud in the banking sector in Kenya, with a special reference to Kenya Commercial Bank in Mombasa County.

1.3 Purpose of the Study

The purpose of this study was to determine the factors influencing the credit card fraud in the banking sector in Kenya.

1.4 Objectives of the Study

The study was guided by the following objectives:

1. To establish how skimming is a factor influencing credit card fraud in the banking sector.
2. To determine how technology influences credit card fraud in the banking sector.
3. To assess how proper card management contributes to credit card fraud in the banking sector.
4. To ascertain how system security contribute to credit card fraud in the banking sector.
5. To examine how systems integration is a factor influencing credit card fraud in the banking sector.

1.5 Research Questions

The study was guided by the following research questions:

1. How does the skimming contributing in the extent of credit card fraud in the banking sector?
2. How does the card management in Kenya Commercial Bank influence credit card fraud?
3. How does proper authenticate of documents influence credit card fraud?
4. What security measures has Kenya Commercial bank taken to detect and mitigate credit cards frauds?
5. How is the magnitude of credit card fraud related to staff experience and volume of work for staff?

1.6 Research Hypothesis

The study tested the following research hypothesis

1. Ho – Knowledge in skimming is not a factor influencing credit card fraud in the banking sector
H1 – Knowledge in skimming is a factor influencing credit card fraud in the banking sector
2. Ho – Proper card management doesn't influence credit card fraud in the banking sector
H1 – Proper card management influence the credit card fraud in the banking sector
3. Ho – System Security is not a factor influencing credit card fraud in the banking sector
H1 – System Security is a factor influencing credit card fraud in the banking sector
4. Ho – System Authentication is not a factor influencing credit card fraud in the banking sector
H1 – System Authentication is a factor influencing credit card fraud in the banking sector

5. Ho – Technology is not a factor influencing credit card fraud in the banking sector
H1 – Technology is a factor influencing credit card fraud in the banking sector

1.7 Significance of the Study

The study is significant to a number of stakeholders, who include:

To KCB: It will help the bank in identifying and reducing the costs and losses associated with incompetence, enable the bank to minimize customers complains, while winning customer's loyalty, building up status and increasing returns.

To other Researchers: This study will contribute to the already rich Literature available on credit card fraud.

To the Customers: This study will assist the customers understand the various factors influencing credit card fraud and how to mitigate them.

1.8 Delimitations of the Study

The researcher focused on credit department in the Banking sector, The following Kenya Commercial Bank Branches within Mombasa County were sampled, Treasury Square, Town Centre, Kilindini, Mwembe Tayari, Mvita, Kisauni, Mtwapa and Mariakani. The Officers whom were being targeted in the Study are Branch Managers, Assistant Branch Managers, Tellers and any other staff that handles credit card during their daily operations.

1.9 Limitations of the Study

The key limitations facing the study are;

1. Financial constraints – The researcher took a soft loan from his cooperative society.
2. Mobilizing of enumerators – Two qualified enumerators were picked and trained before they were send to drop and pick the questionnaires.

1.10 Basic Assumptions of the Study

This study was based on the following assumptions

1. That credit card fraud is prevalent in the banking sector in Kenya
2. That Kenya Commercial Bank doesn't have a system in place to detect and mitigate credit card fraud.
3. The bank employees willingly provided the information required by the researcher on credit card fraud.

1.11 Definition of Significant Terms used in the study

Carding - is a term used for a process to verify the validity of stolen card data

Commercial bank – is a financial institution that accepts deposits and pools those funds to provide credit, either directly by lending, or indirectly by investing through the capital markets

Credit card – is a payment card issued as a system of payment or a card issued by a financial company giving the holder an option to borrow funds, usually at point of sale.

Credit card Fraud - is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft.

Float - is a phenomenon that arises because of the nature of the payments clearing system

Fraud – is defined as “Deceit or trickery deliberately practiced in order to gain some advantage dishonestly”

Skimming - is the theft of credit card information used in an otherwise legitimate transaction.

1.12 Organization of the Study

The study was organized in five chapters excluding the preliminary pages which contains the title, declaration, dedication, abstract, acknowledgements, table of contents, list of figures, list of tables, abbreviations and acronyms and at the back matters containing the references, letter of transmittal and the questionnaires.

Chapter one contains the background of credit card fraud in the Banking sector and its origin. It looks at various case studies globally, regionally and locally.

Chapter two contains the literature review on both theoretical and empirical literature on factors influencing credit card fraud in the banking sector. It concludes with the conceptual framework.

Chapter three contains the research design, target population, sampling procedures and sample size, methods of data collection, data validity ,data reliability, data analysis techniques, ethical considerations and operational definition of variables.

Chapter four contains key findings which include details of respondents, tables of descriptive statistics of variables and analysis on factors influencing credit card fraud in the banking sector.

Chapter five is on summary of findings, discussions, conclusions, recommendations and suggested areas for further research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this section it explains how credit card skimming, proper card management, technology, security systems and systems Integration influences the rise of credit card fraud in the Banking sector.

2.2 Skimming and Credit Card Fraud

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant, and can be as simple as photocopying of receipts. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip (Kingdom 1995)

Instances of skimming have been reported where the perpetrator has put a device over the card slot of a public cash machine (automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's PIN at the same time (Goldberg 1989)

Skimming is difficult for the typical card holder to detect, but given a large enough sample, it is fairly easy for the bank to detect. The bank collects a list of all the card holders who have complained about fraudulent transactions, and then uses data mining to discover relationships among the card holders and the merchants they use. For example, if many of the customers used one particular merchant, that merchant's terminals (devices used to authorize transactions) can be directly investigated. Sophisticated algorithms can also search for known patterns of fraud. Merchants must ensure the physical security of their terminals, and penalties for merchants can be severe in cases of compromise, ranging from large fines to complete exclusion from the merchant banking system, which

can be a death blow to businesses such as restaurants which rely on credit card processing (Bolton and Hand 2002)

Credit card operations expose the lending institution to two primary types of risk, credit and fraud. All circumstances where a cardholder or merchant become indebted to a bank without deception and is unable or unwilling to repay are classified as credit losses. All other situations are classified as fraud. Fraud is a crime although there are variations in its definition among the statutes of various countries where the credit card is used. Fraud includes the following categories: lost, stolen, not received, counterfeit, fraudulent application, fraudulent use of card, and other (Smith and Weber, 2000).

According to Abbey (2005), skimming started in the late 1990's, but has become easier to accomplish with the development of smaller computer components. In the United States alone, there are approximately 365,000 ATM machines, generating greater than 41,000,000 transactions daily. Fifty percent of the ATMs are owned by banks and fifty percent by other merchants that place their ATMs in establishments such as restaurants, hotels, shopping malls, convenience stores, airports, etc. Each of these is a potential target for prospective criminals or crime rings skimming can involve the transfer of huge sums of money. According to the American Bankers Association, \$51 million was lost due to debit card fraud. In a New York crime ring, about \$3.5 million was stolen before the criminals were apprehended. This case involved greater than 20 ATM machines, thousands of ATM cards, 1,400 cards issuers, and in excess of 26,000 ATM transactions. "Most ATM activity occurs during the evening" and the thieves rarely stay in the same area for more than seven to ten days. The "counterfeit cards (are) produced within 24 hours" and fraudulent transactions are performed within 24 to 48 hours after the swipe data and PIN are stolen. Other skimming cases in the United States have been reported in – Boca Raton, Florida, Illinois, Kansas, Maryland, Virginia, Wisconsin, South Carolina, and Colorado, as well (Annese, 2003).

But skimming is not just of national concern, it is also an international problem. Cases have been reported in Australia, South Africa, France, Spain and many other parts of the world. The Australian Crime Commission estimates that skimming is responsible for \$300 million a year in that country and that much of this crime is being committed by

organized crime rings linked with Malaysia, Indonesia, Hong Kong and Thailand. And Ian McKindley, Head of Fraud Control with Visa International, reports that in the last year, skimming increased by 300 percent (Annese, 2003)

2.3 Proper Card Management and Credit Card Fraud

Credit Card Fraud is one of the biggest threats to business establishments today. However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of modus operandi to commit fraud. In simple terms, Credit Card Fraud is defined as: When an individual uses another individuals' credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. Further, the individual using the card has no connection with the cardholder or issuer, and has no intention of either contacting the owner of the card or making repayments for the purchases made (Bhatla 2003)

Contrary to popular belief, merchants are far more at risk from credit card fraud than the Cardholders. While consumers may face trouble trying to get a fraudulent charge reversed, merchants lose the cost of the product sold, pay chargeback fees, and fear from the risk of having their merchant account closed. Increasingly, the *card not present* scenario, such as shopping on the internet poses a greater threat as the merchant (the web site) is no longer protected with advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the 'physical world' checks necessary to detect who is at the other end of the transaction. This makes the internet extremely attractive to fraud perpetrators. According to a recent survey, the rate at which internet fraud occurs is 12 to 15 times higher than 'physical world' fraud. However, recent technical developments are showing some promise to check fraud in the card not present scenario (Bolton and Hand, 2002)

With all the negative impacts of fraudulent credit card activities – financial and product losses, fines, loss of reputation, etc, and technological advancements in perpetrating fraud

it's easy for merchants to feel victimized and helpless. However, technological advancements in preventing fraud have started showing some promise to combat fraud. Merchants and Acquirers and Issuers are creating innovative solutions to bring down on fraudulent transactions and lower merchant chargeback rates. One of the main challenges with fraud prevention is the long time lag between the time a fraudulent transaction occurs and the time when it gets detected, the cardholder initiates a chargeback. Analysis shows that the average lag between the transaction date and the chargeback notification could be as high as 72 days. This means that, if no fraud prevention is in place, one or more fraudsters could easily generate significant damage to a business before the affected stakeholders even realize the problem (Williams, 2007)

The technology for detecting credit card frauds is advancing at a rapid pace – rules based systems, neural networks, chip cards and biometrics are some of the popular techniques employed by Issuing and Acquiring banks these days. Apart from technological advances, another trend which has emerged during the recent years is that fraud prevention is moving from back-office transaction processing systems to front-office authorization systems to prevent committing of potentially fraudulent transactions. However, this is a challenging trade-off between the response time for processing an authorization request and extent of screening that should be carried out (Bhatla, 2003).

As the name suggests this component manages and deals with client or customer requests in general. It is responsible for accepting client's initial communication and creation of a client handler that takes control of all proceeding communications. Once initialisation is complete the manager waits until contacted by a client application at the gateway connection port, which defaults at 1150, but is configurable. Upon connection of a client it opens communication channels between the two and requests a port number from a port manager (Intertek Group, 1994).

The port manager is responsible for allocating free ports to the system. The system is configured to allow only a certain range of ports to be allocated to clients. This prevents the system from acquiring all ports available or ports that are needed by the retail manager or other applications. When a port is no longer needed it must be surrendered

back this manager again so that it may be made available for another client application to connect to the bank. If no ports are available the client application is refused a connection (D'Amato and Sheridan, 2008)

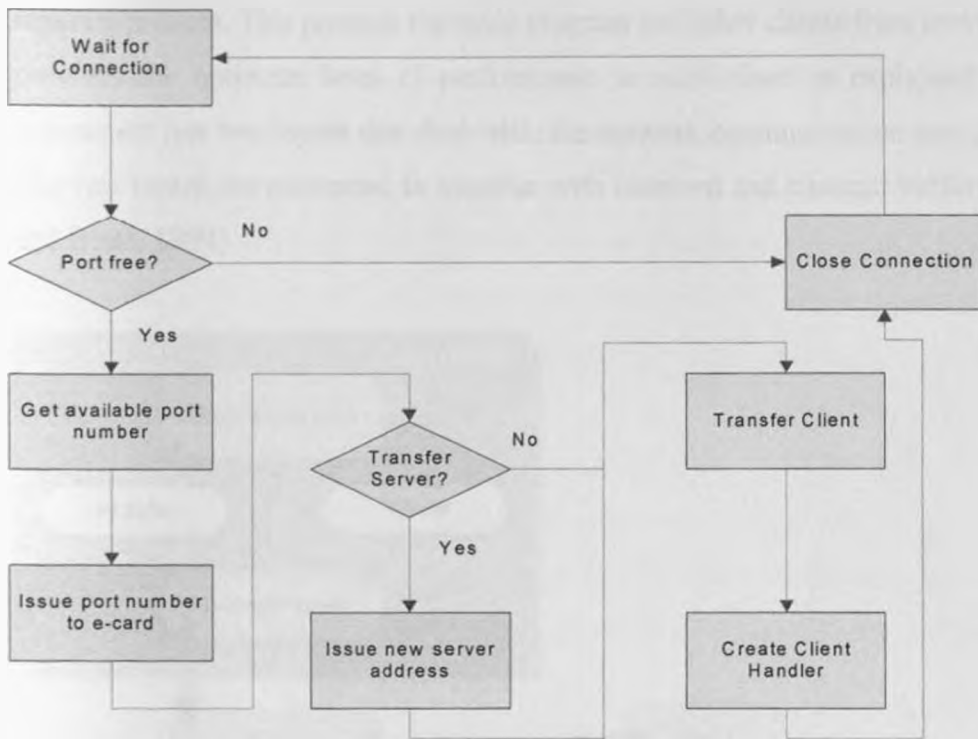


Figure 1: Initial Server-Customer Communication Flow Diagram (Venugopal and Beats, 1994; Shuliang Li, 2000)

The connection is terminated to the client if no port is available otherwise a port is allocated to that client. This port number is then sent to the client along with a transfer server address if desirable. This transfer server address represents the IP address of another server that could be setup with an application similar to this one. This other server is not included in the current design but would be required if the system were scaled up. It would only deal with client transaction requests. The function of this transfer would be part of a load balancing mechanism designed to spread the demand of thousands of client connections to be spread over many servers (Shuliang Li, 2000)

A client handler is then created to deal with further client requests and it is passed the port the client is expected to reconnect on. The client manager then disconnects from the

client and resumes waiting for another client connection. The client handler deals with all client requests after the initial connection. Its main responsibilities include authenticating the customer's device and supporting a transaction. It exists as a thread in Java, which means it executes within the main program's memory space but executes as if it is a separate process. This protects the main program and other clients from serious errors and provides the optimum level of performance to each client as explained before. This component has two layers that deal with; the network communication and client control. The two layers are connected to together with received and transmit buffers (Venugopal and Beats, 1994)

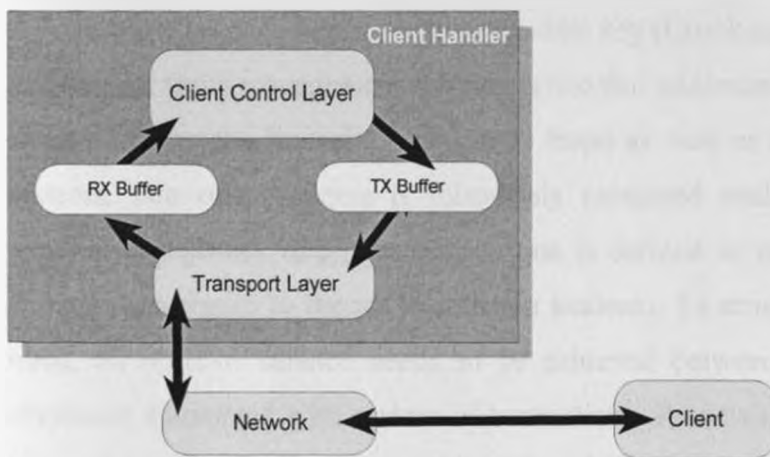


Figure 2: Client Handler Software Architecture (Venugopal and Beats, 1994; Shuliang Li, 2000)

The lower layer, the network layer, is similar to the client manager in that it waits for the client to connect and then it begins processing the data streams. It passes all data messages it receives to the receive buffer and monitors the transmit buffer, sending the data from it when it arrives (Venugopal and Beats, 1994)

There is also a built in security mechanism which will timeout if a client has not reconnected within a certain configurable period of time. This prevents a port being left open to another illegal party for more than typically a second. It also resolves a case where a unit may fail to reconnect causing the port to be left open and exhausting the resource (Shuliang Li, 2000)

The main functionality and responses to the client are generated in this layer. It accepts messages from the client and responds by issuing data or by communicating with a retailer on behalf of a customer. It authenticates the customer's device by issuing challenges and by using two cryptographic algorithms to protect the data. The MD5 and RSA algorithms are used to encrypt any sensitive, personal or important information.

On initialisation of this layer an RSA module is created and two keys are generated. The size of the keys generated is configurable, but 1024 bit keys are suggested as a minimum level of security. The two keys are known as the public and private keys and they are inversely related. The public key is sent with all messages transmitted to the client and the private key is never revealed but held in memory instead. All messages received from the client contain the client's respective public key (Crook and Banasik, 2004).

An efficient fraud management solution is one that minimizes the *total cost* of fraud, which includes the financial loss due to fraud as well as the cost of fraud prevention systems. Too often success is mistakenly measured exclusively by one metric –the monthly chargeback rate (Chargeback rate is defined as the percentage of chargeback amount with regard to the net transaction amount). To minimize the actual *total cost* of fraud, an optimal balance needs to be achieved between reducing fraud losses and overheads associated with review of transactions. Reviewing the appropriate number of transactions is the key to achieve this optimal balance (Bhatla, 2003)

2.4 Technology and Credit Card Fraud

According to Earring wood and Story (1996) the extensive technology innovation and telecommunication, we have seen new financial distribution channels increasing rapidly both in the numbers and form, from ATMs, telephone banking, PC banking to internet banking. Developing alternative distribution channels is not only important in terms of reducing costs and improving competitiveness, but also in terms of financial institution's ability to retain the existing customer case. (Kimball and Gregor, 1995) as well as to attract new customers. Sathye (1999) proposed a model for Internet Banking in Australia is significantly influenced by variables of system insecurity, case of use awareness of service and its benefits, reasonable price, availability of infrastructure and resistance to

change. The transformation from traditional brick-and-mortar banking to E-Banking has been Automatic Teller Machine (ATM) and thus the retail banking industry witnessed significant and extensive change. Formally, E-banking comprises various formats or technologies, including telephone (both land line and cell phone banking, direct bill payment (EFT), and PC or internet banking (Power, 2000). Weitzman, (2000), Lassar, Manolits and Lassar, (2005), Ehou and Chou (2000) identified five basic services associated with online banking: view account balances, and transaction histories, paying bills, transferring funds between accounts, requesting credit card advance, and ordering checks. Majority of banks of banks is planning to introduce ICT for integration of banking service and new finance service, which will play a vital role in bringing efficiency in financial sector (Raihan, 2001). The most commonly factors are ease of use, transaction security, convenience and speediness (Wan, Luk and Chow, 2005).

As card business transactions increase, so too do frauds. Clearly, global networking presents as many new opportunities for criminals as it does for businesses. While offering numerous advantages and opening up new channels for transaction business, the internet has also brought in increased probability of fraud in credit card transactions. The good news is that technology for preventing credit card frauds is also improving many folds with passage of time. Reducing cost of computing is helping in introducing complex systems, which can analyze a fraudulent transaction in a matter of fraction of a second. It is equally important to identify the right segment of transactions, which should be subject to review, as every transaction does not have the same amount of risk associated with it. Finding the optimally balanced 'total cost of fraud' and other measures outlined in this article can assist acquiring and issuing banks in combating frauds more efficiently (Bhatla, 2003)

The mail and the Internet are major routes for fraud against merchants who sell and ship products, as well Internet merchants who provide online services. The industry term for catalog order and similar transactions is "Card Not Present" (CNP), meaning that the card is not physically available for the merchant to inspect. The merchant must rely on the holder (or someone purporting to be the holder) to present the information on the card by

indirect means, whether by mail, telephone or over the Internet when the cardholder is not present at the point of sale (Roberts, 2008).

It is difficult for a merchant to verify that the actual card holder is indeed authorizing the purchase. Shipping companies can guarantee delivery to a location, but they are not required to check identification and they are usually are not involved in processing payments for the merchandise. A common preventive measure for merchants is to allow shipment only to an address approved by the cardholder, and merchant banking systems offer simple methods of verifying this information (Sullivan, 2010)

Additionally, smaller transactions generally undergo less scrutiny, and are less likely to be investigated by either the bank or the merchant, since the cost of research and prosecution usually far outweighs the loss due to fraud. CNP merchants must take extra precaution against fraud exposure and associated losses, and they pay higher rates to merchant banks for the privilege of accepting cards. Anonymous scam artists bet on the fact that many fraud prevention features do not apply in this environment (Roberts, 2008).

Merchant associations have developed some prevention measures, such as single use card numbers, but these have not met with much success. Customers expect to be able to use their credit card without any hassles, and have little incentive to pursue additional security due to laws limiting customer liability in the event of fraud. Merchants can implement these prevention measures but risk losing business if the customer chooses not to use the measures (Bhatla, 2003).

2.5 System Security and Credit Card Fraud

The fraud begins with either the theft of the physical card or the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The compromise can occur by many common routes and can usually be conducted without tipping off the card holder, the merchant or the issuer, at least until the account is ultimately used for fraud. A simple example is that of a store clerk copying sales receipts for later use. The rapid growth of credit card use on the Internet has made

database security lapses particularly costly; in some cases, millions of accounts have been compromised. Stolen cards can be reported quickly by cardholders, but a compromised account can be hoarded by a thief for weeks or months before any fraudulent use, making it difficult to identify the source of the compromise. The cardholder may not discover fraudulent use until receiving a billing statement, which may be delivered infrequently. That is why cardholders need to check their account daily to ensure constant awareness in case there are any suspicious, unknown transactions or activities (Sriganesh, 2008)

In Canada in 2004/05, 278,902 fraud and forgery offences were recorded by the police, a decrease of 12 per cent from the previous year (317,947 fraud and forgery offences recorded) (Nicholas *et al.*, 2005). However, many crimes of this kind are not reported to the police because either victims are not aware of the incident, or if they are aware, they are more likely to report it to their bank or card-holder company. According to the Association of Payment Clearing Services (APACS) recent figures have shown that total card fraud was £219.4million for the period January to June 2005, significantly (13%) lower than in the same time period in 2004. The main reason for this is due to the introduction of chip and pin technology where cardholders have to use their pin number instead of their signature. However, Internet, phone and mail-order fraud was the only type of fraud to have increased in the same time period (APACS, 2005).

First, crime displacement is anything but inevitable and there is little evidence that displacement is in fact ever complete (Gabor, 1990; Clarke, 1992). Even complete displacement may involve a deflection towards less serious crimes (Barr and Pease, 1990). Second, the assumption that offenders are free or motivated to engage indiscriminately in a variety of criminal acts has been challenged on methodological and substantive grounds (Cornish and Clarke, 1988).

In order to improve the analytical search for likely and unlikely displacement effects, it has been suggested that criminologists explicitly uncover the choice structuring properties underlying crime-switching patterns, namely "those single or multiple features of particular criminal activities which make them differentially available and attractive to certain individuals at certain times" (Cornish and Clarke, 1988: 108). For theft involving cash, choice-structuring properties include availability, awareness of method, likely cash

yield, expertise needed or not, degree of planning, amount of resources required, operating with or without associates, time required to commit, cool nerves (or not), risks of apprehension, severity of punishment, confrontation with victim, social cachet, fencing arrangements, moral evaluation (Cornish and Clarke, 1987).

Laptop computers are also used in conjunction with small encoding devices to modify the encoded data on magnetic stripes. According to police officers, a pirate software with the relevant instructions circulate in Montreal. The program is especially designed to add or modify data encoded on the magnetic stripes of credit cards. Thus, with the right equipment and the appropriate technical knowledge, it becomes relatively easy to add the stolen data on the plastic. In the case of white plastic frauds the forger simply has to emboss the credit card numbers onto the plastic card with the help of an embossing machine. He can also have his cards embossed in an establishment specializing in the making of personalized identification cards (even though, as it happened, vigilant employees may realize that the numbers to be embossed are credit cards numbers and contact the police). Recently police officers have also stumbled upon white plastic card bearing magnetic stripe on their back. (Trembley 1986).

Thus, some white plastic forgers also make use of magnetic encoding technology. Altered credit card frauds require a little more effort. Offenders must first erase all the original data embossed and or encoded on the stolen card before they can add a whole new cardholder name and account number. The completion of a pure counterfeit credit card is not intrinsically difficult. The hardest part, the actual fabrication of the blank credit card (Mars, 1992)

According to Trembley (1986), carders used computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which valid accounts were. Another variation would be to take false card numbers to a location that does not immediately process card numbers, such as a trade show or special event. However, this process is no longer viable due to widespread requirement by internet credit card processing systems for additional data such as the billing address, the 3 to 4 digit Card Security Code and/or the card's expiry date, as well as the more prevalent use of wireless card scanners that can process transactions right away. Nowadays, carding is

more typically used to verify credit card data obtained directly from the victims by skimming or phishing (Trembley, 1986).

A set of credit card details that has been verified in this way is known in fraud circles as a phish. A carder will typically sell data files of phish to other individuals who will carry out the actual fraud. Market price for a phish ranges from US\$1.00 to US\$50.00 depending on the type of card, freshness of the data and credit status of the victim (Roberts, 1993).

The new system is designed so that it can work in offline mode, which means that a transaction can take place even if the retailer is not connected to the bank. It can therefore be deduced that the PIN number is stored on the card itself. When the secure protocol protecting these cards is eventually breached then every card worldwide is threatened.

The authenticating terminal used, is placed in a retailer outlet where a keypad for customer use is provided. A criminal can observe the sequence of numbers entered by a customer unambiguously by standing near the terminal while the code is entered. The code is only four digits in length and that is not difficult to memorise. A devious retailer could collude on fraud scam by providing CCTV footage of customers entering PIN codes or by tampering with the terminal itself. Most of these keypads do not provide any visual protection for the customer. (Cusson, 1993).

A PIN number is four digits in length that allows ten thousand combinations equating to less than 14-bit encryption. Most online payment systems provide 128-bit encryption from fraud. The majority of credit card fraud takes place online by using a victim's card numbers, expiry date and sometimes security code to acquire goods or services. "Chip and Pin" does not provide any protection against this type of fraud even though it accounted for thirty per cent of all credit card fraud in 2004 in Britain (Hurley, 1995).

As a result, it is evident that the new system is considerably more effect than the old system. However it dramatically improves protection for the banking industry, it does not protect non-card present transactions and it gives no reassurance to users against an attack. To the contrary, it may provoke violent crime to attain a customer's PIN number and card. The proposed system gives the customer a personal terminal to communicate with their bank while on the move over a secure wireless network. As retailers are

generally stationary their unit will be connected over a wired banking network to their own bank. It must be assumed that the parties can trust their own banks and that the banks communicate with each other in a secure manner (Trembly, 1986).

The customer no longer needs to divulge sensitive and critical information into a possibly insecure environment. Instead by relying on guaranteed trust, a transaction can take place. If a customer can trust their bank with information and a bank can trust a retailer they've accepted with information then a chain of trust can be built between customer and retailer. By securing the links between all parties a guaranteed chain of trust can then be established (Shuliang, 2000).

The proposed system can be interpreted as described by the diagram.

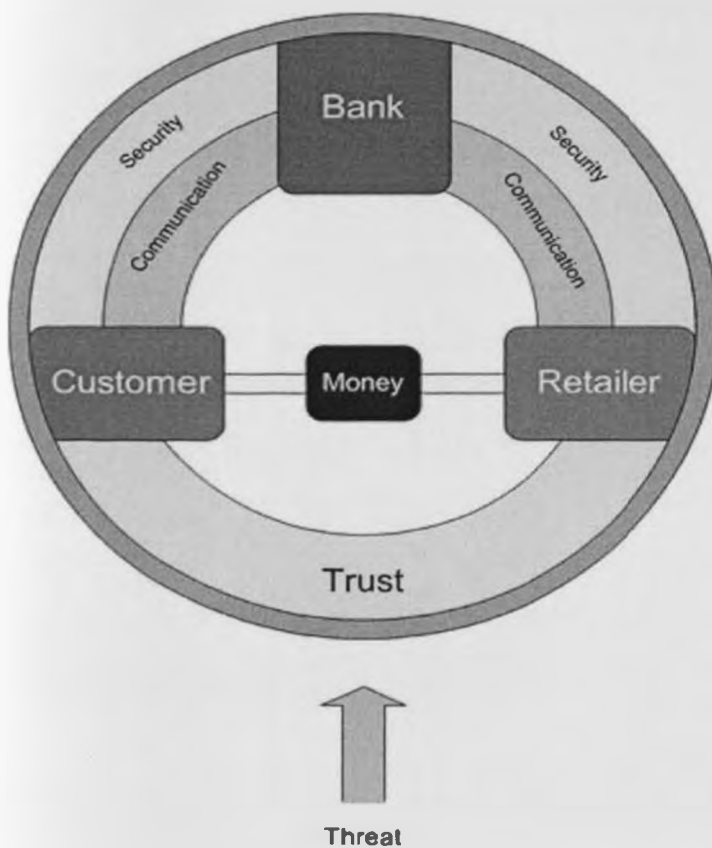


Figure 3: System Diagram (Venugopal and Beats, 1994; Shuliang Li, 2000)

The three main blocks represent the three parties in a secure transaction, the bank, the customer and the retailer. Both customer and retailer communicate with the bank

protected by a secure layer against the threat of a fraudulent attack from outside the system. The resulting protected communication creates trust between both parties. Finally, a secure encapsulated environment denoted by area within the outer dark ring protects against outer threats. These threats will always exist while economic gain is achievable by administering these threats (Shuliang, 2000).

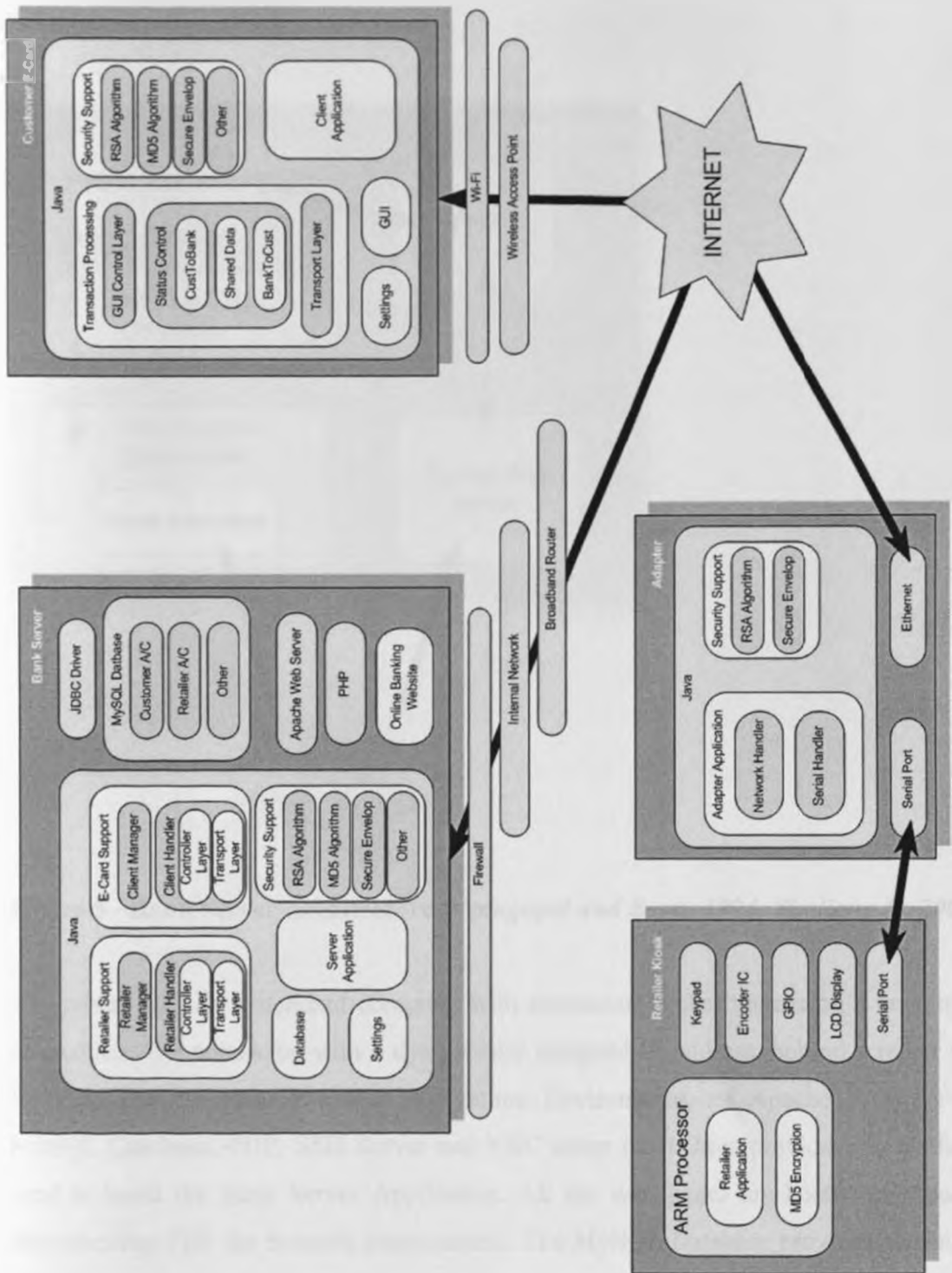


Figure 4 - Full System Architecture (Venugopal and Beats, 1994; Shuliang Li, 2000)

Bank Server

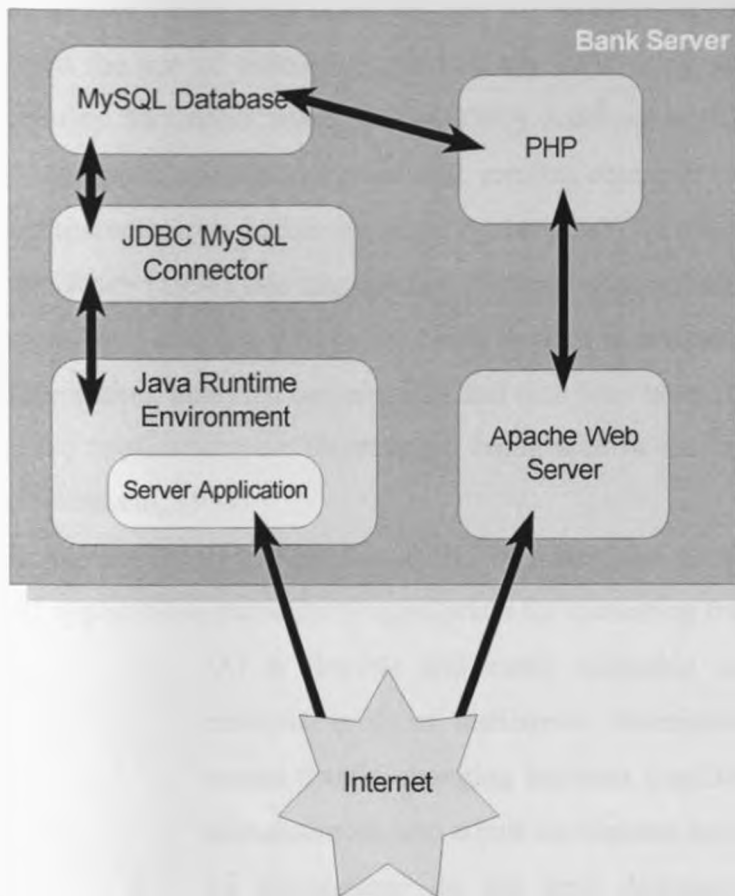


Figure 5 - Bank Server Architecture (Venugopal and Beats, 1994; Shuliang Li, 2000)

The server runs on a standard computer with connected to the Internet on a broadband connection. It's connected with a dynamically assigned IP address, behind a router and firewall. The computer has a Java Runtime Environment, an Apache Web Server, MySQL Database, PHP, SSH Server and VNC setup on it. Java provides the platform used to build the Bank Server Application. All the web pages are hosted on Apache incorporating PHP for dynamic page content. The MySQL Database provides content to the Java Application and to web page requests. SSH and VNC are used to remotely view and control the server (Shuliang, 2000).

2.6 Systems integration and Credit Card Fraud

Computer based fraud discovery and the reactions to such fraud, are increasingly based upon the use of technology, particularly tools using an artificial intelligence approach (Hurley, Moutinho, and Stephens, 1995). Artificial intelligence systems refer to 'a branch of computer science concerned with creating computer programs that can perform actions comparable with decision-making by humans' (Giarratano and Riley, 1994). Giarratano and Riley (1994) also suggest that "increasingly, techniques such as neural nets, genetic algorithms and fuzzy logic are being applied in business paradigms for a wide range of forecasting, analysis, optimization and data base tasks. It is not surprising therefore, that these applications are increasingly being seen in the development of combating fraud" (Giarratano, 1994).

In another report by Kingdon (1995), he asserts that there are three factors that have made AI applications particularly appropriate for combating fraud.

- i. 'AI is flexible and easily adaptable to the solutions developed. For example, artificial intelligence techniques learn from experience, which means that in changing business conditions a system can adapt to new circumstances, and adjust its response accordingly.
- ii. AI applications do not need designers to specify all the operating conditions under which they are to perform as they can learn from experience.
- iii. AI applications create innovations, as they are capable of finding relationship hitherto unknown. This means that AI system itself can contribute creatively to the detection process, finding new links and associations between patterns of fraud' (adapted from Kingdon, 1995d).

The development of hybrid intelligent systems for developing marketing strategies is another factor that has helped AI applications in combating fraud (Venugopal and Beats, 1994; Shuliang Li, 2000). According to Shuliang, (Ibid.), 'neural nets and genetic algorithms are seen as being used as a means for interrogating large customer databases in order to filter customer profiles for direct marketing, credit risk evaluation, and for consumer profiled profit analysis.'

The customer's terminal first needs to be authenticated to guarantee that all information that is sent over this link is secure. To test the security three challenges are presented to the connecting application.

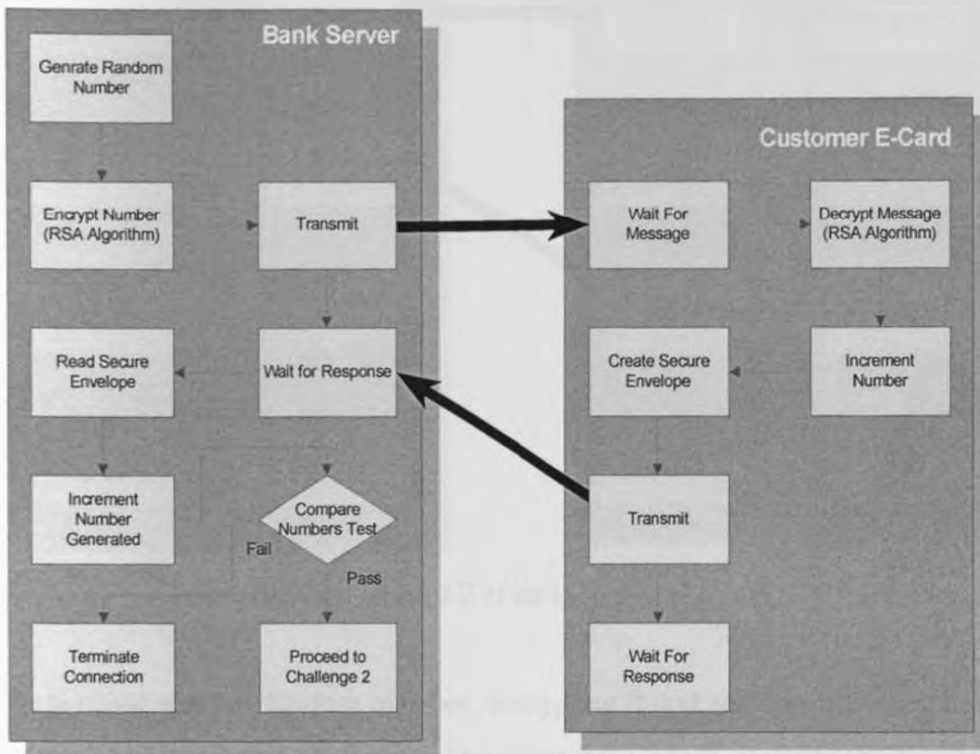


Figure 6 - Authentication Round 1 (Venugopal and Beats, 1994; Shuliang Li, 2000)

A random number is generated and is encrypted in the RSA algorithm and sent to the client. As the client's public key is unknown at this point the server cannot send the data in a secure envelope yet, and instead the information is encrypted only using the bank's public key. The client is expected to decrypt this message using this key, increment the number by one and encrypt the result with its own private key, followed by the bank's public key, creating the secure envelope. The cipher text and the client's public key are then sent to the bank for verification. If the decrypted cipher text received matches what is expected, the client has passed the first challenge. It can be assumed therefore that the RSA security channel is secure (Venugopal and Beats, 1994).

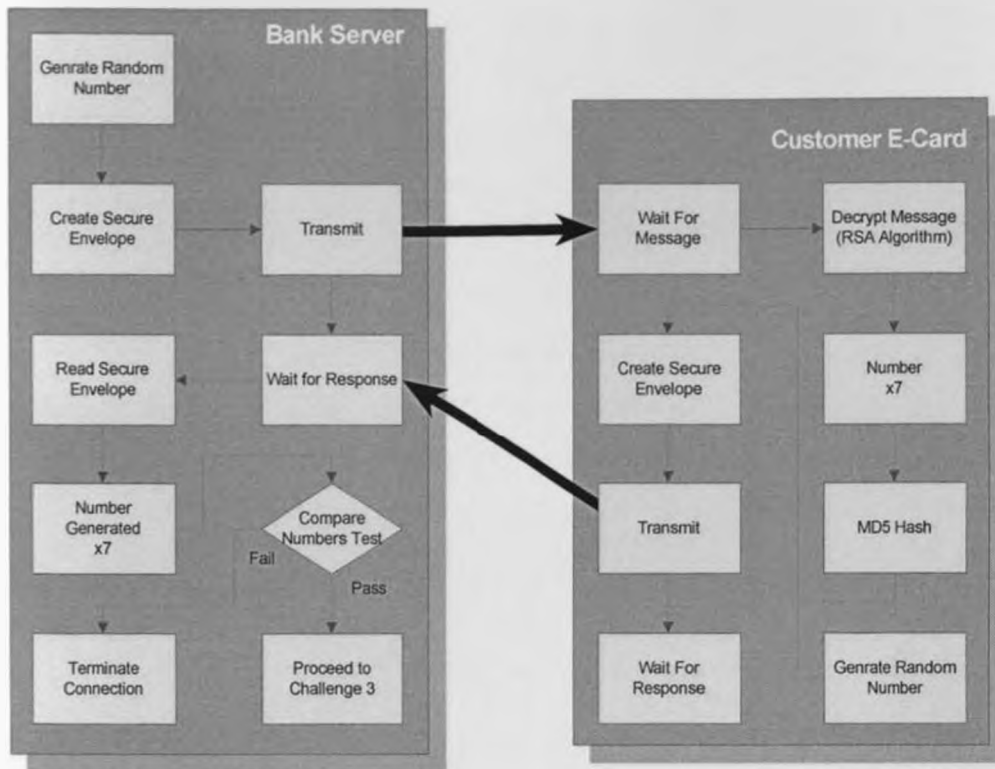


Figure 7 - Authentication Round 2 (Venugopal and Beats, 1994; Shuliang Li, 2000)

Generating another random number, encrypting it and sending it to the client creates the second authentication challenge. The client once again decrypts the number. The client must multiply this number by another arbitrary number; seven in this case and then hash it using the MD5 message digest algorithm. The client also generates another random number. This random number is included in a message with the result of the hashing, which is encrypted using RSA and sent back to the bank. The bank then performs the same operation and compares the recovered received value from the client. If they match then is now assumed that the Client Handler can trust client MD5 hashes (Trembly, 1993).

In the meantime the client multiplies the number it generated itself by the result of the number it received from the bank multiplied by seven. This result is then hashed using MD5 and the hash is held in memory until the next round.

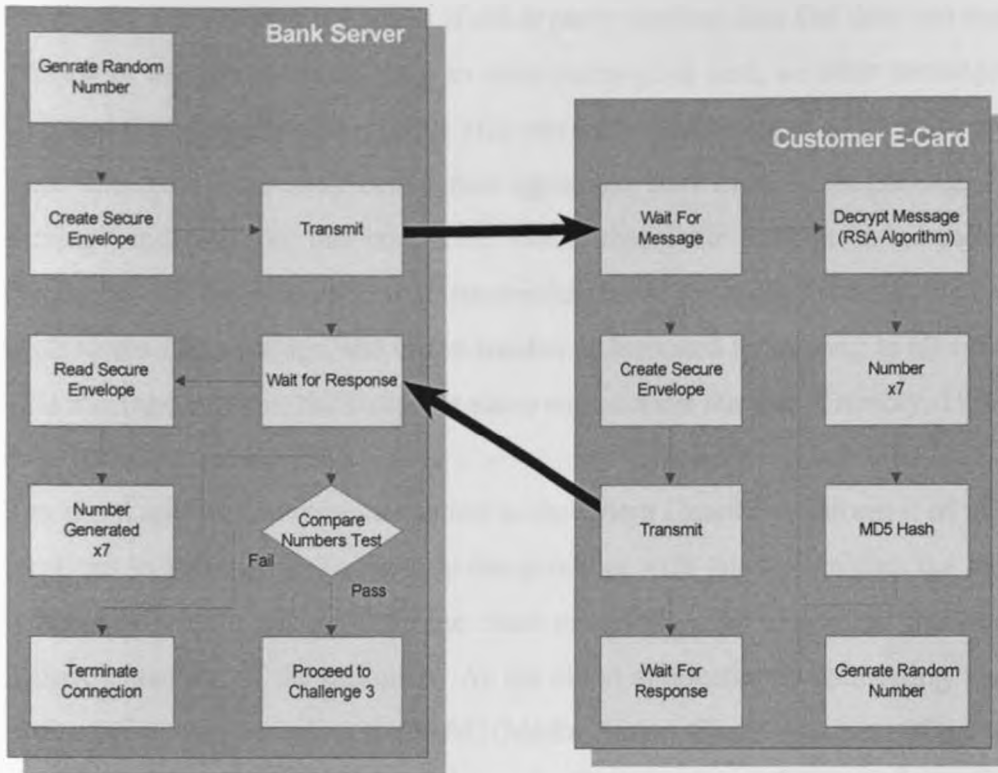


Figure 8: Bank server vs. Customer E-card (Venugopal and Beats, 1994; Shuliang Li, 2000)

The final authentication round begins by the client handler multiplying the last number it generated by the number it received from the client and finally by seven. This number is then MD5 hashed and sent encrypted to client application. The client application compares this value to the value it previously held in memory. If the client is satisfied that these values are the same it prompts the customer for a PIN number. The PIN number is then MD5 hashed and sent with the serial number of the customer's terminal in an encrypted message to the bank. The bank uses the serial number to identify which of its customers the client terminal belongs to. This information is read from the customer database, where the customers PIN number is also held. The PIN number is retrieved and then MD5 hashed. This hash is then compared to the hash received from the customer and if they are identical then the user is authenticated (Shuliang, 2000).

During the authentication process if either party receives data that does not match what it expects or any error occurs then an error message is sent, no other messages are dealt with and the connection terminates after ten seconds. The client application must log into bank through the gateway connection again and start from the beginning. A logged in message indicates to the connected client that their attempt to connect has been successful and the application has successfully passed the authentication process. Once the bank issues this message, the client handler is activated to respond to all other requests. This message contains the customer name and account number (Trembly, 1993).

The client application issues a request to the Client Handler to inform it of all local retail locations in its locality. To provide the customer with this information the bank uses the location information it has from the client and sends a list of retailers that neighbour the believed position of the customer. As the client application is connecting via a wireless access point, by forwarding the MAC (Media Access Control) address of the access point we can determine the approximate location of the customer (Dekker, 1995).

The range of transmission is limited especially in an urban location due to large concrete buildings and re-enforced concrete walls that hinder the transmission of the signal. Using the MAC address the bank can determine the physical location of the access point from its database, and hence determine the approximate location of the customer. While security is a fundamental of this system, it is also important the privacy and confidentiality of each customer should be maintained. For this reason retailers do not get informed of any customer details until the customer wishes to purchase something. When requested to make a transaction on behalf of a customer the Client Handler searches for the desired retailer and informs it of the client's name and account number (Kingdom, 1995).

2.7 Conceptual Framework

According to (Sekaran, 2003), a conceptual framework is a logically developed, described and elaborated network of interrelationships among the variables deemed to be integral to the dynamics of the situation being investigated. (Mathooko, Et al, 2007),

further states that the elaboration of the variables in the theoretical framework addresses the issues of why or how we expect certain relationships to exist and the nature and direction of the relationships among the variables of interest. Therefore it is a scheme of concepts (or variables) which the researcher will operationalize in order to achieve set objectives (Oso and Onen, 2009).

The conceptual framework of this study therefore is developed through explaining and ascertaining the relationships and interconnectivity of the objectives of the study.

All these constitute factors influencing the credit card fraud in Kenya Commercial Bank in Mombasa County. The dependent variable in this study is effects of credit card management in Kenya Commercial Bank and this is influenced by the various independent variables either singly or as a whole.

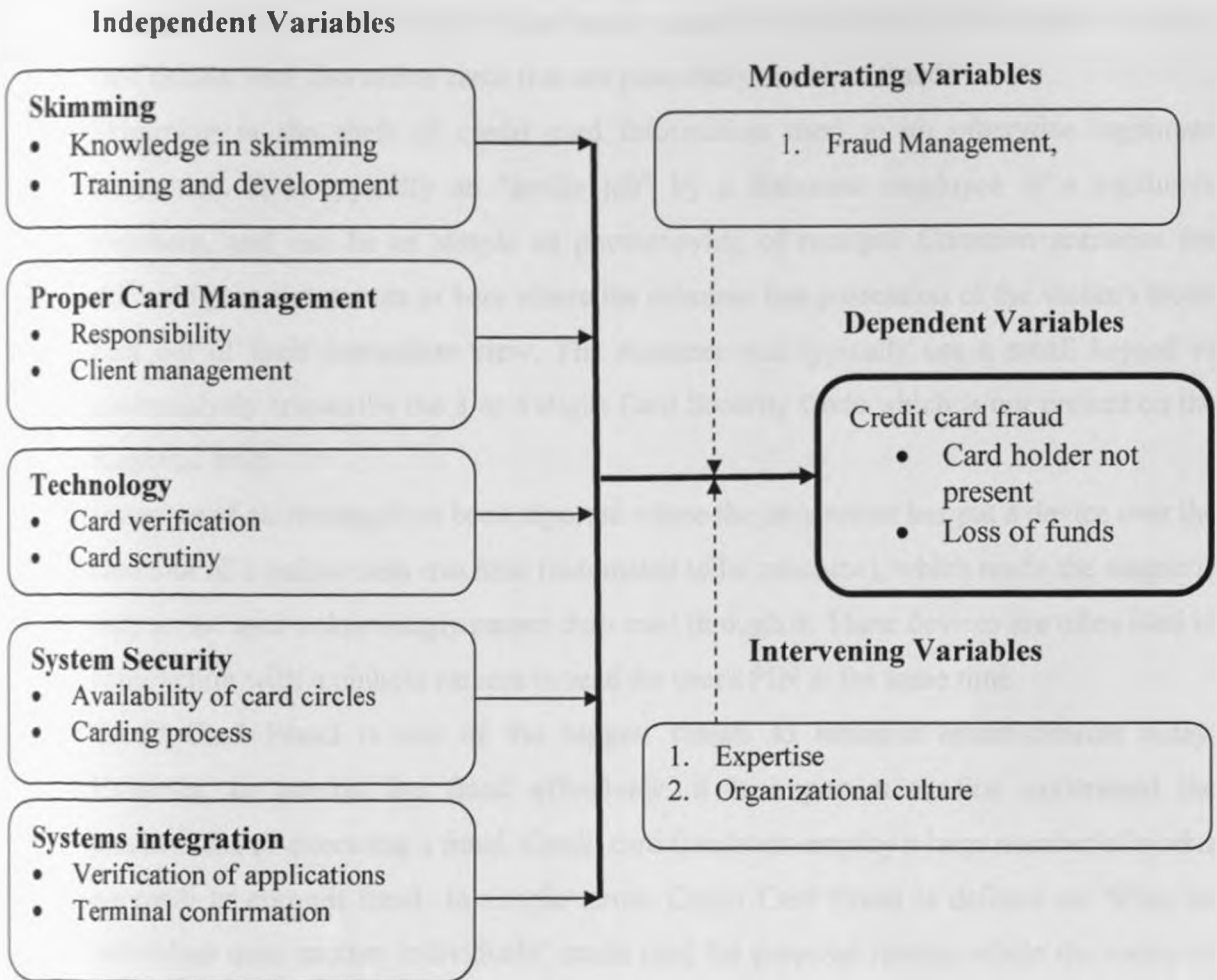


Figure 9: Conceptual Framework

The conceptual framework above shows the relationship between the variables of the study that guide the study. It shows how the independent variables (Skimming, proper leadership, Technology, Security system and System integration) affect the dependent variables (Rise in credit card fraud) moderated by credit card fraud management.

2.8 Summary of Literature

In the credit market literature, only a few studies make use of banking data to analyze the risk of fraud for a given set of credit cards (*i.e.* classic, gold and revolving credit cards). In this paper, a logit analysis has been conducted to assess which factors may lead to the

risk of fraud. Fraud has been defined as an unauthorized use of a credit card, including card details, and also stolen cards that are potentially at risk of fraud.

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant, and can be as simple as photocopying of receipts. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digits Card Security Code which is not present on the magnetic strip.

Instances of skimming have been reported where the perpetrator has put a device over the card slot of a public cash machine (automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's PIN at the same time.

Credit Card Fraud is one of the biggest threats to business establishments today. However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of modus operandi to commit fraud. In simple terms, Credit Card Fraud is defined as: When an individual uses another individuals' credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. Further, the individual using the card has no connection with the cardholder or issuer, and has no intention of either contacting the owner of the card or making repayments for the purchases made.

The transformation from traditional brick-and-mortar banking to E-Banking has been Automated Teller Machine (ATM) and thus the retail banking industry witnessed significant and extensive change. Formally, E-banking comprises various formats or technologies, including telephone (both land line and cell phone banking, direct bill payment (EFT), and PC or internet banking (Power, 2000). Weitzman, (2000), Lassar, Manolits and Lassar, (2005), Ehou and Chou (2000) identified five basic services associated with online banking: view account balances, and transaction histories, paying bills, transferring funds between accounts, requesting credit card advance, and ordering

checks. Majority of banks of banks is planning to introduce ICT for integration of banking service and new finance service, which will play a vital role in bringing efficiency in financial sector (Raihan, 2001). The most commonly factors are ease of use, transaction security, convenience and speediness.

As card business transactions increase, so too do frauds. Clearly, global networking presents as many new opportunities for criminals as it does for businesses. While offering numerous advantages and opening up new channels for transaction business, the internet has also brought in increased probability of fraud in credit card transactions. The good news is that technology for preventing credit card frauds is also improving many folds with passage of time. Reducing cost of computing is helping in introducing complex systems, which can analyze a fraudulent transaction in a matter of fraction of a second. It is equally important to identify the right segment of transactions, which should be subject to review, as every transaction does not have the same amount of risk associated with it. Finding the optimally balanced 'total cost of fraud' and other measures outlined in this article can assist acquiring and issuing banks in combating frauds more efficiently.

Laptop computers are also used in conjunction with small encoding devices to modify the encoded data on magnetic stripes. According to police officers, a pirate software with the relevant instructions circulate in Montreal. The program is especially designed to add or modify data encoded on the magnetic stripes of credit cards. Thus, with the right equipment and the appropriate technical knowledge, it becomes relatively easy to add the stolen data on the plastic. In the case of white plastic frauds the forger simply has to emboss the credit card numbers onto the plastic card with the help of an embossing machine. He can also have his cards embossed in an establishment specializing in the making of personalized identification cards (even though, as it happened, vigilant employees may realize that the numbers to be embossed are credit cards numbers and contact the police). Recently police officers have also stumbled upon white plastic card bearing magnetic stripe on their back.

Computer based fraud discovery and the reactions to such fraud, are increasingly based upon the use of technology, particularly tools using an artificial intelligence approach

(Hurley, Moutinho, and Stephens, 1995). Artificial intelligence systems refer to ‘a branch of computer science concerned with creating computer programs that can perform actions comparable with decision-making by humans’ (Giarratano and Riley, 1994). Giarratano and Riley (1994) also suggest that “increasingly, techniques such as neural nets, genetic algorithms and fuzzy logic are being applied in business paradigms for a wide range of forecasting, analysis, optimization and data base tasks. It is not surprising therefore, that these applications are increasingly being seen in the development of combating fraud”.

UNIVERSITY OF NAIROBI
KIKUYU LIBRARY
P. O. Box 20197
NAIROBI

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter examined the research design, the location of the study, population, sample size, data collection and data analysis procedures that was used during the study. It has describe in detail what has been done and how it was done.

3.2 Research Design

The research problem was studied through a descriptive survey design. Orodho (2003) defines a research design as the scheme, outline or plan that is used to generate answers to research problems. According to Cooper and Schindler (2003), a descriptive study is concerned with finding out the what, where and how of a phenomenon. Descriptive research design was chosen because it enables the researcher to generalize the findings to a larger population.

According to Mugenda and Mugenda (1999) it is important and appropriate to use data where subjects are observed in their natural setup without manipulating the environment. It is chosen because the study was not confined to the collection and description of the data, but it investigated and established the existence of certain relationship among the variables under investigation.

3.3 Target Population

According to Ngechu (2004), a population is a well defined or set of people, service, elements, events, group of things or households that are being investigated. Population studies are more representative because everyone has equal chance to be included in the final sample that is drawn (Mugenda and Mugenda 1999).

The target population of this study was 1200 comprising of employees and some customers who were sampled randomly as they came to the Branch.

3.4 Sample Size and Sampling Procedure

Statistically, in order for generalization to take place, a sample of at least 30 must exist (Cooper and Schindler, 2003). Moreover large sampling minimizes errors. Kotler (2001) argues that if well chosen, samples of about 10% of a population can often give good reliability. Other literatures have shown that sample size selection to a greater extent is judgmentally decided.

The appropriate sample size for a population-based survey is determined largely by three factors:

- (i) The estimated prevalence of the variable of interest – Credit card fraud in this instance
- (ii) The desired level of confidence
- (iii) The acceptable margin of error.

For a survey design based on a simple random sample, the sample size required can be calculated according to the following formula.

Formula:

$$n = \frac{t^2 \times p(1-p)}{m^2}$$

Key:

n = required sample size

t = confidence level at 95% (standard value of 1.96)

p = estimated customers in the study area

m = margin of error at 5% (standard value of 0.05)

$$n = \frac{1.96^2 \times .9(1-.9)}{.05^2}$$

$$n = \frac{3.8416 \times .9}{.0025}$$

n = $\frac{3.4374}{.0025}$
n = 120

The sample of this study consisted of a total of 120 respondents selected from all Kenya Commercial Bank Branches within Mombasa County, made up of 20 employees from the upper level management and 80 from middle level management and 20 customers who were sampled randomly as they visit the bank..

The sample size of the study was as shown in the table below;

Table 3.1: Sample size

Section	Frequency	Percentage	Sample Size
Upper level Employees	200	10%	20
Lower level employees	800	10%	80
Customers	200	10%	20
	1200		120

Key:

Upper level employees comprise of Regional Manager, Branch Manager and Ass. Manager

Lower level employees: comprise of Tellers, Senior Cashiers, Customer Care Officers, clerks and back office staff.

3.5 Data Collection Methods

The researcher used a questionnaire for Kenya Commercial bank employees as primary data collection instrument. According to Sproul (1998), a self administered questionnaire is the only way to elicit self-report on peoples opinion, attitudes, beliefs and values. The questionnaire was design to give a brief introduction of the employees and customers. The questionnaire was divided into sections representing the various variables adopted for the study.

For each section of the chosen study included closed structured and open ended questions which assisted to seek the views, opinion and attitude from the respondent which might

not have been captured by the researcher. The questions were designed to collect qualitative and quantitative data. The open ended questions gave unrestricted freedom of answers to respondents.

3.6 Data Collection Procedure

Data collection procedures will represent the actual information that was obtained for the purpose of the research study; it included raw facts like answered questionnaires', recorded interviews and observed facts. The questionnaires was administered through drop and pick method to the offices of the selected respondents except for the customers who filled the questionnaires while in the banking hall.

3.7 Validity and Reliability of Research Instruments

3.7.1 Validity of Research instrument

According to Berg and Gall (1989) validity is the degree by which the sample of test items represents the content the test is designed to measure. Content validity which is employed by this study is a measure of the degree to which data collected using a particular instrument represents a specific domain or content of a particular concept. Mugenda and Mugenda (1999) contend that the usual procedure in assessing the content validity of a measure is to use a professional or expert in a particular field. To establish the validity of the research instrument the researcher seeked opinions of experts in the field of study especially the researcher's supervisor and lecturers in the department. These facilitate the necessary revision and modification of the research instrument thereby enhancing validity.

3.7.2 Reliability of the Research Instruments

According to Shanghverzy (2003), reliability refers to the consistency of measurement and is frequently assessed using the test-retest reliability method. Reliability is increased by including many similar items on a measure, by testing a diverse sample of individuals and by using uniform testing procedures (ibid). The researcher selected a pilot group of

10 individuals from the target population to test the reliability of the research instruments. This was achieved by first stratifying the individuals according to level of management, level of education and number of years worked. The researcher did put into consideration gender equity and geographical background of individuals.

The pilot study allowed for pre-testing of the research instruments. The clarity of the instrument to the respondents was established so as to enhance the instrument's validity and reliability. The pilot study enabled the researcher to be familiar with research and its administration procedures as well as identifying items that required modification. The result helped the researcher to correct inconsistencies that arose from the instruments, which ensured that they measured what was intended.

According to Cooper and Schindler (2003), the pilot group can range from 25 to 100 subjects depending on the method to be tested but it does not need to be statistically selected. This will be in line with a qualitative research design methodology employed in this research project.

3.8 Data Analysis Techniques

Before processing the responses, the completed questionnaires were edited for completeness and consistency. The data was then coded to enable the responses to be grouped into various categories. Data collected was both quantitative and qualitative and it was analyzed using descriptive statistics. The descriptive statistical tools such as Microsoft Excel and xlstat helped the researcher to describe the data and determine the extent used. The findings are represented using tables. The likert scale will be used to analyze the mean score and standard deviation, this has helped in determining the extent in which credit card fraud has impacted on the Banks revenue. Data analysis used Statistical Package of Social Scientist (SPSS) for tabulations, means and other central tendencies. The research hypothesis was tested by use of chi-square, correlation and regression to be able to identify any relationships between the variables of the study. Tables have been used to summarize responses for further analysis and to facilitate comparison.

3.9 Ethical Considerations

Due to sensitivity of some information collected, the researcher holds a moral obligation to treat the information with utmost propriety. Since the respondents were reluctant to disclose some information, the researcher assured the respondents of confidentiality of the information given.

3.10 Operational Definition of Variables

The researcher attempted to show the relationship among independent variables and dependent variable. The table 3.2 below summarized the key variables that guided the study.

Table 3.2 Operational Definition of Variables

Variable	Indicators	Measure	Scale	Data Analysis Tools
Dependent Variable Credit card fraud	1) Revenue lost	Income per month	Ratio	Chi-Square test
	2) Cards stolen	Number of cards reported lost	Nominal Scale	
	3) Fraudulent accounts	Number of fraudulent accounts opened		Nominal Scale
	4) Fake Identification documents	Number of fake identification documents used to open accounts	Median	

				Nominal Scale	
Independent Variable	1) Fake cards	Number of reported fake cards	of	Nominal Scale	Chi-square test
Skimming	2) Hot cards	Number of cards cancelled in the system		Nominal Scale	Mean Mode Median
	3) Plastic cards	Number of plastic cards produced for transaction		Nominal Scale	
Proper Management	1) Transparency and Accountability	Extent of Transparency and Accountability in card handling	of	Interval	Chi-square test
	2) Disclosure standards				Mean
	3) Controls	Strictness of the standards		Ordinal Scale	Mode
		Types and stringent controls		Ordinal Scale	Median
Technology	1) Servers in place	Types of servers and applications running in them		Nominal Scale	Chi-square test
	2) Card management			Nominal	

	system	Kind of Card	Scale	Mode
	3) Computerized help desk	management system		
	4) Call centre	Service desk applications	Interval Scale	Median
		Number of staff in call centre and their competency	Nominal Scale	Mean
Security System	1) Type of firewall	Type of firewall	Nominal Scale	Chi-square test
	2) Outsourcing of card manufacture	Competency of the Company	Ordinal Scale	Mode
	3) Strong antivirus			
	4) Deleting of drop doors	Number of times Antivirus is updated	Interval	Mean
		Management of new systems	Nominal Scale	Median
Systems Integration	1) User training	Number of staff trained in new systems	Nominal Scale	Chi-square test
	2) System platform			
	3) Update of applications			Mean
	4) User Involvement	Type of platform running in the bank	Nominal Scale	
		Number of times the application is	Nominal	Mode

		updated	Scale	
		How often are users involved in system integration	Interval Scale	Median
Moderating Variable	1) Fraud detection systems	Number of fraud detection systems in place	Nominal Scale	Mode
Fraud Management	2) Systems Audit	Number of times the Audit is done	Nominal Scale	Mean

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

The study investigated the factors influencing credit card fraud in Kenya Commercial Bank Mombasa County. This was in light of the fact that many banks currently are losing a lot of funds to fraud stars due to credit card frauds. Despite the efforts by many private institutions and Kenya Institute of Bankers carrying out trainings on how to detect and prevent frauds before they can occur. Data collected yielded nominal values with the exception of numerical data requiring years of experience of the Bank employees and age of all the respondents. The data is presented using frequency distribution tables and percentages. In all instances the chi-square statistic was calculated to test the significance in the relationship between variables. The relevant measures of association for nominal data were then calculated for all significant relationships in order to determine the degree of correlation between the variables.

4.2 Response rate

Questionnaires were administered to 120 respondents. A total of 100 questionnaires were collected giving a response rate of 83.31%. According to Mugenda and Mugenda (2003), studies using questionnaires to collect data usually have a lower response rate of below 50%. This response rate is high thus the results are reliable and can be applied to the entire population as shown in table 4.1.

Table 4.1: Response Rate

	Respondents	Non-Respondents	Percentage
Senior Management	20	5	75%
Other KCB Employees	80	15	81.25%
Customers	20	-	100%
Total	120	20	83%

Out of the 120 questionnaires distributed to the respondents, only 100 fully filled forms were returned. The Senior Management had a response rate of 75% while the customers had 100% of the total questionnaires distributed. All the 20 customers who had been chosen in the sample managed to fill their questionnaires while in the banking hall. The rest of the Kenya Commercial Bank employees had a response of 81.25%. This gives a satisfactory response rate of 83%. This implies that the researcher can generalize the findings as the response is a true a representation of the population of study.

4.3 Demographic Characteristics of the Respondents

The study wanted to find out the level of management, years of experience and age of the respondents the study. This was done in order to profile the respondents based on this characteristics. The results of their level of management, age and years of experience in the organization are presented in table 4.2, table 4.3 and table 4.4 respectively.

Table 4.2: Summary of respondents on Level of Management

Level of Management	Frequency	Percentage
Regional Manager	5	6.3
Branch Manager	10	12.5
Ass. Manager	5	6.3
Section Head	4	5
Front office staff	6	7.5
Back Office Staff	50	62.5
Total	80	100

The banks positions had been categorized as per the levels of management in any given branch of Kenya Commercial Bank. Out of 80 respondents 6.3% are Regional Managers, Branch Managers are 12.5%, Assistant Managers are 6.3%, Heads of Departments are 5%, Section Heads are 7.5% and the rest which comprised of Tellers, Customer care officers, clerks were making up 62.6%. This is relevant to the study as each level of the Banks employees were represented in the sample used by the researcher.

Table 4.3: Age of Respondents

Age Bracket	Frequency	Percentage
20 - 25	12	12%
25 - 30	28	28%
30 - 35	40	40%
35 - 40	12	12%
40 - 45	3	3%
45 - 50	2	2%
Above 50	3	3%
Total	100	100%

The distribution of the respondents according to their ages were as follows: 12% were in the 20 – 25 years bracket, 28% in the 25 – 30 years bracket, 40% in the 30 – 35 years bracket, 12% in the 35 – 40 years bracket, 3% in the 40 – 45 years bracket, 2% in the 45 – 50 years bracket while 3% are above 50 years of age. The results show that the average age for both the Kenya Commercial Bank employees and their customers is between 30 – 35 years. This is relevant to the study as this shows the age in which it contributes to the bank being hit by fraud stars and also the customers affected by the credit card fraud.

Table 4.4: Profile of Respondents on Years of Experience

Number of Years Worked	Frequency	Percent
Below 1 year	8	10.0
1-5 years	55	68.8
5 - 10 years	11	13.8
10 - 15 years	4	5.0
Above 15	2	2.5
Total	80	100.0

The results in Table 4.4 shows that 10% of the respondents have worked in the Bank below one year, 68.8% of the respondents have worked in the bank between 1 – 5 Years, 13.8% of the respondents have worked in the Bank between 5 – 10 years, 5% of the respondents have worked in the bank between 10 – 15 Years and 2.5% of the respondents

have worked in bank above 15 years. This result is important for the study as it shows that a larger number of employees have been in the bank for less than 5 years and this could be one of the reasons why there has been a rise in credit card fraud due to lack of enough experience to detect and eradicate frauds.

4.4 Skimming and Credit Card Fraud in the Banking Sector

The study sought to establish whether skimming is a factor influencing credit card fraud. The results in Table 4.6 below shows the respondent’s knowledge in credit card skimming the response was as follows. 25% of the respondents have knowledge in credit card skimming while 75% of the respondents don’t have knowledge at all in credit card skimming. These findings are very valid to the study as credit card skimming was a factor that contributes to credit card fraud and this shows that many employees in the bank didn’t have knowledge in the credit card skimming and this might have been the reason why credit card fraud has been rising in the bank.

Table 4.5: Respondents Knowledge on Credit Card Skimming

Do you have knowledge in credit card skimming		Frequency	Percent
All employees	yes	20	25.0
	No	60	75.0
Total		80	100%

The study also sought to establish whether there was any training conducted for staff during their years of operations in the bank to be able to sensitize them on credit card fraud and especially credit card skimming. Table 4.6 shows the respondents results on Training on Credit Card skimming, 19% of the respondents have been trained by the Bank on credit card skimming while 81.2% haven’t been trained on the credit card skimming. The findings on this table is very valid to the study this is because lack of training to a large number of staff makes staff incompetent to detect the credit card skimming which is a factor to credit card fraud.

Table 4.6: Respondents Training on Credit Card Skimming

Were you trained on credit card skimming		Frequency	Percent
All Employees	Yes	15	19
	No	65	81
Total		82	100

The data was analyzed using the Chi-square statistic to determine if lack of knowledge in credit card skimming has a significant effect on credit card fraud in the banking sector. An alpha level of 0.05 was adopted for all statistical tests. The analysis was done based on the following hypothesis.

H₀: Knowledge in skimming is not a factor influencing credit card fraud in the banking sector.

H₁: Knowledge in skimming is a factor influencing credit card fraud in the banking sector

Table 4.7: Summary of the Chi-square statistic Based on Knowledge in Skimming and influence on credit card fraud in the Banking sector

	Pearson Chi-Square Value	Asymp. Sig. (2 sided)	Fishers Exact Test [Exact Sig. (2 sided)]
Training in skimming	8.453	0.160	0.372
Knowledge in skimming	12.035	0.459	1.001

The results of table 4.7 indicate that there is a significant relationship between lack of knowledge in credit card skimming and the influence of credit card fraud in the banking sector. The Chi-square indicates significant values on the influence of credit card fraud by the knowledge in credit card skimming. However 50% of the cells on the relationship between having knowledge in credit card skimming and influence of credit card fraud had an expected count of less than five. The researcher therefore determined that the Chi-Square test may not have been accurate. The Fishers Exact Test was thus applied while interpreting the results.

This result (= 0.372) lent support to the Chi-Square results. Therefore the null hypothesis is rejected meaning that the knowledge in credit card fraud is a factor influencing credit card fraud in the banking sector.

The researcher further calculated the Phi (ϕ) coefficient to determine the degree of correlation between the two variables. The Phi coefficient can be thought of as a Pearson Product Moment Correlation for categorical variables. It is a measure of the nominal association applicable only to 2 contingency tables (Scanlan, n.d). A value of 0.196 was obtained for knowledge in credit card skimming and 0.181 for whether skimming is a factor influencing credit card fraud. Both these values indicate a weak association between the variables and the knowledge in credit card skimming between 18.1% - 19.8% of the factors influencing credit card fraud

4.5 Proper card Management and Credit Card Fraud in the Banking Sector

The study sought to establish whether proper card management is a factor influencing credit card fraud in the banking sector. The result of the study is shown in table 4.8 where 75% of the respondents indicated that card management system was the responsibility of Customer Care Officer.

Table 4.8: Respondents on Card Management Systems Responsibility

Whose is responsible for card management system	Frequency	Percent
Branch Manager	9	11.3
Customer care officer	60	75.0
Teller	7	8.8
Clerks	4	5.0
Total	80	100

The results in table 4.8 shows the group of staff responsible for Card Management System and the findings were as follows. 11.3% of the respondents stated that Branch Managers are responsible for card management system, 75% of the respondents showed that it is the responsibility of Customer care officers, 8.8% of the respondents stated that it is the responsibility Tellers to manage card management system while 5.5% of the

respondents stated that it is the responsibility of Clerks. These results are very valid for the study reason being Customer Care Officers are the group of staff close to the customers and need to manage all customer systems for them to mitigate the frauds from occurring as they understand the customers better than anyone else in the bank.

The data was analyzed using the Chi-square statistic to determine if lack of proper card management has a significant effect on credit card fraud in the banking sector. An alpha level of 0.05 was adopted for all statistical tests. The analysis was done based on the following hypothesis.

H₀: proper card management is not a factor influencing credit card fraud in the banking sector.

H₁: Proper card management is a factor influencing credit card fraud in the banking sector

Table 4.9: Summary of Chi-square Analysis based on Card Management System and credit card fraud

Test of independence between the rows and the columns (Chi-square):

Chi-square (Observed value)	20.044
Chi-square (Critical value)	5.991
DF	2
p-value	0.001
alpha	0.05

Test interpretation:

H₀: Proper card management is not a factor influencing credit card fraud

H1: Proper card management is a factor influencing credit card fraud.

The computed probability value (p) is lower than the significance level $\alpha = 0.05$, then the null hypothesis H0, is rejected and the alternative hypothesis H1 is accepted.

Therefore this shows that proper card management is a factor influencing credit card fraud in the banking sector.

4.6 System integration and credit card fraud in the banking sector

The study sought to access whether system integration is a factor influencing credit card fraud. The findings from the study showed that 60% of the respondents indicated that the systems are not verified and there is no mechanism in the bank to even verify new applications to be able to detect any fraudulent applications. table 4.9 shows the results of the findings.

Table 4.10: Percentage Respondents on Vetting of system Integration

Is there a mechanism in place to verify system and new applications before they are integrated		Frequency	Percent
All Employees	Yes	25	31
	No	55	69
Total		80	100

The results on table 4.9 shows whether all customers' application for credit cards are vetted for fraudulent applications before customers are allocated credit cards. 31% of the respondents indicated that customer's applications are vetted before card allocation while 68% of the respondents stated that customer's applications are not vetted for fraudulent applications before new cards are allocated. These findings are very valid for this study because it shows that fraud stars can make applications for new cards and since they are not vetted this means that the Bank could be prone to credit card fraud.

The data was analyzed using the Chi-square statistic to determine if lack of proper card management has a significant effect on credit card fraud in the banking sector. An alpha level of 0.05 was adopted for all statistical tests. The analysis was done based on the following hypothesis.

H₀: System Integration is not a factor influencing credit card fraud in the banking sector.

H₁: System Integration is a factor influencing credit card fraud in the banking sector

Table 4.11: Summary of Chi-square Analysis based on System Integration

And credit card fraud

Test of Independence between system integration and credit card fraud

Chi-square (Observed value)	34.278
Chi-square (Critical value)	8.131
DF	4
p-value	0.001
Alpha	0.05

Test interpretation:

H₀: There was no relationship between system integration and credit card fraud in the banking sector

H₁: There was a relationship between system integration and credit card fraud In the banking sector

The computed p-value is lower than the significance level $\alpha=0.05$, the null

Hypothesis H₀ is rejected, and the alternative hypothesis H₁ is accepted. This is then

concluded that there is a relationship between system integration and credit card fraud in the banking sector.

Further, the Fishers Exact test was applied to ascertain the test and the interpretation.

Fisher's exact test:

p-value (Two-tailed) < 0.001
 alpha 0.05

Test interpretation

H0: There was no relationship between system integration and credit card fraud in the banking sector

H1: There was a relationship between system integration and credit card fraud in the banking sector

As the computed p-value is lower than the significance level $\alpha=0.05$, the null hypothesis H0, is rejected and the alternative hypothesis H1 is accepted.

Table 4.12: Percentage Respondents on Training of Customers on safe card usage

Are the customers trained on safe card usage	Frequency	Percent
Yes	12	60
No	8	40
Total	20	100

The results on table 4.10 shows the results of the customers responds as to whether they are trained on safe card usage as they are being issued with credit cards by the bank as

follows. 60% of the respondents indicated that they are trained on safe use of credit card by the bank employees, while 40% of the respondents indicated that they weren't trained as they were being issued with the credit cards. These results shows that most of the customers are trained during credit card issue and some just learn it through the hard way after their cards have been skimmed or stolen this encourages the fraud starts to continue posing as customer assistants in ATM lobby.

4.7 System Security and Credit Card Fraud in the Banking Sector

The study sought to examine the extend in which system security influences the credit card fraud in the banking sector. The results show that the respondents were not aware whether the system was secure or not this is because only 32% of the customers indicated that the system was secure.

The results in table 4.10 show how the bank system is vulnerable to external threats as follows. 18.8% of the respondents indicated that the bank system is very secure from external threats, 32.5% of the respondents indicated that the bank system is secure from external threats, 25% of the respondents indicated that the bank system is somehow secure, 10% of the respondents indicated that the bank system is not secure while 13.8% of the respondents don't know whether the bank system is secure or not. This results are valid for the study because if the bank system is vulnerable to the external threats that means that the bank data can be stolen so easily by fraud stars and this can increase credit card fraud. The study had sought to establish whether system security is a factor influencing credit card fraud. From the findings in table 4.11 it shows very clearly that the banking system is not secured enough against external threats such and this affirms the researcher's objective that system security is a factor influencing credit card fraud in the banking sector.

Table 4.13: Percentage Respondents on External Threats to System Security

How secure is the banking system against external threats	Frequency	Percent
Very Secure	15	18.8
Secure	26	32.5
Somehow secure	20	25.0
Not secure	8	10.0
Don't know	11	13.8
Total	80	100%

CHAPTER FIVE

SUMMARY OF FINDINGS, DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter represents the summary of the findings of the data collected, discussions, conclusions and proposed recommendations. The findings were based on five objectives of the study one of which was to establish how skimming is a factor influencing credit card fraud in the banking sector. The second is to determine how technology influences credit card fraud in the banking sector. The study also sought to assess how proper card management contributes to credit card fraud in the banking sector. The fourth is to ascertain how system security contributes to credit card fraud in the banking sector. The study also sought to examine how system integration is a factor influencing credit card fraud in the banking sector.

5.2 Summary of Findings

The response rate for this study was 83.31% with the employees and customers of Kenya Commercial Bank responding in the study. Most of the respondents in the bank were bank employees of the lower rank that is Tellers, Customer care officers and clerks, Majority of the respondents were female whereas of the employees have only been in the bank between 1 – 5 years.

The study sought to establish whether skimming was a factor influencing credit card fraud in the banking sector. The study found out that skimming is a factor influencing credit card fraud due to lack of training of bank employees on the credit card skimming. 81.3% of Kenya Commercial Bank employees were not trained on credit card skimming. The study also found out that 75% of the respondents indicated that they lack knowledge in credit card skimming and this means that they are unable to discover the skimmed cards.

The study sought to establish whether proper card management was a factor that influences credit card fraud in the banking sector. The results showed that the respondents seem not to be aware of the person or group of persons who are responsible for proper card management system this is because 11% of the respondents indicated that the Branch Manager is responsible, 75% of the respondents indicated that customer care officer were responsible, 9% of the respondents indicated that Tellers were responsible and 5% indicated that clerks were responsible. This shows that the bank doesn't have a laid down policy on who exactly is responsible and this is a very big weakness that can be used by fraudsters to capitalize on credit card fraud.

The study sought to establish whether systems security is a factor influencing credit card fraud in the banking sector. The study revealed that the bank has a security system in place in that there was a firewall but the respondents gave various views as how the system was secure from external threats 18.8% of the respondents indicated that they system was very secure from external threats, 32.5% of the respondents indicated that the system was secure, 25% of the respondents indicated that the systems was somehow secure, 10% of the respondents indicated that the system was not secure while 13.8% of the respondents were not sure of system security from external threats and this means that the bank systems are vulnerable to external threats and especially black hackers who steal data for malicious use. This shows that system security is a factor that contributes to credit card fraud.

Finally, the study sought to establish whether authentication of documents is a factor influencing credit card fraud in the banking sector. The study revealed that new applications are partly verified or scrutinized for fraudulent applications. 32% of the respondents indicated that credit cards are scrutinized before a card is issued, while 68% of the respondents indicated that the new applications are not authenticated or scrutinized for fraudulent applications before new cards are issued. This shows that this is a lop hole which fraudsters can use to steal from the bank and as such authentication of documents is a factor that influences credit card fraud.

5.3 Discussions

The study found out that credit card skimming is the most significant influence on credit card fraud. According to Kingdom (1995) credit card skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant, and can be as simple as photocopying of receipts. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Recent studies carried out by other researchers such as Annese (2003) has shown that skimming can transfer large sums of money. In a New York crime ring, about \$3.5 million was stolen before the criminals were apprehended. This case involved greater than 20 ATM machines, thousands of ATM cards, 1,400 cards issuers, and in excess of 26,000 ATM transactions. "Most ATM activity occurs during the evening" and the thieves rarely stay in the Same area for more than seven to ten days. The "counterfeit cards (are) produced within 24 hours" and fraudulent transactions are performed within 24 to 48 hours after the swipe data and PIN are stolen. Other skimming cases in the United States have been reported in – Boca Raton, Florida, Illinois, Kansas, Maryland, Virginia, Wisconsin, South Carolina, and Colorado.

But skimming is not just of national concern, it is also an international problem. Cases have been reported in Australia, South Africa, France, Spain and many other parts of the world. The Australian Crime Commission estimates that skimming is responsible for \$300 million a year in that country and that much of this crime is being committed by organized crime rings linked with Malaysia, Indonesia, Hong Kong and Thailand. And Ian McKindley, Head of Fraud Control with Visa International, reports that in the last year, skimming increased by 300 percent. As per classified information in the bank, Kenya commercial Bank lost Kshs. 16,000.000/- in the year 2011 alone and these figures

could not be published due to customers concerns. Thus this finding is consistent with literature.

The study found out that proper management of card system was a major factor that influences credit card fraud in the banking sector. Contrary to popular belief, merchants are far more at risk from credit card fraud than the Cardholders. While consumers may face trouble trying to get a fraudulent charge reversed, merchants lose the cost of the product sold, pay chargeback fees, and fear from the risk of having their merchant account closed. Increasingly, the *card not present* scenario, such as shopping on the internet poses a greater threat as the merchant (the web site) is no longer protected with advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the 'physical world' checks necessary to detect who is at the other end of the transaction. This makes the internet extremely attractive to fraud perpetrators. According to a recent survey, the rate at which internet fraud occurs is 12 to 15 times higher than 'physical world' fraud. However, recent technical developments are showing some promise to check fraud in the card not present scenario (Bolton and Hand, 2002) Recent studies has shown that technology for detecting credit card frauds is advancing at a rapid pace – rules based systems, neural networks, chip cards and biometrics are some of the popular techniques employed by Issuing and Acquiring banks these days.

Apart from technological advances, another trend which has emerged during the recent years is that fraud prevention is moving from back-office transaction processing systems to front-office authorization systems to prevent committing of potentially fraudulent transactions. However, this is a challenging trade-off between the response time for processing an authorization request and extent of screening that should be carried out (Bhatla, 2003). He further stated that an efficient fraud management solution is one that minimizes the total cost of fraud, which includes the financial loss due to fraud as well as the cost of fraud prevention systems. Too often success is mistakenly measured exclusively by one metric –the monthly chargeback rate (Chargeback rate is defined as

the percentage of chargeback amount with regard to the net transaction amount). To minimize the actual *total cost* of fraud, an optimal balance needs to be achieved between reducing fraud losses and overheads associated with review of transactions. Reviewing the appropriate number of transactions is the key to achieve this optimal balance. This finding is consistent with literature.

The second most significant factor that influenced credit card fraud in the banking sector is system security. This is consistent with literature. Many organizations have firewalls that prevents intrusion from the external world and especially the unauthorized access but all the organizations don't take time to test the dump proof of such systems which are very vulnerable and are bound to be hacked every time. Recent studies done by Association of payment clearing services (2005) Laptop computers are also used in conjunction with small encoding devices to modify the encoded data on magnetic stripes. According to police officers, pirate software with the relevant instructions circulate in Montreal. The program is especially designed to add or modify data encoded on the magnetic stripes of credit cards. Thus, with the right equipment and the appropriate technical knowledge, it becomes relatively easy to add the stolen data on the plastic. In the case of white plastic frauds the forger simply has to emboss the credit card numbers onto the plastic card with the help of an embossing machine. He can also have his cards embossed in an establishment specializing in the making of personalized identification cards (even though, as it happened, vigilant employees may realize that the numbers to be embossed are credit cards numbers and contact the police). Recently police officers have also stumbled upon white plastic card bearing magnetic stripe on their back.

In the past, carders used computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which valid accounts were. Another variation would be to take false card numbers to a location that does not immediately process card numbers, such as a trade show or special event. However, this process is no longer viable due to widespread requirement by internet credit card processing systems for additional data such as the billing address, the 3 to 4 digit Card Security Code and/or

the card's expiry date, as well as the more prevalent use of wireless card scanners that can process transactions right away. Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by skimming or phishing (Trembley, 1986). Systems integration had the least influence on credit card fraud but was still a significant factor, a fact consistent with most literature. Computer based fraud discovery and the reactions to such fraud, are increasingly based upon the use of technology, particularly tools using an artificial intelligence approach (Hurley, Moutinho, and Stephens, 1995). Artificial intelligence systems refer to 'a branch of computer science concerned with creating computer programs that can perform actions comparable with decision-making by humans' (Giarratano and Riley, 1994). Giarratano and Riley (1994) also suggest that "increasingly, techniques such as neural nets, genetic algorithms and fuzzy logic are being applied in business paradigms for a wide range of forecasting, analysis, optimization and data base tasks. It is not surprising therefore, that these applications are increasingly being seen in the development of combating fraud" (Giarratano and Riley, 1994).

The final authentication round begins by the client handler multiplying the last number it generated by the number it received from the client and finally by seven. This number is then MD5 hashed and sent encrypted to client application. The client application compares this value to the value it previously held in memory. If the client is satisfied that these values are the same it prompts the customer for a PIN number. The PIN number is then MD5 hashed and sent with the serial number of the customer's terminal in an encrypted message to the bank.

As card business transactions increase, so too do frauds. Clearly, global networking presents as many new opportunities for criminals as it does for businesses. While offering numerous advantages and opening up new channels for transaction business, the internet has also brought in increased probability of fraud in credit card transactions. The good news is that technology for preventing credit card frauds is also improving many folds with passage of time. Reducing cost of computing is helping in introducing complex systems, which can analyze a fraudulent transaction in a matter of fraction of a second.

It is equally important to identify the right segment of transactions, which should be subject to review, as every transaction does not have the same amount of risk associated with it. Finding the optimally balanced 'total cost of fraud' and other measures outlined in this article can assist acquiring and issuing banks in combating frauds more efficiently.

5.4 Conclusions

The study sought to establish the influence of credit card skimming as a factor in credit card fraud. The study found that knowledge in card skimming and training were significant in influencing credit card skimming as lack of the two is a loop hole used by fraud stars.

The study found out that technology is factor that influences credit card fraud, the good news is that technology for preventing credit card frauds is also improving only that many institutions are yet to adopt.

Proper card management system was also found out to be an important factor as far as credit card fraud in the banking sector is concerned. The factor if properly managed and given support and embraced by management can assist achieve all the project objectives as it plays a greater role in this.

The study also sought to establish the influence of systems security as a factor in credit card fraud in the banking sector. The study found that system security is a backbone for preventing credit card fraud but institutions are yet to embrace the fact.

5.5 Recommendations

The study makes the following recommendations based on the findings of this study:

1. All banks adopt smart credit cards as their main mode of operation, smart credit cards operate in the same way as their magnetic counterparts, the only difference being that an electronic chip is embedded in the card which can be loaded with customers biometric details.
2. Within the context of long term strategy banks need to implement Europay MasterCard and Visa (EMV) specifications for embedding chips in credit cards

and processing transactions from such cards. As this will prevent fraud stars from skimming the credit cards.

3. All banks should try to install risk scoring systems as risk scoring tools are based on statistical models designed to recognize fraudulent transactions, based on a number of indicators derived from the transaction characteristics. Typically, these tools generate a numeric score indicating the likelihood of a transaction being fraudulent, the higher the score, the more suspicious the order.
4. Institutions should always try to embrace the changes in technology and make sure that there are no gaps left out during systems integrations as this are used by fraud stars to gain access to vital information that assist them defraud the institutions.

5.6 Suggestions for Further Research

This study was undertaken in Kenya Commercial Bank in Mombasa County. A similar study may be undertaken in the entire Kenya Commercial Bank branch network in the country and also in the entire banking sector and other sectors that use credit and debit cards.

REFERENCES

- Abbey J. (2009). *An Architecture Selection Procedure using In-Sample Performance*, Technical Report, Department of Computer Science, University College London.
- Austin Jay Harris and David C Yen. (2002). *Biometric Authentication- Assuring access to Information*, *Information Management and Computer Security*, 10(1): 12-19.
- Barr, Robert and Ken Pease (1990) *Crime placement, displacement, and deflection*. In *N.Morris and M.Tonry and N. Morris (eds)*, *Crime and Justice: An Annual Review of Research* (vol.12).
- Bill Rini. (2002). *White Paper on Controlling Online Credit Card Fraud*, Window Six, January 2002. <http://www.windowsex.com>
- Brantingham, Paul J. and Patricia L. Brantingham (1984) *Patterns in Crime*. New York: Macmillan.
- Card Fraud Facts (2002). *APACS (Administration) Ltd*, Association for Payment Clearing Services (APACS), April 2002.
- Caudill, M., and Bulter, C. (1992). *Understanding Neural Networks: Computer Explorations*. Harvard: MIT Press.
- Circular to Participating Organisations. (2000a). *ASX Business Rules 2.2.4 Prevention of Manipulative Trading When Acting on Behalf of Clients (No. 332)*, Canberra, Government Gazette.
- Circular to Participating Organisations (2000b). *ASX Business Rules 2.8 False or Misleading Appearances (No. 600)*. Canberra, Government Gazette.
- Clarke, Ronald V. (1992) *Situational Crime Prevention: Successful Case Studies*. Albany, NY: Harrow and Heston.
- Clarke, Ronald V. and David Lester (1989) *Suicide: Closing the Exits*. NY: Springer-Verlag.
- Clarke, Ronald V. and Pietro Marongiu (1993) *Ransom kidnapping in Sardinia, subcultural theory and rational choice*. In R.Clarke and M.Felson (eds), *Advances in Theoretical Criminology* (vol.5).
- Coleman, James S., Elihu Katz and Herbert Menzel (1966) *Medical Innovatiom*. New York: Bobbs-Merril.

- Cook, Philipp (1986) *The Demand and supply of criminal opportunities*. In M.Tonry and N.Morris (eds), *Crime and Justice: An Annual Review of Research* (vol.7).
- Cornish, Derek and Ronald V. Clarke (1987) *Understanding crime displacement: An application of rational choice theory*. *Criminology*, 25, 4, 933-947.
- Cornish, Derek and Ronald V. Clarke (1988) *Crime specialization, crime displacement and rational choice theory*. In H.Wegener, F.Losel and J.Haisch (eds), *Criminal behavior and the Justice System: Psychological Perspectives*. NY: Springer-Verlag.
- Cosson, Jean (1971) *Les industriels de la fraude fiscale*. Paris: Seuil.
- Cusson, Maurice (1993) *Situational deterrence: Fear during the criminal event*. In Ronald V. Clarke (ed), *Crime Prevention Studies* (Vol.1).
- Duncan M D G. 1995. *The Future Threat of Credit Card Crime*, RCMP Gazette, 57 (10): 25-26.
- Felson, Marcus and Lawrence E. Cohen (1981) *Modeling crime rate trends - A criminal opportunity perspective*. *Journal of Research in Crime and Delinquency*, 18, 128-64 (corrected 1982, 19:1).
- Felson, Marcus (1993) *Crime and Everyday Life: Insights and Implications for Society*. Thousand Oaks, CA: Pine Forge.
- Gabor, Tom (1990) *Crime displacement and situational prevention: Toward the development of some principles*. *Canadian Journal of Criminology*, 32, 41-74
- Gartner's Survey Report. (2000, Aug 21). *Online Card Fraud Target*. Framingham: Network World Press.
- Giarratano, J., and Riley, G. (1994). *Expert Systems (2nd ed)*. New York: PWS Publishing Press.
- Goldberg, D.E. (1989). *Genetic Algorithms*. Boston: Addison-Wesley Publishing Press.
- Holland, J. H. (1992). *Adaptation in Natural and Artificial Systems*. Harvard: MIT Press.
- How Each Anti-fraud System Works*. (2000, Oct 15). *Card Card News*, Chicago, p. A2
- Hurley, S., Moutinho, L., and Stephens, N.M. (1995). *Solving Marketing Optimization Problems Using Genetic Algorithms*. *European Journal of Marketing*, 29(4), 4-5.

- Intertek Group. (1994). *Adaptive Computational Methods*: Management Report. Paris, France: Author.
- Kingdon, J. (1995a). *Redundancy in Neural Nets*: An Architecture Selection Procedure using In-Sample Performance. Technical Report, Department of Computer Science, University College London.
- Kingdon, J., and Dekker, L. (1995b). *The Shape of Space*(Tech. Rep.), London: Department of Computer Science, University College.
- Kingdon, J. (1995c). *Intelligent systems for fraud detection*. In Sanchez, H., Shibata, T., Zadeh, L. (Eds), *Genetic Algorithms and Fuzzy Logic Systems* (pp. 133-141).
- Maguire S. (2002). *Identifying Risks During Information System Development*: Managing the Process, *Information Management and Computer Security*, 10(3): 126–134.
- Neural Networks in Fraud Watch (1994, Sept). *Card World Publications*, p. A2.
- Responsibility of Trading Participants for Bids and Offers in SEATS. (2000, Feb 15). *Financial Review Report*, p. A7.
- Online Fraud Report – *Online Credit Card Fraud Trends and Merchant's Response*, Mindware Research Group, Cyber Source.
- P Chan, W Fan, A Prodromidis and S Stolfo. 1999. *Distributed data mining in credit card fraud detection*, *IEEE Intelligent Systems*, 14(6): 67–74
- Sampson, Robert J. (1993) *Linking time and place: Dynamic contextualize and the future of criminological inquiry*. *Journal of Research in Crime and Delinquency*, 30, 4, 426-444.
- Shuliang, L. (2000). *The Development of a Hybrid Intelligent System for developing marketing strategy*. *Decision Support Systems*, 27(1), 394-409.
- Stemming the Telemarketing Fraud Tide in Fraud Watch (1994, July). *Card World Publications*, Northants, p. A3.
- Tremblay, Pierre (1986) *Designing Crime*. *British Journal of Criminology*, 26, 3, 234-253.
- Venugopal, V., and Beats, W. (1994). *Neural Networks and Statistical Techniques in Marketing Research*: A conceptual Comparison. *Marketing Intelligence and Planning*, 12(7), 30-38.

Van Leeuwen. (2002). *A Surge in Credit Card Fraud*, H. Financial Review, 24 September, p.49.

White Paper on Efficient Risk Management for *Online Retail*, *Clear Commerce Product Management*, Clear Commerce Corporation, September 2002.

APPENDICES

APPENDIX I: LETTER OF TRANSMITTAL

Haron A. K. Sitienei
P O BOX 41427 – 80100

MOMBASA

17TH APRIL, 2012

THE REGIONAL MANAGER,
KENYA COMMERCIAL BANK,
P O BOX 31243 – 80100,

MOMBASA.

Dear Sir,

REF: PERMISSION TO CONDUCT RESEARCH

I am a Master's Student at the University of Nairobi. In line, with my studies it is a requirement to undertake a research on a particular area of interest and write a Proposal for the award of the relevant Masters Degree. The topic of my research is:

"Factors Influencing Credit Card Fraud in the Banking Sector, Mombasa County – Kenya".

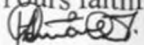
I am thus, conducting a Research Study to establish the factors. It is, in recognition of the role played by your Company in reduction of Credit card Fraud. The Research will seek to distribute questionnaires. I wish therefore, to kindly seek for permission to conduct this Research in your Company.

Please, take note that the information collected through this process will be used strictly for purpose of the study only.

Your assistance will be highly appreciated.

Thank you.

Yours faithfully



HARON A. K. SITIENEI

L50/61248/2011

APPENDIX II: Employees Questionnaire

Introduction and Seeking Consent

Hello my name is Haron A. K. Sitienei. I am doing a Masters Degree in Project Management at University of Nairobi and conducting a study in this area.

I am conducting a study to familiarize myself with the current status of extent of credit card frauds within Mombasa County in order to identify factors that are likely to contribute to the rise in credit card frauds. Participation in the study is voluntary. Whatever information you provide will be treated with confidentiality and will not be used for any other purpose other than the objectives of this study.

Signature of interviewer: _____

Date: _____

Seek to proceed: Can I proceed?

- Respondent agreed to be interviewed
1. Yes.....
2. No.....

Start time: _____

Section One (Personal Information)

- 1) What is your name (Optional):
- 2) What is your current position in the Bank
 - a) Regional Manager
 - b) Branch Manager
 - c) Ass. Branch Manager

- d) Head of Department
- e) Section Head
- f) Others: Specify:

3) What is your gender

- a) Male
- b) Female

4) For how long have you worked with KCB?

- a) Below 1 Year
- b) 1 – 5 Years
- c) 5 – 10 Years
- d) 10 – 15 Years
- e) Above 15 years

5) What position were you holding before you were appointed to the current position?

.....

Section Two (Skimming)

1) Do you have any knowledge in credit card skimming?

- a) Yes
- b) No

2) Have you been trained in prevention of credit card skimming?

- a) Yes
- b) No

3) If the answer above is Yes, Please tell us briefly how the training was?

.....

-
- 4) Whose responsibility is credit card management system?
- a) Branch Manager
 - b) Customer Care Officer
 - c) Tellers
 - d) Clarks

Section Three (Proper Card Management)

- 1) At what point is credit card verification done?
.....
.....
- 2) Does the bank scrutinize all card applications to ascertain whether there are fraudulent applications?
- a) Yes
 - b) No
- 3) Please explain your answer above
.....
.....
- 4) Do you have a card management system in place?
- a) Yes
 - b) No
- 5) Explain your answer above:
- 6) Who is charged with the responsibility of issuing Pin Codes to the customers?
.....

-
- 7) Does the customer validate his pin code at the Teller terminal?
 - a) Yes
 - b) No
 - 8) Please explain your answer above.....
-

Section Four (System Security)

- 1) How secure are your systems from various external threats?
 - a) Very secure
 - b) Secure
 - c) Somehow secure
 - d) Not secure
 - e) Don't know
- 2) Does the bank have a firewall in place?
 - a) Yes
 - b) No
- 3) What are the factors you think it has lead to credit card fraud?
.....
.....
- 4) In how much do you think the Bank has lost in the last two years due to credit card fraud?
.....
- 5) How often do you handle credit card fraud complaints from customers?
 - a) Once a week
 - b) By weekly

c) Once a Month

d) Very Often

e) Rarely

f) Not sure

6) In your opinion what should the bank do to mitigate or eliminate credit card fraud?

.....

.....

.....

APPENDIX III: Customers Questionnaire

Section one (Personal Information)

- 1) What is your name (Optional):.....
- 2) What is your gender:
- 3) What is your age bracket?
 - a) 20 – 25
 - b) 26 – 30
 - c) 31 – 35
 - d) 36 – 40
 - e) Above 40 Years

Section Two

- 4) Do you have a KCB credit card?
 - a) Yes
 - b) No
- 5) If Yes, for how long have you been having it?
 - a) Below 1 Year
 - b) 1 – 3 Years
 - c) 3 – 5 Years
 - d) Above 5 years
- 6) Have you ever been hit by credit card fraudsters?
 - a) Yes
 - b) No

7) If the answer in question 6 is yes, what happened?.....
.....
.....

8) How much did you loose as a result of credit card fraud?
.....

9) How did you discover that you had been defrauded?
.....

10) How did the bank handled the situation?
.....

11) How can you rate how the problem was handled by the bank

- a) Very satisfied
- b) Satisfied
- c) Somehow satisfied
- d) Not satisfied

12) Did the bank train you on the proper usage and safety of credit card?

- a) Yes
- b) No

13) If your answer above is yes, please tell us how the training was done?
.....

14) What factors do you think contribute to credit card fraud?
.....

15) What would you advice the other customers on credit card fraud?
.....