FACTORS INFLUENCING ELECTRONIC FRAUD IN THE BANKING INDUSTRY IN KENYA:A CASE OF KENYA COMMERCIAL BANK CENTRAL REGION

BY

DAMARIS KARIMI MWABU

A RESEARCH PROJECTREPORT SUBMITTED IN PARTIAL FULFILMENT FOR THE AWARD OF THE DEGREE OF MASTER OF ARTS IN PROJECT PLANNING AND MANAGEMENT OF THE UNIVERSITY OF NAIROBI

2013

DECLARATION

This research project is my original work and has not been presented for the award of any degree in any other university.

Sign……………………………………… Date ……………………………………

DamarisKarimiMwabu

L50/73361/2012

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

Sign ……………………………………… Date ……………………………………

Dr. Angeline Mulwa

Lecturer

Department of Extra Mural Studies

University of Nairobi

DEDICATION

I dedicate this to my mother Lucia Mwabu: You taught me that it's not only about getting to the destination, but how one gets there is what ultimately counts. My sincere dedication also to my late father Mr. MwabuKirii, who taught me that education, is the premise of progress in every human being, family and every society.

ACKNOWLEDGEMENT

I wish to acknowledge the support I have received in the course of writing this project. First to my supervisor, Dr Angeline Mulwa, who has guided me with great patiencethroughout the entire project.All the scholars whose work has either directly or indirectly contributed to the betterment of my work, without which it would not have been possible to put this piece of work together.

The University of Nairobi Extra-Mural center, as well as the all the lectures who taught me or who gave me a helping hand in the course of my studies. All of you have given me the platform and impetus to not only to compile this work but also to do greater things in future.

My colleagues in the office have been very supportive especially when I had to take leave to do my exams; they were always willing to take over my duties. I must also appreciate all my branch managers and the manager operations in both KCB Makuyu and KCB Kangari because they were willing to release me to sit for my exams, and to carry out my data collection.

Kenya Commercial Bank has also given me a chance to go back to school to better myself as an individual, as a woman and most importantly as an employee of the bank. The support that staff, who are willing to study, enjoy in the bank is overwhelming and I am proud of being associated with an organization that appreciates the value of an educated workforce.

My Mother and my late father, my siblings and my friends were always there for me to encourage me when the going got really tough. I must appreciate your support and thank God for all of you.

My dear friend Terrence Muthoka, you were always so far yet so close. You played a great role in my Masters Program by not only encouraging me but also mentoring me in many academic issues that I did not know about. I will always love you and I’llbe grateful to you because you are my hero.

TABLE OF CONTENTS

Page

DECLARATION ii
DEDICATION iii
ACKNOWLEDGEMENT iv
TABLE OF CONTENTS v
LIST OF TABLES viii
LIST OF FIGURES ix
ABBREVIATIONS AND ACRONYMS x
ABSTRACT xi
CHAPTER ONE: INTRODUCTION 1
1.1 Background of the Study 1
1.2 The Statement of the Problem 5
1.3 Purpose of the Study 6
1.4 Objectives Of the Study. 6
1.5 Research Questions 6
1.6 Significance of the study 7
1.7 Delimitation of the study 7
1.8 Limitations of the Study 8
1.9 Assumptions of the study 8
1.10 Definition of Significant terms as used in the study 8
1.11 Organisation of the study 9
CHAPTER TWO: LITERATURE REVIEW 11
2.1 Introduction 11
2.2 Theoretical Review on Fraud in the Banking Industry 11
2.3 Quality of management and electronic fraud in the banking industry 14
2.4 Security controls and electronic fraud in the banking industry 17
2.5 Salaries and remuneration and electronic fraud in the banking industry 20
2.6 Awareness of the customer and electronic fraud in the banking industry 22
2.7 Conceptual Framework 26

CHAPTER THREE: RESEARCH METHODOLOGY 29
3.1 Introduction 29
3.2 Research Design 29
3.3 Target Population 29
3.4 Sample Size 30
3.5Sample size and Sampling Procedure 31
3.6 Data Collection Instruments ……………………………………………………………… 31
3.7 Validity and reliability of research instruments 32
3.7.1 Validity of Research Instruments.....…………………………………………….33
3.7.2 Reliability of Research Instruments ……………………………………………….33
3.8 Data Collection Procedure………………………………………………………...33
3.9 Data Analysis 34
3.10 Ethical Consideration 35
3.11 Operationalization of Variables 35
CHAPTER FOUR: DATA ANALYSIS, PRESENTATION AND INTERPRETATION 36
4.1 Introduction 36
4.1.1 Response Rate……………………….……………………………………...36
4.2 Demographic Characteristics 36
4.2.1 Gender of respondents ……………….………………………………………… 36
4.2.2 Age of the respondents ....…………………………………………………...37
4.2.3 Respondents Level of Education …...……………………………………………38
4.2.4 Duration of Work in the company……….……………………………………….39
4.3 Quality of Management and Electronic Fraud in the Banking Industry…………………..40
4.4 Security Controls and Electronic Fraud in the Banking Industry 43
4.5 Salaries and Remuneration and Electronic Fraud in the Banking Industry 45
4.6 Level of Awareness of the Customerand Electronic Fraud in the Banking Industry.......... 47
4.7 Electronic Fraud in the Banking Industry 49
4.8 Regression Analysis 49

CHAPTER FIVE: SUMMARY OF FINDINGS, DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS 53
5.1 Introduction 53
5.2 Summary of Findings 53
5.2.1 Quality of Management and Electronic Fraud in the Banking Industry ……………53
5.2.2 Security Controls and Electronic Fraud in the Banking Industry .....………………..54
5.2.3 Salaries and Remuneration and Electronic Fraud in the Banking Industry...…..……54
5.2.4Level of Awarenessof the Customer and Electronic Fraud in the BankingIndustry.54
5.3 Discussion 55
5.3.1 Quality Managementand Electronic Fraud in the Banking Industry 55
5.3.2 Security Controlsand Electronic Fraud in the Banking Industry 56
5.3.3 Salaries and remunerationand Electronic Fraud in the Banking Industry 57
5.3.4 Level of Awareness of the Customerand Electronic Fraud in the Banking Industry ... 58
5.4 Conclusion ……………………………………………………………………..59
5.5 Recommendations 60
5.6 Suggestion for Further Studies 61
REFERENCES 63
APPENDICES 68
Appendix 1: Introduction letter 68
Appendix 2: Questionnaire 69
Appendix 3: Required Size for Randomly Chosen Sample 73

LIST OF TABLES

Page

Table 3.1: Target Population and Sample Size 30

Table 3.2: Operational definition of variables 36

Table 4.1: Gender of the Respondents …..………………………………………………….. 37

Table 4.2: Age bracket of the respondents ……………………………………………….....38

Table 4.3: Respondents’level of education 39

Table 4.4: Duration of work in the company 40

Table 4.5: Extent that quality of management influence electronic fraud in banking industry.... 41

Table 4.6: Extent that aspects of quality of managementinfluenceelectronic fraud in the banking industry 42

Table 4.7: Extent that security controls influence electronic fraud in the banking industry 43

Table 4.8:Extent that aspects of security control influence electronic fraud in the banking industry 44

Table 4.9: Extent that salaries and remuneration influence electronic fraud in the banking industry 45

Table 4.10: Extent that aspects of salaries and remuneration influence electronic fraud in the banking industry 46

Table 4.11: Extent that level of awareness of the customer influence electronic fraud in the banking industry 47

Table 4. 12: Extent that aspects of level of awareness of the customer influence electronic fraud in the banking industry 48

Table 4. 13: Trend of Electronic Fraud in the bank for the last five years 49

Table 4.14: Model Summary 50

Table 4.15: Summary of One-Way ANOVA results 50

Table 4. 16: Regression coefficients of the relationship between electronic fraud in the banking industry and the four predictive variables 51

LIST OF FIGURES

Page

Figure 1: Conceptual Framework 28

ABBREVIATIONS AND ACRONYMS

KCB:	Kenya Commercial Bank
KYC:	Know Your Customer
CBK:	Central Bank of Kenya
AML:	Anti-Money Laundering
BRMS:	Business Rule Management Systems
ATM:	Automatic Teller Machines
FFIEC:	Federal Financial Institutions Examination Council
CCIBN:	Chief Inspectors of Banks in Nigeria
OTP:	One Time Passwords
PIN:	Personal Identification Number
PC:	Personal Computer

ABSTRACT

Fraud isone of the most serious corporate problems, and challenges in today's business environment. In the banking industry, many frauds are perpetrated through falsified payment instruments including computer fraud, Card fraud and Mail order fraud that's commonly referred to as internet fraud.Frauds in Kenyan banks only prove that financial liberalization aggravates the inherent tendency of shallow markets to foster excessive speculation and worsens the systematic consequence of such speculative activity. Revelations of electronic fraud, evidence of insider trading and consequent collapse of investor interest have led to an almost unstoppable downturn in Kenyan banks. Bank frauds concern all citizens. It has become a big business today for fraudsters.KCB Kenya is divided into 5 regions of operation namely; Western region, Coast Region, Central Region, Nairobi Region, and Great Rift Region. The study specificallysought to determine the factors influencing electronic fraud in the banking industry in Kenya in reference to Kenya Commercial Bank (Central Region).This study employed descriptive survey design. The population of interest in this study comprisedof all staff of Kenya Commercial Bank central region.KCB Kenya Central region had 37 branches and a total of 630staff members as at time of the study. From the above population of 630, a representative sample of 241 staff members was drawn. The study employed stratified random sampling technique in selecting the staff members based on their department and their management level. Primary data was collected using questionnaires.On the other hand secondary data wascollected from newspapers, published books, journals and magazines as well as other sources. The data was then analyzed using descriptive statistics. The researcher further employedmulti-linear regression model to study the causes of electronic fraud in the banking industry in Kenya.The findings were presented using tables and graphs for further analysis and to facilitate comparison.The study found thatlevel of awareness of the customer had the greatest effect on the electronic fraud in the banking industry, followed by security controls, then quality management while level of salaries and remuneration had the least effect to the electronic fraud in the banking industry.The study recommends that the top management in the banks should ensure that they fully support fraud detection policies by allocating enough resources to them in order to gain a competitive edge.The banks should encourage teamwork, improve the working environments and set clear roles and responsibilities. There is need to improve on the efficiency of communication between the branches and interdepartmental communication at Kenya Commercial Bank as network failure is a major contributor to fraud. This will enhance the vigilance at all the quotas and enhance better understanding of policies and fastens decision making. The administration at the banks should enhance the employee morale and satisfaction through bonuses and allowances. Customers should review their agreement with the bank and know what rights they may be waiving by not using certain security measures.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Fraud and management have been the precipating factor in the distress of banks worldwide, and as muchas various measures have been taken to minimize the incidence of electronic fraud, it still rises by the day becausefraudsters always device tactical ways of committing fraud (Rezaee, 2004). This has become a point of great attentionin the banking sector in the international scene. Fraud is now the crime of choice of organized criminal gangs worldwide. The likely gains are enormous and the likelihood of apprehension and thus of conviction and punishment comparatively small compared with conventional crimes of dishonesty involving guns, intimidation and violence of all kinds (Cain, 1999). Professional criminals are targeting big business.

Young (2002) observed that ample evidence exists thatindividual integrity of those running the banks today has never been at a higher level. Never before havewe seen attention to the actual steps; procedures andcontrol of monetary transactions. Although the existenceof fraud in the banks is not an uncommon orunexpected behavior, the prevalence of it is what isworrying because of all the various problemsconfronting the most untraceable (Akindele et al, 2008).

Alashi (1994) grouped the major causes of the bank fraud into two. These are institutional factors and environmental factors. Institutional factors are those traceable to the internal environment of the financial institution while the environmental factors are those which result from the influence of the environment on the banking industry. Among the major causes include the volume of work, nature of services, banking experience of staff, poor security arrangement, inadequate infrastructure, delays in procuring document and lack of effective deterrent/punishment.

Frauds in banks lead to loss of monies thatordinarily belong to someone other than the banks. The loss results in some cases in reducing the levelof resources available for use in the operations of thebanks. In very bad cases where frauds occur withcrippling frequency and in wholesomeness, the bankmay be forced to close down as a result. When thebank loses money and is wound up, the customerslose money. This leads to loss of confidence andeventually reduced patronage. Another reason forworrying in the banking industry is the vast variety ofnature, character and methodology employed infraud (Katz, 2009). The financial loss is sometimes carefully hidden in the accounting records that are used to track activity involving the resources, allowing it to continue until a great deal of money and other assets are siphoned off and no longer in the control of the owner.

Failure to prevent and detect fraud has serious consequences for organizations. Although rare in occurrence, financial statement fraud can result in devastating losses to investors, creditors and auditors. Detecting fraud is a difficult task for auditors, in part because most have never experienced fraud in their careers (Montgomery et al., 2012). The risks of fraud within and upon corporations cannot be understated. They include the immediate risks to the company affected, which can fail completely. There is also the reputation risk to the company that has suffered major fraud. This is one reason that companies and particularly financial institutions are so reluctant to report fraud to law enforcement, where they fear that the likelihood of their names hitting the headlines associated with major losses will result in competitors' obtaining an advantage and customers walking away. Systemic risk, that affects an entire financial market or system, and not just specific participants, cannot be underestimated. After the secondary banking crisis in the 1980s, where so many minor financial houses failed, largely as a result of fraud, confidence in the banking sector was shaken severely.

Nearly 45 percent of the 141 million adults in America pay their bills online (according to the Garter 2004 Survey). Banks also enjoy providing the option of online banking because they can save on operating costs. However, during the popularization of online banking, nearly 2 million Americans suffered from fraudulent bank activity in 2004. Consumers reported an average loss of $1, 200 per bank fraud. Most market researchers attributed the increase in the number of bank frauds to online banking (Apostolou, Hassell and Webber, 2001).

The Brazilian Banks Federation (Febraban) recently released data from a survey revealing that losses caused by electronic fraud are on the rise. These losses totaled R$ 685 million (US$ 460 million) from January to June this year, up from R$ 504 million (US$ 340 million) for the same period last year. That’s an increase of 36% (Coffin, 2009).

According to Nwankwo (2001), bank fraud in Nigeria has increased and will continue to increase because it is a part of everyday life. In 1998, the nation’s banking industry lost $3.196 Billion while in 1999; it lost a whopping sum of $7.404 Billion to fraud. Nigeria's banks have seen almost $10m disappear through employee fraud in 2002, a rise of more than 40% on the year before, a survey by the country's banking regulator has found.

The phenomenon is empirically supported by a number of studies; for example, Cain (1999) and the KPMG Australia fraud survey (KPMG, 2002) each indicate that over 50 per cent of all interviewees surveyed believed that fraud is a major business problem. Similarly, reviews of fraud cases by Rezaee (2004) revealed that financial statement fraud has cost market participants more than $500 billion during recent years, with serious litigation consequences for associated auditors.

The level of electronic fraud in the present day Kenya has assumed an epidemic dimension. According to the CBK (2012), the figures of cybercrimes are higher than before because of the growing use of electronic devices as payment tools, the lack of legislation that inhibits criminal action with effective punishment, and the carelessness of some users regarding security procedures.Internet fraud often occurs when a consumer is deceived into revealing personal codes and passwords to fraudsters. This can happen when the consumer does not adopt recommended safety measures for equipment such as scanners, legitimate operating systems and software and updated firewalls.

Fraudsters are constantly devising new plans,updating old methods and trying out new techniquesof bypassing these electronic systems meant to ensurehigh security of banking operations (KPMG, 2001). Theintroductions of automated systems that losehandwriting and fingerprint trails have not helpedmatters either.In view of the staggering sums lost to fraudsters bythe Kenyan financial sector, in these recent timesand the rate at which fraudsters appear to have shiftedtheir attention and directed their energies to banks,devising all unimaginable tactics to exploit loopholesin the control measures and capitalize on carelessnessof the staff and customers, Fraud in the industry hasprevented many banks from achieving their goals.There is, therefore,a great need to study the causes of electronicfraud perpetrated in the banking industry in Kenya.

1.2 The statement of the Problem

Fraud is believed to be amongst the most serious corporate problems, and challenges in today's business environment, indeed Palshikar (2002) suggests that fraud or scam is a dominant white collar crime in today's business environment particularly in financial and related services, suffer from fraud of various kinds. In the banking industry, many frauds are perpetrated through falsified payment instruments including computer fraud, Card fraud and Mail order fraud that's commonly referred to as internet fraud.

Frauds in Kenyan banks only prove that financial liberalization aggravates the inherent tendency of shallow markets to foster excessive speculation and worsens the systematic consequence of such speculative activity. Revelations of electronic fraud, evidence of insider trading and consequent collapse of investor interest have led to an almost unstoppable downturn in Kenyan banks. Bank frauds concern all citizens. It has become a big business today for fraudsters.

Prior studies have found that failing to detect fraudulent financial reporting can expose the auditor to adverse legal and/or regulatory consequences. For example, Carcello and Palmrose (1994) found a significant positive association between the presence of fraud and litigation against the auditor. The reviewed studies have focused on different aspects of fraud like detection and extent of its effects on different sectors of the economy. Further, most of them are on international scenes or on developed countries. To the researcher's knowledge, at the time of the study, no local or international studies had ever focused on the causes of electronic fraud in the banking industry in Kenya. This is despite the ever increasing cases of electronic fraud risks that had claimed a number of financial institutions in Kenya and thus calling for strategic responses to curb the spread of the crime. It is in this light that the researcher aims to fill the existing gap by carrying out an investigation into the factors influencing electronic fraud in the banking industry in Kenya with reference to Kenya Commercial Bank.

KCB central region is my area of study because it has seen a number of frauds both staff and customer engineered. The researcher also focused on central region because of ease of data collection.

1.3 Purpose of the Study

The purpose of the study was to investigate the factors influencing electronic fraud in the banking industry in Kenya with reference to Kenya commercial Bank.

1.4Objectivesof the Study.

1. To establish the influence of quality of management onelectronic fraud in the banking industry
2. To establish the extent of influence of security controls on electronic fraud in the banking industry
3. To assess the influence of salaries and remuneration of staffon electronic fraud in the banking industry
4. To establish the influence of the level of awareness of the customer, how this influences their behavior in relation toelectronic fraud in the banking industry

1.5 Research Questions

1. What is the influence of the quality of management on electronic fraud in the banking industry?
2. To what extent do security controls influence electronic fraud in the banking industry?

3. How doessalaries remuneration for staff influence the occurrence of electronic fraud in the banking industry?
4. To what extent does the level of customer awareness and exposure influence their behavior in relation to electronic fraud in the banking industry?

1.6 Significance of the study

The study would be important not only to Kenya Commercial Bank managers but also other managers in the banking sector and to larger extent managers of other industries. It would help them understand the causes of electronic fraud in the banking industry in order to strategically plan on the practices to employ in their internal control systems. The study would also highlight other important relationships that require further research; this will be in the areas of relationships between fraud related risks and the strategic responses to impact on their performance. The results of this study would also be invaluable to researchers and scholars, as it will form a basis for further research. The students and academics would use this study as a basis for discussions on causes of electronic fraud and the strategic responses. The study would be a source of reference material for future researchers on other related topics; it will also help other academicians who undertake the same topic in their studies.

1.7Delimitation of the study

The study was about the factors influencing electronic fraud in the banking industryand it focused on Kenya Commercial Bank(Central Region). The researcher believed that this provided an adequate population for the study and therefore gave reliable results and findings. It focused on senior managers, middle level managers and unionisable staff in KCB Kenya (Central

Region). KCB Central region has had a number of electronic frauds ranging from card skimming to funds transfers.

1.8 Limitations of the Study

The main limitation of study was its inability to include more organizations. This was a case study focusing on Kenya Commercial Bank. The study would have covered more institutions across all sectors so as to provide a more broad based analysis. However, time and resource constraints placed this limitation. The study also encountered unwillingness by interviewees to reveal information which was classified as confidential. Some respondents were biased and could not reveal the correct answers to questions.

1.9 Assumptions of the study

The researcher assumed the following during the study: That the information given by the respondents would be true facts as per the status in these organizations, and that the organizations acknowledge the risk and magnitude of electronic fraud in the banking industry. The researcher also assumed that the respondents would co-operate and submit relevant documentations and that organizations, that is banks, as routine measures, undergo an audit periodically aimed at ensuring internal controls are not compromised.

1.10 Definition of Significant terms as used in the study.

This section gives the definition of significant terms used in the study. The definitions given were limited to the study, and the terms include:

Customer awareness: This term means the degree of exposure and level of education of each and every individual that has an account with KCB.

Fraud/Fraudster: This is a scheme whose intent is to swindle a person/s of a certain amount of money or goods. A fraudster is the person who perpetrates fraud.

Fraud Management:This is an eight stage process of whose main agenda/aim is to uncover frauds and sojourn frauds, which mostly leads to arrest and prosecution.

KCB Central Region: Kenya Commercial Bank(Kenya) is divided into 5 thematic regions in Kenya, namely, Coast, Nairobi, Central, Western and Great Rift Region. This study focuses on the central region.

Management: This term, as used in this study implies the systematic way of organizing, directing, supervising and controlling individual(bank staff), in order to achieve a certain result(which in this case is mitigation of fraud.)

Unionisable staff: These are staff members in KCB who are in the clerical tier, hence they are in the KCB union. We can also define this term as all the non-management staff in KCB.

1.11 Organization of the study

The study isorganized into five chapters: Chapter one is introduction, this chapter gives the historical background of electronic fraud in the banking industry, provides the purpose of study under which there are the objectives and the research questions. The significance of the study, scope, limitations as well as the assumptions of the studyhas been captured in this chapter.

Chapter two is the literature review. This chapter cites and explores literature that has been done in the area of electronic fraud internationally, locally and finally in KCB Kenya. It also presents a conceptual framework on which the research will be based.Chapter three is research methodology. This chapter presents the research design, target population, sample and sampling procedure, description of the research instruments, data collection procedures and data analysis techniques.

Chapter four presents analysis and findings of the study as set out in the research methodology. The study closes with chapter five which presents the discussion, conclusion, and recommendations for action and further research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this second chapter, relevant literature information that is related and consistent with the objectives of the study is reviewed. Important issues and practical problems are brought out and critically examined so as to determine the current facts. This section is vital as it determines the information that link the current study with past studies and what future studies will still need to explore so as to improve knowledge.

2.2 Theoretical Review on Fraud in the banking industry.

Fraud losses continue to form a substantial part of losses incurred by various business enterprise. Caveat Emptor, let the buyer beware, tells only half the story. The other half is told by Caveat Venditor, let the seller beware. The costs of fraud are passed on to society in the form of increased customer inconvenience, opportunity costs, unnecessarily high prices for goods and services, and criminal activities funded by the fraudulent gains. Despite significant advances in fraud detection technologies, fraud losses continue to pose a significant problem to many industries, including telecommunications, banking and finance, insurance, health care, Internet merchants, brokerage and securities, and many others (Deming, 1986).

Fraud losses are frequently part of an economic externality. An economic externality is present when one business takes actions or refrains from actingand, as a result, passes on, imposes, or facilitates costs upon another business. An example from the internal fraud perspective would be when a financial institution decides not to facilitate law enforcement's arrest and prosecution of a staff member who stole from them. As a result of their decisions, the ex-staff member may very well obtain employment at another financial institution and commit the same crime again. This situation is quite aptly described by the following "While fraud does exist in retail originations, it is typically related to a particular loan officer and is more often than not quickly discovered. Theemployee is usually terminated from his [or her] position and moves on to a new company until the same thing happens all over (Prieston and Dreyer, 2001).

Previous research regarding fraud generally, and credit card fraud in particular, has focused upon the crimes, the criminals, or both. For example, Mativat and Tremblay (1997) studied credit card counterfeiting and offenders along with displacement, as opposed to the methods, procedures, and policies employed by the victims to prevent the fraud. It is this author's premise that no comprehensive analysis has been performed of the entire Fraud Management Lifecycle and the appropriate relationships among each of the various stages and the activities therein.

Effective management of the Fraud Management Lifecycle starts with a common understanding or definition of the stages in the lifecycle. Without this awareness and understanding, fraud management professionals are unlikely to communicate effectively with each other, with their peers in other industries, and within their respective businesses.

The Fraud Management Lifecycle is made up of eight stages. Deterrence, the first stage, is characterized by actions and activities intended to stop or prevent fraud before it is attempted; that is, to turn aside or discourage even the attempt at fraud through, for example, card activation programs. The second stage of the Fraud Management Lifecycle, prevention, involves actions and activities to prevent fraud from occurring. In detection, the third stage, actions and activities, such as statistical monitoring programs are used to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity. The intent of detection is to uncover or reveal the presence of fraud or a fraud attempt. The goal of mitigation, stage four, is to stop losses from occurring or continuing to occur and/or to hinder a fraudster from continuing or completing the fraudulent activity, by blocking an account or freezing a certain amount of funds or the whole amount of funds in an account, for example. In the next stage, analysis, losses that occurred despite deterrence, detection, and prevention activities are identified and studied to determine the factors of the loss situation, usingmethods such as root cause analysis. The sixth stage of the Fraud ManagementLifecycle, policy, is characterized by activities to create, evaluate, communicateand assist in the deployment of policies to reduce the incidence of fraud (Mativat and Tremblay, 1997).

Balancing prudent fraud reduction policies with resource constraints and effectivemanagement of legitimate customer activity is also part of this stage. Investigation, the seventh stage, involves obtaining enough evidence andinformation to stop fraudulent activity, recover assets or obtain restitution, and toprovide evidence and support for the successful prosecution and conviction ofthe fraudster(s). Covert electronic surveillance is a method used in this stage.

The final stage, prosecution, is the culmination of all the successes and failuresin the Fraud Management Lifecycle. There are failures because the fraud wassuccessful and successes because the fraud was detected, a suspect wasidentified, apprehended, and charges filed. The prosecution stage includes assetrecovery, criminal restitution, and conviction with its attendant deterrent value (Mena, 2002).

2.3 Quality of management and electronic fraud in the banking industry

The increasing sophistication of fraudulent attacks against card issuers, checking accounts and ACH together with the increased importance of compliance with global Anti-Money Laundering (AML) legislation serves to focus the attention of financial institutions around the world. Evolving threats include: increased opportunistic, non-pattern based fraud, growth of organized crime and terrorism and their requirement for significant funding and increased reputational risk associated with poor fraud detection capabilities among the management staff (Mohammad, 2010).

According to Heli (2006), strategic and operational changes should be made to ensure the effective, optimal overlay of industry and domain knowledge with relevant strategies, technology and methodologies. This includes the need to integrate effective detection, decision and monitoring paradigms such as business rule management systems (BRMS) to enable the execution of a holistic and integrated fraud detection strategy.

The increasing prevalence of enterprise financial crimes has made fraud prevention and investments in prevention technology a long-overdue priority to organizations around the world. As a result, organizations are learning that the consolidated software platform approach to fraud detection is fundamentally flawed and falls short on detecting and preventing fraudulent transactions. The management should learn how they can integrate risk management into theirmost important operational decisions and business processes, such as Anti-Money Laundering (AML), Know Your Customer (KYC) and credit risk (Afam, 2009).

Technology helps to alert banks of potentially fraudulent activities before the damage is done and large losses are encountered. The challenge is monitoring for suspicious behavior. Banks need to move from being reactionary to being more proactive when it comes to internal fraud. Such was the case with Spokane, Wash-based Washington Trust ($3.6 billion in assets). According to the Aite case study, the bank's pre-employment screening process was sufficient, but its post-hiring employee monitoring was not. The bank worked with NextSentry (Spokane) to develop and deploy ActiveSentry, a product designed to "better protect customer privacy by reducing and preventing opportunities for account information to be printed, stolen and used (Lee and Lee, 2000).

The more sophisticated the technology used in the internet gaming industry gets, the more advanced the levels of fraud become. From card fraud to identity theft and misrepresentation, providers have had to adapt the way they manage their businesses, their customer identification procedures and their fraud prevention tools. Let’s examine the main challenges the online gaming industry faces when it tackles the issue of fraud (McFadden, 2007).

Still very common are manual checks - agents flag cases they consider to be ‘suspicious’ based on risk alerts, customer tip-offs and unusual gaming and wagering play by customers. These risk alerts are typically pre-defined rules based on business knowledge and past experiences. Another way of preventing fraud is the limitation on the number of credit cards that can be used, limitation of payment methods on the other hand leads to the reduction of conversion.

More sophisticated are device reputation models like device fingerprinting. They provide information about good, bad, and historical activities conducted from particular desktops and mobile devices. Furthermore, statistical profiling determines exceptions of transactional behavior through regression analysis. Risk scoring models incorporate these techniques for modeling and analyzing several customizable variables. Data is then checked against the rule parameters and external databases to determine its likelihood of being fraudulent. Advanced Analytics and artificial intelligence are creating predictive modeling techniques to assist the human thought process in detecting fraudulent trends (Loviglio, 2012). All these measures aim to accurately and swiftly detect, block and prohibit individuals attempting to engage in fraudulent transactions. This continuous need of an end-to-end monitoring system for online merchants creates a whole industry around detecting and preventing online fraud.

Risk management solutions combined with trusted e-identity and authentication mechanisms are needed. Consumers have more and more online identities of various natures. Initiatives to re-use these identities in the online commerce context, with security levels that can be adapted to the risk or the value of the transaction (basic security for low value, high level of security for higher values) are emerging. They vary from verified credentials (for example, bank passes) to unverified credentials with stored preferences (social media credentials such as Facebook). There are many benefits, including the improvement of the security of cards, credit transfers and direct debits. By using a similar international online identity solution for all payment types, the online banking and shopping experience will be harmonized. This leads to a better experience, more trust and therefore more sales if implemented in a way that the consumer’s privacy is warranted.

Furthermore, empirical evidences have justified that network failure is another common cause of ATM fraud. In the view of Ellen (2009), mass compromise of merchant networks and card processors is viewed as the main cause of payment-card fraud. According to the survey, sponsored by a security firm, Actimize, 94% of the 113 financial-services firms could trace some percentage of payment-card fraud they experienced directly back to mass compromises of networks. Also in the survey, several examples of mass compromise events were given, including those known to have occurred at Heartland Payment Systems and grocery retailer.

2.4 Security controls and electronic fraud in the banking industry

E-commerce payments have seen a tremendous development in the past decade. During the last 15 years, the market matured and is still growing. The gaming industry, however, suffers from the lack of standardized online identity verification and authentication tools. Country specific rules and regulations add to the disorder. As a result, gaming and gambling sites are forced to introduce their own 'know-your-customer' (KYC) processes and fraud prevention tools that cost the industry hundreds of millions. Regardless of efforts to stop criminal activities - such as money laundering, fraudulent deposits, charge backs, cheating etc. - today's sophisticated fraud rings pose a greater threat to online gaming providers than ever before (Adsit, 2011).

The steps most banks follow to prevent cybercrime from happening starts with the gamer registration processes – the initial screenings – authentication and verification. These processes are performed to identify their customers and ascertain relevant information. This definition requires revalidation of their identity – knowing their customers identity and not who they say they are. KYC is typically a policy implemented to conform to a customer's identification program to prevent identity theft fraud. To what extent this process is executed depends upon factors including jurisdiction, risk and resources as it involves a lot of manual work. Another common measure to identify their customers is to use third party services such as address and age verification lists as well as credit scoring lists sourced from firms in the market. Hotlists, including the sorts of data sources used by banks to identify terrorists and public officials. Another emerging authentication and verification strategy is built on the most ubiquitous device of modern technology – the telephone. Phone verification and notification products can be used to protect the customers by automatically calling to validate transactions (such as purchases or top-ups) or actions (such as changes to personal information) on the platform (Olmos, 2009).

The alarming rate of ATM fraud can be attributed to a number of factors. Afam (2009) confirmed this when he submitted that there is nowhere in the world that experiences the embarrassingly high level of ATM card fraud other than Nigeria because the implementation of the technology in Nigeria is characterized by ineptitude, lack of knowledgeable programmers and security experts that could guide and implement a secure transaction channel regardless of the level of education of the ATM card users. He further accused the Nigerian ATM technology of being too simplistic. What this means in essence is that the ATM cards we carry about in Nigeria is not well suited for electronic transactions. In fact, it should not be used for electronic transactions without address verification and an extra security layer that can make it impossible for anyone to use someone else’s ATM card to make unauthorized withdrawals electronically. The reason is that the uncomplicated nature of Nigeria ATM system has widened the latitude for scammers to gain unauthorized access into people’s account which in turn lead to ATM fraud.

Since modern banking emerged in the 16th century, there have been countless numbers of frauds and schemes to get access to the money that is kept behind bank vaults. Some have aimed to take advantage of individuals and some have aimed to take advantage of institutions. With the introduction of electronic banking on the Internet, fraud has become even more of a problem, but new methods of detection have been adapted.

According toWole and Louisa (2009),in 2006, the Federal Financial Institutions Examination Council (FFIEC), the government agency responsible for overseeing electronic banking in America, introduced a requirement that all online banks use a two-factor authentication procedure. Previously, to access online banking services, all that was generally required was a user name and a password. Two-factor authentication requires the account holder to both enter the initial login information and also provide an answer, such as the name of a certain immediate family member, to a personal question.

If a consumer has special reasons to fear fraud, a bank may supply the consumer with one time passwords, or OTPs, that are required to access the consumer's electronic account. The consumer receives a physical list of different passwords that he then uses in succession with each new transaction. This extra step helps detect fraud by insuring that an account password is secure from spyware and other computer hacking programs (Ovia, 2001).

Many debit and credit card companies have begun to implement special transaction monitoring programs that look at every transaction made with a bank card. A special computer database examines each transaction and compares it to the regular pattern of a consumer. If something seems out of the ordinary, the bank and consumer will be alerted, and a manual verification of the transaction is often required (Ernst and Young, 2000).

2.5 Salaries andremunerationand electronic fraud in the banking industry

This type of fraud is not new, but online banking has added another channel through which an employee can steal. If a financial institution allows employees access to customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud. Because of this, financial institutions should require a password or PIN for online banking, and the password or PIN should be stored in an encrypted format. Another option is to truncate account numbers and customer data and limit employee access to the full numbers. Of the three types of fraud, internal fraud can be the most costly to financial institutions (Ellen, 2009).

Keeping financial information secure and confidential, including within Online Banking, is one of our most important responsibilities. Whenever personal information is requested or displayed on our website we use encryption technology, such as Secure Socket Layer (SSL), to prevent unauthorized access to data (Helmut, 2004). As the rapid expansion of the banking industry began in the mid 80's there was no adequate experienced personnel to cope with it. The few experiences hands went for the high pecked jobs thereby creating opportunities for both inexperienced and those who had no business being in banking to flood the industry. This was followed by rapid promotion for these inexperienced hands due to the polarization of the system. This led to the dilution of standards and professionalism was thrown to the wind. Honesty and integrity, which are the hallmark of banking, took secondary position. Materialism and inordinate ambition to amass wealth have become the order of the day.

While online banking has been around for many years, virtually no cases of fraud have been reported until recently. Since the beginning of the year 2004, reports of fraud cases nearly explode and banks are looking for ways to protect their online banking channel. Most online banking fraud schemes involve two steps. First, the criminal obtains the customer's account access data that is logon name and password. Second, the criminal uses this information to transfer money to other accounts and withdrawals the funds. Fraud, Forgeries and Insider abuse have become very rampant in the banking sector, because the staggering volume of money involved, they have contributed in no small way in rendering the banks insolvent (Laderman, 2010).

Apart from the simplicity of the ATM technology being used in Nigeria, insincerity of bank staff is another reason that has contributed to the widening rate of ATM scam in Nigeria. This has aborted virtually all the attempts made by banks to fight the ATM scam improprieties. The banks, too, open a window for fraudsters in their indiscriminate issuance of cards to customers without regard to their ability to utilize them. Furthermore, it was recently noted at the 12th Quarterly General Meeting of the Committee of Chief Inspectors of Banks in Nigeria (CCIBN) that the lack of co-operation among banks in the fight to stem the incidence of ATM frauds plaguing the industry is not helping to abet it. It has been said “that the various ATM service providers, whose fierce competition for market share makes the possibility of a united attack on the menace of ATM fraudsters impossible, are another factor that sustains the peril (Valentine, 2010).

2.6 Awareness of the customer and electronic fraud in the banking industry

The most common plastic cards in Uganda today are the Debit cardsfor example. ATM and point of sale cards. ATM and credit fraud occurs when a stolen or cloned card is used by criminals to withdraw cash from a customers' account. The fraud takes various forms: A customer may be accompanied by a close friend or even a relative to an ATM point to withdraw cash. In the process the relative or friend may learn the PIN number of the card and subsequently steals the card and withdraws the money from the bank without the knowledge of the customer. In more sophisticated cases, fraudsters mount cameras and other gadgets on ATMs and steal or capture the details of the card plus the PIN as it is entered, make a copy of the card and withdraw funds using the obtained details.

These gadgets are cleverly disguised to look like normal ATM equipment or leaflet/brochure holders. In other instances criminal gangs or employees obtain the particulars of a credit card through imaging techniques when being used to pay for goods and services and use the information to clone a fraudulent card which is then used to defraud the holder of the card. To protect against such frauds, customers are advised to memorize their PINs and never to write it down or share it with any other person. They should desist from the habit of giving cards and PINs to other people to withdraw money on their behalf. Cardholders should never use a card in an ATM where they see suspicious equipment or people. Always insist that cashier's swipe customer's cards in a machine that should be well located at the counters in the site of the cardholder and not under the counters or back offices (Mena, 2002).

According to Adeyemi (2010), criminal obtains the customer's account access data, that is, logon name and password using different schemes.The "over the shoulder looking" scheme occurs when a customer performs financial transactions while being observed by a criminal. A fair number of cases have been reported where customer's account access data was obtained by the criminal just by observing customers at a public Internet access point.

The "phishing" scheme involves using fake emails and/or fake websites. The word "phishing" stems from combining the words "password" and "fishing". Criminals send emails that appear to be from the customer's bank that direct customers to a fake website. This website impersonates the bank's website and prompts customers for their account access data. Over the past months, most banks have executed customer education programs, thereby reducing the effectiveness of this scheme. It will, however, take a while before all customers are smart enough to extinct phishing. The "Trojan horse" scheme is based on embedding a computer virus type software program onto the customer's PC. Trojans often tie themselves into the keyboard driver and record keystrokes. Once a Trojan detects that the customer opens an online banking website, it captures login name and password, and sends it to the criminal (Samociuk and Iyer 2003).

In the year 2003, phishing was the dominant fraud scheme. In the year 2004, banks experienced a sharp rise in Trojan fraud scheme attacks. To improve security, some banks use "one time passwords", also called OTP. Upon activation of the customer's account for online banking, the bank mails a list of OTPs to the customer. Each time the customer perform a transaction, he enters one OTP for verification. Once used, the OTP becomes invalid. If the customer runs out of OTPs, he is sent a new list. While this approach effectively prevents "over the shoulder looking", it generally fails to prevent other fraud schemes. Phishing emails also ask for OTPs, and a customer naive enough to give out his logon name and password will likely also provide OTPs. Trojans simply also capture the OTP once entered. At the same time, they falsify the customer's input in the browser software (for example by adding an invisible character) or cause the browser software to crash. This causes the customer's transaction to be intercepted and the OTP to still be valid. The criminal can then use this valid OTP to perform a fraudulent transaction(Prieston and Dreyer, 2001).

Hackers often take aim at small firms' computers because they are easier to infiltrate than banks' systems. One common mode of attack is to send a "spear phishing" email containing an infected file or a link to a malicious Web site to employees with access to the firm's financial accounts. Once the employee opens the attachment or goes to the Web site, malware is installed on the computer that allows criminals to access banking logins and passwords. While up-to-date antivirus software offers substantial protection against malware, it isn't 100% effective (MacRae, 2001).

According to theNilson Report (2000), customers should review their agreement with the bank and know what rights they may be waiving by not using certain security measures. While agreements between banks and commercial customers typically absolve banks of responsibility for fraud losses, the bank down the street may offer better protections. Also, they should consider adding insurance coverage for fraud losses.Many banks, concerned about damage to customer relationships, have stepped up their defenses against cyber-attacks, rolled out new protections for customers and begun sharing more threat information with each other and law enforcement.He also urges companies to report all computer crimes immediately to the FBI. The agency has relationships with law-enforcement organizations around the world that are starting to bear fruit.

The crime of identity theft is on the rise. According to a February 2013 Javelin Study, more than 12.6 million adults became a victim of identity theft in the United States during 2012. Identity theft was the number one complaint filed with the Federal Trade Commission's Consumer Sentinel during 2011.Using a variety of methods; criminals steal Social Security numbers, driver's licenses, credit card numbers, ATM cards, telephone calling cards, and other pieces of individuals' identities such as date of birth. They use this information to impersonate their victims, spending as much money as they can in as short a time as possible before moving on to someone else's name and identifying information.

There are two types of identity theft: Account takeover occurs when a thief acquires the customer existing credit account information and purchases products and services using either the actual credit card or simply the account number and expiration date. On the other hand, application fraud is what some experts call "true name fraud." The thief uses the customers SSN and other identifying information to open new accounts in the customer’s name. Victims are not likely to learn of application fraud for some time, because the monthly account statements are mailed to an address used by the imposter. In contrast, victims learn of account takeover when they receive their monthly account statement. This guide discusses strategies for reducing the risk of both types of fraud (Whatley, 2008).

Even though victims are usually not saddled with paying their imposters' bills, they are often left with a bad credit report and must spend months and even years regaining their financial health. In the meantime, they have difficulty getting credit, obtaining loans, renting apartments, and even getting hired. Victims of identity theft find little help from the authorities as they attempt to untangle the web of deception that has allowed another person to impersonate them.Stealing wallets used to be the best way identity thieves obtained SSNs, driver's licenses, credit card numbers and other pieces of identification. While still employed, identity thieves now use a variety of means:Dumpster diving in trash bins for non-shredded credit card and loan applications and documents containing SSNs; Stealing mail from unlocked mailboxes to obtain newly issued credit cards, bank and credit card statements, pre-approved credit offers, investment reports, insurance statements, benefits documents, or tax information. Unfortunately, even locked mailboxes may not stop the most determined thief; Accessing your credit report fraudulently, for example, by posing as an employer, loan officer, or landlord; Obtaining names and SSNs from personnel or customer files in the workplace; "Shoulder surfing" at ATM machines and phone booths in order to capture PIN numbers; Finding identifying information on Internet sources, via public records sites and fee-based information broker sites; Sending email messages that look like they are from your bank, asking you to visit a web site that looks like the bank's in order to confirm account information. This is called phishing; Hacking into unsecured and unencrypted data files of financial institutions, retailers, and credit card transaction processing companies and accessing unsecured web sites that contain sensitive personal information such as Social Security numbers and financial account numbers.To minimize the amount of information a thief can steal, customers are advised not to carry extra credit cards, debit cards, Social Security card, birth certificate or passport in the wallet or purse, except when needed (Adeyemi, 2010).

2.7 Conceptual Framework

Conceptualframeworks are obviously critical in deductive, theory-testing sorts of studies. In those kinds of studies, the theoretical framework must be very specific and well-thought out. A theoretical framework is used in this study to show the link between independent variables and dependent variable. A conceptualframework below is used in this study to show the link between independent variables and dependent variable.

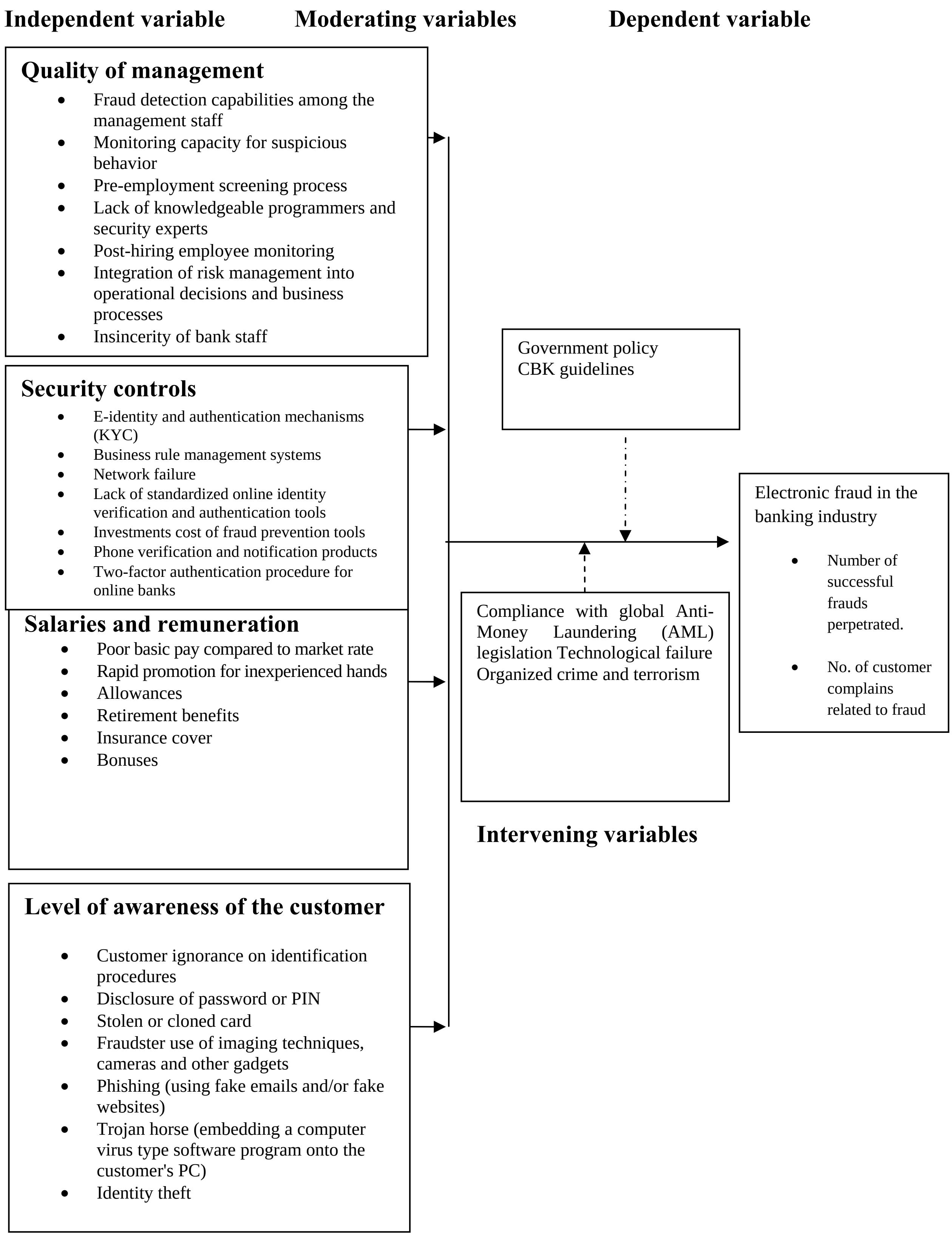

Figure 1: Conceptual Framework

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines a plan for the data collection, measurement and analysis. Therefore, this section sets to answer the research question raised in the study. To achieve the objective of this chapter, it therefore includes research design, target population, data collection instruments, data collection procedures and finally data analysis techniques.

3.2 Research Design

Orodho (2003) defines research design as the scheme outline or plan that is used to generate answers to research problems. This study employed descriptive survey design. A descriptive study attempts to describe or define a subject, often by creating a profile of a group of problems, people, or events, through the collection of data and tabulation of the frequencies on research variables or their interaction as indicated by Cooper and Schindler (2007). Descriptive research is more rigid and seeks to describe uses of a product, determine the proportion of the population that uses a product, or predict future demand for a product (Orodho, 2003). The choice of the descriptive survey design was made based on the fact that in the study, the research was interested on the state of affairs already existing in the field and no variable was manipulated.

3.3 Target Population

Cooper and Schindler (2007) define target population as the entire group that is of interest to the researcher. The target population of interest in this study comprised of all 630unionisable staff members as well as the management staffof all the KCB branches in Central Region.

Table 3.1: Target Population and Sample Size

	Target Population	Sample size
Senior managers	6	6/630x241= 2
Middle level and Lower Level managers	162	162/630x241= 62
Unionisable staff members	462	462/630x241= 177
Total	**630**	**241**

3.4 Sample Size

The researcher used a sample size of 241 staff members as shown on Table 3.2

Source: Author, 2013

The formula by Kathuri and Pals (1993) is as follows:

$$n = \frac{\chi^2 NP\,(1-P)}{\sigma^2\,(N-1) + \chi^2\,P\,(1-P)}$$

Where:

n = required sample size

N = the given population size from the sampling frame

σ^2 = the degree of accuracy; σ value is 0.05

χ^2 = Table value of chi-square for one degree of freedom, which is 3.841

P = Population proportion, assumed to be 0.50

3.5Sample size and Sampling Procedure

Sampling is the process of selection of appropriate number of subjects from a defined population (Chalmers, 2002). From the above population of 630 respondents, a representative sample of 241staff members was drawn usingKrejie and Morgan (1970) table. (See appendix 5 for results table). Random sampling was used to obtain the study sample proportionately. The study employed stratified random sampling technique in selecting the managers based on the management level. Stratified random sampling is unbiased sampling method of grouping heterogeneous population into homogenous subsets then making a selection within the individual subset to ensure representativeness. The goal of stratified random sampling was to achieve the desired representation from various sub-groups in the population. In stratified random sampling subjects are selected in such a way that the existing sub-groups in the population are more or less represented in the sample (Mugenda and Mugenda, 2003).

3.6Data Collection Instruments

To collect primary data a semi-structured questionnaire was used. In order to ensure uniformity in response, and to encourage participation, the questionnaire was kept short and structured with mostly multiple-choice selections in a likert scale. This study collected both primary and secondary data. Primary data was collected using a questionnaire with close ended and open ended questions administered to the respondents. The questionnaire was divided into two parts. The first part was mainly on the demographics which enables the researcher get an indication of the nature of the institution, while the other was to evaluate the study variables. The questionnaires were preferred in this study because respondents of the study were literate and quite able to answer questions asked adequately. According to Mugenda and Mugenda (2003), questionnaires are commonly used to obtain important information about a population under study. The questionnaire was carefully designed and tested with a few members of the population for further improvements. This was done in order to enhance its validity and accuracy of data to be collected for the study. This study collected data using a semi structured questionnaire. The researcher delivered the questionnaires to the respondents either personally or through the research assistants and had them filled as she waits.

3.7 Validity and reliability of research instruments

Validity is the degree to which results obtained from the nanalysis of trhe data actually represent the phenomenon under study (Mugenda and Mugenda, 1999). Piloting wasconducted to check the questionnaires content, general form, question sequence, question formulation and wording in all the KCB Branches in Muranga County. There are 5KCB branches in MurangaCounty, and the total staff in these 5 branches is 105 staff members. The researcher selected a sample of subjects for pilot study using simple random sampling. Mugenda and Mugenda (2003)argue that a sample of 10% of the study sample is sufficient for piloting the study instrument. This therefore meant that there were 11 staff members involved in the pilot study. The tools were thereafter revised according to the findings of the pilot test, and the revised tool was used in the final study.

3.7.1Validity of Research Instrument

According to Cooper and Schindler (2007), content validity is determined by expert judgment. To establish the content validity of the research instrument the researcher sought opinions of experts in the field of study especially the lecturers in the department of project management. This helped to improve the content validity of the data that was collected. It facilitated the necessary revision and modification of the research instrument thereby enhancing validity.

3.7.2 Reliability of Research Instruments

Mugenda and Mugenda (1999), define reliability as a measure of the degree to which research instruments yield consistent results after repeated trials. Reliability was increased by including many similar items on a measure, by testing a diverse sample of individuals and by using uniform testing procedures. The researcher selected a pilot group of 18 individuals from the target population to test the reliability of the research instruments. The study usedSplit-Half Reliability method to establish the reliability which assessed the degree to which test scores are consistent between the two halves of a test. Measurements were gathered from a single rater who uses the same methods or instruments and the same testing conditions. If the correlation between the halves administrations of the test is high (for example 0.7 or higher), then it had good reliability. Split-Half Reliability is a useful measure when impractical or undesirable to assess reliability with two tests or to have two test administrations (because of limited time or money) (Cohen &Swerdlik, 2001).

3.8 Data Collection Procedure

The researcherapplied for permission for research from Kenya Commercial Bank Limited, Audit and Risk department. The researcher also applied for a permit from the Ministry of Science and

Technology to carry out the research.Meanwhile the researcher recruited research assistant and train them on data collection techniques. The pilot study was conducted in all KCB branches in Muranga County in Kenya, after which the data was analyzed and the questionnaire was amended/revised as per the findings of the pilot test. This revised research tool was used in the final study.

The researcher created a rapport with the Risk and Audit department so that the research assistants could proceed with the distribution of the questionnaires among the identified respondents. The researcher and the assistants guided the respondents throughout the questionnaire to ensure that the respondents were aware and clear with the questions and answers they were providing.

3.9 Data Analysis

The researcher edited the completed questionnaires for completeness and consistency. Data clean-up followed. The data was then analyzed using descriptive statistics. The descriptive statistical tool (SPSS and Excel) were used to help the researcher to describe the data. Likert scale was used to analyze the mean score and standard deviation. The findings were presented using tables and graphs for further analysis and to facilitate comparison. This generated quantitative reports through tabulations, percentages, and measure of central tendency.

The researcher further employed multivariate regression model to study the causes of electronic fraud in the banking industry in Kenya. The research deemed regression method to be useful for its ability to test the nature of influence of independent variables on a dependent variable. Regression was able to estimate the coefficients of the linear equation, involving one or more independent variables, which best predicted the value of the dependent variable. Therefore, the researcher used linear regression analysis to analyze the data.

3.10 Ethical Consideration

The study collected sensitive information; therefore, the researcher had a moral obligation to treat the information with utmost modesty. The researcher ensured the respondents confidentiality of the information given so that the respondents were not reluctant to give the information sought by the study.

3.11 Operationalization of Variables

The tabulation below shows the operational indicators which was used during the study on the influence of electronic fraud in the banking industry in Kenya, a case of KCB Kenya, Central Region.

Table 3.2: Operational definition of variables

Objective	Variable	Indicators	Measurement scale	Tools of analysis	Type of data analysis
To establish the influence of quality of management on electronic fraud in the banking industry	**Independent:** Quality management	Fraud detection capabilities among the management staff Monitoring capacity for suspicious behavior Pre-employment screening process Lack of knowledgeable programmers and security experts Post-hiring employee monitoring Integration of risk management into operational decisions and business processes Insincerity of bank staff	Ordinal Ratio	Mean Percentage Correlation	Descriptive Regression
To establish the extent of influence of security controls on electronic fraud in the banking industry	Security controls	E-identity and authentication mechanisms (KYC) Business rule management systems Network failure Lack of standardized online identity verification and authentication tools Investments cost of fraud prevention tools Phone verification and notification products Two-factor authentication procedure for online banks Transaction monitoring programs for debit and credit card Using a similar international online identity solution for all payment types	Ordinal Ratio	Mean Percentage Correlation	Descriptive Regression

		Protection of customer privacy (account information) Manual checks Statistical profiling			
To assess the influence of salaries and remuneration on electronic fraud in the banking industry	Salaries and remuneration	Poor basic pay compared to market rate Rapid promotion for inexperienced hands Allowances Retirement benefits Insurance cover Bonuses	Ordinal Ratio Interval	Mean Percentage	Descriptive Regression
To establish the influence of the level of awareness of the customer, how this influences their behavior in relation to electronic fraud in the banking industry	Level of awareness of the customer	Customer ignorance on identification procedures Disclosure of password or PIN Stolen or cloned card Fraudster use of imaging techniques, cameras and other gadgets Phishing (using fake emails and/or fake websites) Trojan horse (embedding a computer virus type software program onto the customer's PC) Identity theft	Ordinal Ratio	Mean Percentage	Descriptive Regression
	Dependent: Electronic fraud in the banking industry	Number of frauds reported Number of customer complains related to electronic fraud.	Interval	Mean Percentage	Descriptive Regression

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

This chapter discusses the interpretation and presentation of the findings. This chapter presents analysis of the data on the factors influencing electronic fraud in the banking industry in Kenya: a case study of Kenya Commercial Bank (central region). The chapter also provides the major findings and results of the study.

4.1.1 Response Rate

The study targeted a sample size of 241 respondents from which 176 filled in and returned the questionnaires making a response rate of 73%. This response rate was good and representative and conforms to Mugenda and Mugenda (1999) stipulation that a response rate of 50% is adequate for analysis and reporting; a rate of 60% is good and a response rate of 70% and over is excellent.

4.2 Demographic Characteristics

The study sought to establish the background information of the respondents including respondents' gender, age bracket, level of education and work experience.

4.2.1 Gender of the Respondent

The gender of the respondents was a key factor in determining extent to which the various variables influence electronic fraud in the banking industry. The researcher was able to tell whether the gender has any effect on the various variables used on the study. The response was as shown on Table 4.1.

Table 4.1: Gender of the Respondents

	Frequency	Percent
Female	85	48
Male	91	52
Total	176	**100.0**

The findings in Table 4.1 show the gender of the respondents. From the findings, the study established that the majority of respondents were male as shown by 52% while females were 48% of the respondents. This shows that there was gender equality at Kenya Commercial Bank.

4.2.2 Age of the respondents.

The researcher felt that the age of the respondents was a key component while caarying out this research. The results of this demographic characteristic is as shown on Table 4.2.

Table 4.2: Age Bracket of the Respondents

AGE (YEARS)	Frequency	Percent
Less than 30yrs	38	21.74
30 to 39 years	126	71.74
40 to 49 years	8	4.35
50 to 59 years	4	2.17
Total	**176**	**100.0**

The study sought to find out the age of the respondents. The study found that the majority of the respondents were between 30 - 39 years (71.74%), 21.74% were aged less than 30 years, 4.35% were aged 40 - 49 years and 2.17% were aged between 50-59 years. This shows that majority of the employees are middle aged.

The study also sought to establish the respondents' highest level of education.

4.2.3 Respondents' level of education

The level of education was also a demographic characteristic that the researcher felt was important to incorporate in the study, because it can greatly influence the results of the study, and the results are as shown on Table 4.3.

Table 4.3: Respondents' level of education

	Frequency	Percent
Postgraduate	32	17.9
Undergraduate	95	53.7
Diploma	29	16.4
Certificate	21	11.9
Total	**176**	**100.0**

According to the findings, shown on Table 4.3 the majority of the respondents (53.7%) had an undergraduate degree, 17.9% had a postgraduate degree, 16.4% had a diploma while 11.9% of the respondents had a certificate. That is satisfactory level of education that can comfortably facilitate proper understanding of the research questionnaire and respond from a point of knowledge.

The study also sought to establish the years of service/working period(experience) at Kenya Commercial Bank.

4.2.4 Duration of work in the company

It's important to know how long the respondents have worked in the bank because the longer they have worked the more experience they have especially on fraud related issues like fraud detection and fraud investigation. The findings are as elaborated in Table 4.4.

Table 4.4: Duration of work in the company

	Frequency	Percent
1 to 5 years	42	23.9
6 to 10years	11	6.0
11 to 15 years	53	29.9
16 to 20 years	24	13.4
21 years and above	47	26.9
Total	**176**	**100.0**

On the years of service/working period at Kenya Commercial Bank, the findings in Table4.4 show that 26.9% of the respondents had worked for 21 years and above, 29.9% had worked for 11 to 15 years, 23.9% had worked for 1 to 5 years, 13.4% had worked for 16 to 20 years, while 6% had worked at the bank for 6 to 10years.

4.3Quality of Management and Electronic Fraud in the Banking Industry

The study sought to establish the extent that quality of management influence electronic fraud in the banking industry.

Table 4.5: Extent that quality of management influences electronic fraud in the banking industry

	Frequency	Percent
Moderate extent	8	4.5
Great extent	18	10.4
Very great extent	150	85.1
Total	176	**100.0**

Regarding the extent that quality of management influence electronic fraud in the banking industry, as shown on Table 4.5 majority of the respondents (85.1%) indicated that quality of management influence electronic fraud in the banking industry to a very great extent, 10.2% said to a great extent while 4.5% of the respondents felt that quality of management influence electronic fraud in the banking industry to a moderate extent.

Table 4.6: Extent that aspects of quality of managementinfluenceelectronic fraud in the banking industry

	Mean	Std. Deviation
Fraud detection capabilities among the management staff	4.44	.66
Monitoring capacity for suspicious behavior	3.96	1.17
Pre-employment screening process	3.91	1.01
Lack of knowledgeable programmers and security experts	4.06	.72
Post-hiring employee monitoring	4.19	.68
Integration of risk management into operational decisions and business processes	4.40	.68
Insincerity of bank staff	3.54	1.03
Work load of the staff	3.82	0.13
Lack of experience	4.01	0.22

On the extent that aspects of quality management affect electronic fraud in the banking industry, the respondents indicated that the aspects of quality management affect electronic fraud in the banking industry to a great extent include fraud detection capabilities among the management staff as shown by a mean score of 4.44, integration of risk management into operational decisions and business processes as shown by a mean score of 4.40, post-hiring employee monitoring as shown by a mean score of 4.19, lack of knowledgeable programmers and security experts as shown by a mean score of 4.06, lack of experience as shown by a mean score of 4.01, monitoring capacity for suspicious behavior as shown by a mean score of 3.96, pre-employment screening process as shown by a mean score of 3.91, work load of the staff as shown by a mean score of 3.82 and insincerity of bank staff as shown by a mean score of 3.54.

4.4 Security Controlsand Electronic Fraud in the Banking Industry

The study further sought to find out the influence of security controls on electronic fraud in the banking industry.

Table 4.7: Extent that security controls influence electronic fraud in the banking industry

	Frequency	**Percent**
Little extent	11	6.0
Moderate extent	16	9.0
Great extent	37	20.9
Very great extent	113	64.2
Total	176	**100.0**

From the study findings portrayed in Table 4.7, most of the respondents (64.2%) indicated that security controls influence electronic fraud in the banking industry to a very great extent, 20.9% said to a great extent, 9% said to a moderate extent while 6% of the respondents were of the view that security controls influence electronic fraud in the banking industry to a little extent.

The researcher also wanted to establish the extent that various aspects of security controls influence electronic fraud in the banking industry.

Table 4.8: Extent that aspects of security control influence electronic fraud in the banking industry

	Mean	Std. Deviation
E-identity and authentication mechanisms (KYC)	3.67	.56
Business rule management systems	4.04	.64
Network failure	4.49	.68
Lack of standardized online identity verification and authentication tools	4.19	.68
Investments cost of fraud prevention tools	3.82	0.34
Phone verification and notification products	3.90	0.80
Two-factor authentication procedure for online banks	3.42	0.13
Transaction monitoring programs for debit and credit card	4.28	0.10
Using a similar international online identity solution for all payment types	3.22	0.60
Protection of customer privacy (account information)	4.32	0.31
Manual checks	3.81	0.22
Statistical profiling	4.12	0.80

According to the findings on Table 4.8, majority of the respondents indicated that the aspects of security control that influence electronic fraud in the banking industry to a great extent include network failure as shown by a mean score of 4.49, protection of customer privacy (account information) as shown by a mean score of 4.32 transaction monitoring programs for debit and credit card as shown by a mean score of 4.28, lack of standardized online identity verification and authentication tools as shown by a mean score of 4.20, statistical profiling as shown by a mean score of 4.12, business rule management systems as shown by a mean score of 4.04, phone verification and notification products as shown by a mean score of 3.90, investments cost of fraud prevention tools as shown by a mean score of 3.82, manual checks as shown by a mean score of 3.81 and E-identity and authentication mechanisms (KYC) as shown by a mean score of 3.67. They however indicated that two-factor authentication procedure for online banks and using a similar international online identity solution for all payment types influence electronic fraud in the banking industry to a moderate extent as shown by a mean score of 3.42 and 3.22 respectively.

4.5 Salaries and Remunerationand Electronic Fraud in the Banking Industry

The study further sought to establish the influence of salaries and remuneration on electronic fraud in the banking industry.

Table 4.9: Extent that salaries and remuneration influence electronic fraud in the banking industry

	Frequency	Percent
Moderate extent	3	1.5
Great extent	50	28.4
Very great extent	123	70.1
Total	**176**	**100.0**

From the findings as shown on Table 4.9, 70.1% of the respondents indicated that salaries and remuneration influence electronic fraud in the banking industry to a very great extent, 28.4% said to a great extent while 1.5% said salaries and remuneration influence electronic fraud in the banking industryto a moderate extent.

The study sought to establish the extent that aspects of salaries and remuneration influence electronic fraud in the banking industry.

Table 4.10: Extent that aspects of salaries and remuneration influence electronic fraud in the banking industry

	Mean	Std. Deviation
Poor basic pay compared to market rate	4.02	.50
Rapid promotion for inexperienced hands	4.03	.52
Allowances	4.14	.60
Retirement benefits	3.93	.86
Insurance cover	3.34	.72
Bonuses	4.23	.15

As shown on Table 4.10 the study found that the aspects of salaries and remuneration influence electronic fraud in the banking industry to a great extent include bonuses as shown by a mean score of 4.23, allowances as shown by a mean score of 4.14, rapid promotion for inexperienced hands as shown by a mean score of 4.03, poor basic pay compared to market rate as shown by a mean score of 4.02 and retirement benefits as shown by a mean score of 3.93 while insurance cover had a moderate influence as shown by a mean score of 3.34.

4.6 Level of Awareness of the Customerand Electronic Fraud in the Banking Industry

The study sought to explore the influence of level of awareness of the customer on electronic fraud in the banking industry.

Table 4.11: Extent that level of awareness of the customer influence electronic fraud in the banking industry

	Frequency	Percent
No extent	14	7.7
Moderate extent	5	2.9
Great extent	42	23.8
Very great extent	115	65.6
Total	**176**	**100.0**

As shown on Table 4.6 majority of the respondents (65.6%) indicated that level of awareness of the customer influence electronic fraud in the banking industry to a very great extent, 23.8% said it influences to a great extent, 7.7% said it does not influence at all while 2.9% of the respondent indicated that level of awareness of the customer influence electronic fraud in the banking industry to a moderate extent.

The study also sought to find out the extent that aspects of level of awareness of the customer influence electronic fraud in the banking industry.

Table 4.12: Extent that aspects of level of awareness of the customer influence electronic fraud in the banking industry

	Mean	Std. Deviation
Customer ignorance on identification procedures	4.49	.86
Disclosure of password or PIN	3.87	.80
Stolen or cloned card	4.19	.97
Fraudster use of imaging techniques, cameras and other gadgets	3.74	.97
Phishing (using fake emails and/or fake websites)	4.02	.61
Trojan horse (embedding a computer virus type software program onto the customer's PC)	3.82	.61
Identity theft	3.91	.13

On the extent that various aspects of level of awareness of the customer influence electronic fraud in the banking industry, as shown on Table 4.12 majority of the respondents indicated that the aspects of level of awareness of the customer influence electronic fraud in the banking industry to a great extent include customer ignorance on identification procedures as shown by a mean score of 4.49, stolen or cloned card as shown by a mean score of 4.19, phishing (using fake emails and/or fake websites) as shown by a mean score of 4.02, identity theft as shown by a mean score of 3.91, disclosure of password or pin as shown by a mean score of 3.87, trojan horse (embedding a computer virus type software program onto the customer's pc) as shown by a mean score of 3.82 and fraudster use of imaging techniques, cameras and other gadgets as shown by a mean score of 3.74.

4.7 Electronic Fraud in the Banking Industry

The study also sought to determine whether the departments that respondents work in have strategies that are intended to conserve environment.

Table 4.13: Trend of Electronic Fraud in the bank for the last five years

	Mean	Std. Deviation
Card fraud	4.02	.60
Identity theft	3.34	.70
Misrepresentation	4.18	.66
Money laundering	3.25	.66
Fraudulent deposits	4.12	.90

On the trend of electronic fraud in the bank for the last five years, as shown on Table 4.13 majority of the respondents indicated that misrepresentation, fraudulent deposits and card fraud has increased as shown by a mean score of 4.18, 4.12 and 4.02 respectively while identity theft and money laundering were constant as shown by a mean score of 3.34 and 3.25 respectively.

4.8 Regression Analysis

In this study, a multiple regression analysis was conducted to test the influence among predictor variables and electronic fraud in the banking industry. The research used statistical package for social sciences (SPSS V 21.0) to code, enter and compute the measurements of the multiple regressions

Table 4.14: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.87	0.75	0.69	0.73

R-Squared is a commonly used statistic to evaluate model fit. R-square is 1 minus the ratio of residual variability. The adjusted $R^{2,}$ also called the coefficient of multiple determinations, is the percent of the variance in the dependent explained uniquely or jointly by the independent variables. 69.02% of the changes in the electronic fraud in the banking industry could be attributed to the combined effect of the predictor variables.

Table 4.15: **Summary of One-Way ANOVA results**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	9.22	4	2.31	9.20	0.0001
	Residual	42.88	171	0.25		
	Total	52.10	175			

The probability value of 0.0001 indicates that the regression relationship was highly significant in predicting how quality management, security controls, salaries and remuneration and level of awareness of the customer influenced Electronic fraud in the banking industry. The F calculated at 5% level of significance was 9.20 since F calculated is greater than the F critical (value = 2.5252), this shows that the overall model was significant.

Table 4.16: Regression coefficients of the relationship between electronic fraud in the banking industry and the four predictive variables

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.053	0.217		4.85	2.73E-06
	Quality management	0.682	0.149	0.613	4.58	9.03E-06
	Security controls	0.701	0.181	0.149	3.87	1.53E-04
	Salaries and remuneration	0.599	0.196	0.234	3.06	2.60E-03
	Level of awareness of the customer	0.763	0.091	0.138	8.39	1.82E-14

As per Table 4.16, the equation ($\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon}$) becomes:

$Y = 1.053 + 0.682X_1 + 0.701X_2 + 0.599X_3 + 0.763X_4$

Where Y is the dependent variable Electronic Fraud in the Banking Industry

X_1 - Quality management

X_2 - Security controls

X_3 - Salaries and remuneration

X_4 - Level of awareness of the customer

The regression equation above has established that taking all factors into account (quality management, security controls, salaries and remuneration and level of awareness of the customer) constant at zero electronic fraud in the banking industry will be 1.053. The findings presented also show that taking all other independent variables at zero, a unit increase in the quality management would lead to a 0.682 increase in the scores of electronic fraud in the banking industry and a unit increase in the scores of security controls would lead to a 0.701 increase in the scores of electronic fraud in the banking industry. Further, the findings shows that a unit increases in the scores of salaries and remuneration would lead to a 0.599 increase in the scores of co electronic fraud in the banking industry. The study also found that a unit increase in the scores of level of awareness of the customer would lead to a 0.763 increase in the scores of electronic fraud in the banking industry.

Overall, level of awareness of the customer had the greatest effect on the electronic fraud in the banking industry, followed by security controls, then quality management while level of salaries and remuneration had the least effect to the electronic fraud in the banking industry in Kenya. All the variables were significant ($p<0.05$).

CHAPTER FIVE

SUMMARY OF FINDINGS, DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presented the discussion of key data findings, conclusion drawn from the findings highlighted and recommendation made there-to. The conclusions and recommendations drawn were focused on addressing theobjective of the study.

5.2 Summary of Findings

The study sought to establish the influence of security controls, level of awareness of the customer, communication strategy and quality management on electronic fraud at Kenya Commercial Bank

5.2.1 Quality of Management and Electronic Fraud in the Banking Industry

The study deduced that quality of management influences electronic fraud in the banking industry to a very great extent such that a unit increase in the scores of security controls would lead to a 0.701 increase in the scores of electronic fraud in the banking industry. This is mainly through fraud detection capabilities among the management staff, integration of risk management into operational decisions and business processes, post-hiring employee monitoring, lack of knowledgeable programmers and security experts, lack of experience, monitoring capacity for suspicious behavior, pre-employment screening process, and work load of the staff and insincerity of bank staff.

5.2.2 Security Controlsand Electronic Fraud in the Banking Industry

The study further established that security controls influence electronic fraud in the banking industry to a very great extent. The aspects of security controls that influence electronic fraud at Kenya Commercial Bank to a very great extent include network failure, protection of customer privacy (account information), transaction monitoring programs for debit and credit card, lack of standardized online identity verification and authentication tools, statistical profiling, business rule management systems, phone verification and notification products, investments cost of fraud prevention tools, manual checks and E-identity and authentication mechanisms (KYC).

5.2.3 Salaries and Remunerationand Electronic Fraud in the Banking Industry

The study established that salaries and remuneration strategies such as bonuses, allowances, rapid promotion for inexperienced hands, poor basic pay compared to market rate and retirementbenefits influence the electronic fraud in the banking industry to a very great extent.

5.2.4 Level of Awareness of the Customerand Electronic Fraud in the Banking Industry

This study also revealed that level of awareness of the customer influence electronic fraud in the banking industry to a very great extent mainly through customer ignorance on identification procedures, stolen or cloned card, phishing (using fake emails and/or fake websites), identity theft, disclosure of password or pin, trojan horse (embedding a computer virus type software program onto the customer's pc) and fraudster use of imaging techniques, cameras and other gadgets.

It was clear that misrepresentation, fraudulent deposits and card fraud has increased for the last five years while identity theft and money laundering were constant. Overall, level of awareness of the customer had the greatest effect on the electronic fraud in the banking industry, followed by security controls, then quality management while level of salaries and remuneration had the least effect to the electronic fraud in the banking industry in Kenya.

5.3 Discussion

This section sought to discuss the effect of security controls, level of awareness of the customer, level of salaries and remuneration and quality management on electronic fraud in the light of previous studies done.

5.3.1 Quality of Managementand Electronic Fraud in the Banking Industry

The study deduced that that quality of management influence electronic fraud in the banking industry to a very great extent. These findings correlate with Afam (2009) who indicated that the management should learn how they can integrate risk management into their most important operational decisions and business processes, such as Anti-Money Laundering (AML), Know Your Customer (KYC) and credit risk.

The study found that the aspects of quality of management influence electronic fraud in the banking industry to a great extent fraud detection capabilities among the management staff, integration of risk management into operational decisions and business processes, post-hiring employee monitoring, lack of knowledgeable programmers and security experts, lack of experience, monitoring capacity for suspicious behavior, pre-employment screening process, work load of the staff and insincerity of bank staff. The findings are consistent with McFadden (2007) who observed that from card fraud to identity theft and misrepresentation, providers have had to adapt the way they manage their businesses, their customer identification procedures and their fraud prevention tools. Loviglio (2012) also posited that risk management solutions combined with trusted e-identity and authentication mechanisms are needed.

5.3.2 Security Controlsand Electronic Fraud in the Banking Industry

The study revealed that security controls influence electronic fraud in the banking industry to a very great extent.Afam (2009) confirmed this when he submitted that there is nowhere in the world that experiences the embarrassingly high level of ATM card fraud other than Nigeria because the implementation of the technology in Nigeria is characterized by ineptitude, lack of knowledgeable programmers and security experts that could guide and implement a secure transaction channel regardless of the level of education of the ATM card users. He further accused the Nigerian ATM technology of being too simplistic.

The aspects of security controls that influence electronic fraud at Kenya Commercial Bank to a very great extent include network failure, protection of customer privacy (account information), transaction monitoring programs for debit and credit card, lack of standardized online identity verification and authentication tools, statistical profiling, business rule management systems, phone verification and notification products, investments cost of fraud prevention tools, manual checks and E-identity and authentication mechanisms (KYC). In line with this, empirical evidences have justified that network failure is another common cause of ATM fraud. In the view of Ellen (2009), mass compromise of merchant networks and card processors is viewed as the main cause of payment-card fraud. According to the survey, sponsored by a security firm, Actimize, 94% of the 113 financial-services firms could trace some percentage of payment-card fraud they experienced directly back to mass compromises of networks. Also in the survey, several examples of mass compromise events were given, including those known to have occurred at Heartland Payment Systems and grocery retailer.

The findings also concurs with Ernst and Young (2000) who posited that many debit and credit card companies have begun to implement special transaction monitoring programs that look at every transaction made with a bank card. A special computer database examines each transaction and compares it to the regular pattern of a consumer. If something seems out of the ordinary, the bank and consumer will be alerted, and a manual verification of the transaction is often required

5.3.3 Salaries and remunerationand Electronic Fraud in the Banking Industry

Keeping financial information secure and confidential, including within Online Banking, is one of our most important responsibilities. Whenever personal information is requested or displayed on our website we use encryption technology, such as Secure Socket Layer (SSL), to prevent unauthorized access to data (Helmut, 2004). The study findings indicated that salaries and remuneration strategies such as bonuses, allowances, rapid promotion for inexperienced hands, poor basic pay compared to market rate and retirementbenefits influence the electronic fraud in the banking industry to a very great extent.

These findings are in line with those by Valentine (2010) who indicated that apart from the simplicity of the ATM technology being used in Nigeria, insincerity of bank staff is another reason that has contributed to the widening rate of ATM scam in Nigeria. This has aborted virtually all the attempts made by banks to fight the ATM scam improprieties. The banks, too, open a window for fraudsters in their indiscriminate issuance of cards to customers without regard to their ability to utilize them. It has been said “that the various ATM service providers, whose fierce competition for market share makes the possibility of a united attack on the menace of ATM fraudsters impossible, are another factor that sustains the peril (Valentine, 2010).

5.3.4 Level of Awareness of the Customerand Electronic Fraud in the Banking Industry

ATM and credit fraud occurs when a stolen or cloned card is used by criminals to withdraw cash from a customers' account. The study found that level of awareness of the customer influence electronic fraud in the banking industry to a very great extent. To protect against such frauds, customers are advised to memorize their PINs and never to write it down or share it with any other person. They should desist from the habit of giving cards and PINs to other people to withdraw money on their behalf. Cardholders should never use a card in an ATM where they see suspicious equipment or people. Always insist that cashier's swipe customer's cards in a machine that should be well located at the counters in the site of the cardholder and not under the counters or back offices (Mena, 2002).

It was deduced that the level of awareness of the customer affecting electronic fraud in the banking industry to a great extent include customer ignorance on identification procedures, stolen or cloned card, phishing (using fake emails and/or fake websites), identity theft, disclosure of password or pin, trojan horse (embedding a computer virus type software program onto the customer's pc) and fraudster use of imaging techniques, cameras and other gadgets. In line with this, Adeyemi (2010) observed that criminal obtains the customer's account access data, that is, logon name and password using different schemes. The "over the shoulder looking" scheme occurs when a customer performs financial transactions while being observed by a criminal. A fair number of cases have been reported where customer's account access data was obtained by the criminal just by observing customers at a public Internet access point. Hackers often take aim at small firms' computers because they are easier to infiltrate than banks' systems. One common mode of attack is to send a "spear phishing" email containing an infected file or a link to a malicious Web site to employees with access to the firm's financial accounts. Once the employee opens the attachment or goes to the Web site, malware is installed on the computer that allows criminals to access banking logins and passwords. While up-to-date antivirus software offers substantial protection against malware, it isn't 100% effective (MacRae, 2001).

5.4 Conclusions of the study

The increasing prevalence of enterprise financial crimes has made fraud prevention and investments in prevention technology a long-overdue priority to organizations around the world. From the findings, the study concludes that quality of management influence electronic fraud in the banking industry through fraud detection capabilities among the management staff, integration of risk management into operational decisions and business processes and post-hiring employee monitoring.

The study revealed that the aspects of security controls such as network failure, protection of customer privacy (account information), transaction monitoring programs for debit and credit card, lack of standardized online identity verification and authentication toolsinfluence the electronic fraud in the banking industry.

The study also concludes that salaries and remuneration influence electronic fraud in the banking industry to a very great extent. This is mainly through bonuses, allowances, rapid promotion for inexperienced hands, poor basic pay compared to market rate and retirement benefits.

The study further deduced that level of awareness of the customer through customer ignorance on identification procedures, stolen or cloned card, phishing (using fake emails and/or fake websites), identity theft and disclosure of password or pin.

The study finally concludes that level of awareness of the customer had the greatest effect on the electronic fraud in the banking industry, followed by security controls, then quality management while level of salaries and remuneration had the least effect to the electronic fraud in the banking industry.

5.5 Recommendations of the study

i. From the study findings and conclusions, the study recommends that the top management in the banks should ensure that they fully support fraud detection policies by allocating enough resources to them in order to gain a competitive edge. It is recommended that the management at the banks should be dedicated to encourage fraud detection training among staff to enhance their capabilities. The banks should also recruitknowledgeable programmers and security expert to deal with the recurring menace. The banks should encourage teamwork, improve the working environments and set clear roles and responsibilities.

ii. The study further recommends that there is need to improve on the efficiency of communication between the branches and interdepartmental communication at Kenya Commercial Bank as network failure is a major contributor to fraud. This will enhance the vigilance at all the quotas and enhance better understanding of policies and fastens decision making. The banks should protect customer privacy (account information) by deploying standardized online identity verification and authentication tools and statistical profiling.

iii. The study also recommends that the administration at the banks should enhance the employee morale and satisfaction through bonuses and allowances. The banks should also lid of the high turnover rate experienced at the banks by having a rapid promotion scheme for the experienced hands.

iv. The study finally recommends that the management at the banks should enhance the training among the customers on the possible loopholes which the fraudsters use to defraud those creating distinctive capabilities among them. The study recommend that the customers should be trained on the importance of fraud prevention through seminars and workshops as the study found awareness of the customer to be a major factor affecting electronic fraud in the banking industry. Customers should review their agreement with the bank and know what rights they may be waiving by not using certain security measures. Further, banks, concerned about damage to customer relationships, should stepped up their defenses against cyber-attacks and roll out new protections for customers and begin sharing more threat information with each other and law enforcement.

5.6 Suggestion for Further Studies

Another study should be done to investigate the factors influencing electronic fraud in the other commercial banks in Kenya to allow for generalization. A similar study should also be done on other companies such as the insurance and microfinance institutions since their operations are different from that of banks. Further studies should be done on the influence of the electronic fraud on performance of commercial banks.

REFERENCES

Adeyemi, A. (2010). Winning customers' confidence: The new banking focus. *The Guardian*, May 26: 25.

Adsit, D. (2011). Small Daily Security Breaches Worse than Large High-Profile Ones. *cardnotpresent.com*. Archived from the original on 2012-07-09.

Afam, N. (2009). The real problems with ATM card fraud in Nigeria. [Online] Available:http://www.technologytimesng.com/2009/10/29/the-real-problems-with-atm-cardfraudin-nigeria/ (May 12, 2010)

Akindele R.I, Nassar M.L and Owolabi A.A. (2008).Essentials of Research methodology ObafemiAwolowo University Publisher, Ile- Ife.

Alashi, S.O (1994). *Bank Failure Resolution: The Main Option.*NDIC Quarterly Vol. 3 (2).

Apostolou, B., Hassell, J., Webber, S. (2001a). Management fraud risk factors: ratings by forensic experts, *The CPA Journal*, October, :48-52.

Cain, S. (1999), Fraud in the workplace, *Orange County Business Journal*, Vol. 22 No.16, pp.78.

Carcello, D. and Palmrose, S. (1994). The transactions demand for cash: An inventory theoretic approach. *The Quarterly Journal of Economics*, Vol. 66 No. 4, :545-556.

CBK (2012), banking survey report

Chalmers, M. (2002).*Fundamental of Social Research Methods*.2nd edition. Cape Town: Juta.

Coffin, B. (2009). Trends in corporate fraud, *Risk Management*, Vol. 50 No.5, :9.

Cohen, R.J. and M. Swerdlik, (2001). Psychological Testing and Assessment: An Introduction to Tests and Measurement. 5th Edn., McGraw-Hill, Boston, ISBN: 10: 0767421574, pp: 800.

Cooper, D.R and Schindler, P.S. (2007).*Business Research Methods* (8th edn) McGraw-Hill: New York.

Deming, W. E. (1986). Out of the Crisis. MIT Center for Advanced Engineering Study, Cambridge, MA.

Ellen, M. (2009).Mass network compromise cause of most online fraud. [Online] Available:http://pcworld.about.com/od/security2/Mass-Network-Compromise-Cause.htm (June 30, 2010)

Ernst and Young. (2000). Fraud, The Unmanaged Risk an International survey of the effect of fraud on businesses. 2000 International Survey Ernst and Young. www.E&Y.com.

Heli, S. (2006).*Automated teller machine network market structure and cash usage*. Scientific monographs: ISSN 1456-5951.

Helmut, S. (2004). The Impact of ATM Transactions and Cashless Payments on Cash Demand in Austria.*Monetary Policy & the Economy*, Q1/04, : 90-105.

Katz, D. (2000). Elements of a comprehensive security solution, *Health Management Technology*, Vol. 21 No.6, :12-16

Kathuri, J.N., and Pals, D.A. (1993).*Introduction to Educational Research*.Njoro: Egerton University Press.

KPMG (2001). 2001 global e.fraud survey, available at: www.kpmg.ie/irm/efraud.pdf, .

KPMG (2002). Fraud Survey 2002, KPMG, Darwin, .

Krejcie, R.V. &*Morgan*, D.W. *1970*.Determining sample size for research activities.Educational and psychological measurement. 30. : 607-610.

Laderman, E. S. (2010). The public policy implications of state laws pertaining to automated teller machines.*Federal Reserve Bank of San Francisco Economic Review*, No. 1, pp. 43-58.

Lee, E., and Lee, J. (2000). Haven't adopted electronic financial services yet? The acceptance and diffusion of electronic banking technologies.*Financial counseling and Planning*, Vol. 11 No.1, :49-60.

Loviglio, J. (2012). If Microsoft co-founder's ID isn't safe, is yours?.*msnbc.com*. Archived from the original on 2012-09-03.

MacRae, J. (2001). The Evolution of Insurance Fraud Detection: Claims, Sept 2001 v49 i9 p 51. Insurance Week, Inc. Article #A78542863.

Mativat, N. and Tremblay, U. (1997). Counterfeiting credit cards: displacement effects, suitable offenders and crime wave patterns: British Journal of Criminology, Spring 1997 v 37 n2 p 165(19) .

McFadden, L. (2007). Detecting synthetic identity fraud.*Bankrate.com*. pp. 1–2.Archived from the original on 2012-07-18.Retrieved 2008-09-21.

Mena, J. (2002). Investigative Data Mining for Security and Criminal Detection, Butterworth-Heinemann.

Mohammad, A. (2010). Technology acceptance in Kenyan retail banking.*International Journal of Bank Marketing*, Vol. 6 No.4, :31-41.

Montgomery, D.D., Beasley, M.S., Menelaides, S.L., Palmrose, Z. (2012), Auditors' new procedures for detecting fraud, *Journal of Accountancy*, No.May, pp.63-6.

Mugenda, O.M and Mugenda, A.G (2003) *Research Methods, Quantitative and Qualitative Approaches*, Acts Press, Nairobi

Nwankwo, G.O. (2001). Bank management principles and practices, Malthouse press ltd,Lagos.[12]

Olmos, D. (2009). Social Security Numbers Can Be Guessed From Data, Study Finds. Bloomberg.Archived from the original on 2012-07-19.Retrieved 2011-01-04.

Orodho J.A. (2003), Financing Education in Kenya: Secondary School Bursary School Implementation and Challenges, Discussion Paper 035/2003, Institute of Policy Analysis and Research

Ovia, J. (2001), Internet Banking: Practices and Potentials in Nigeria, A Paper at the Conference Organized by the Institute of Chartered Accountants of Nigeria (ICAN), Lagos, September 5.

Palshikar, G.K. (2002), The hidden truth, Intelligent Enterprise.com, 28 May, :46-51.

Prieston, A. J. and Dreyer, J. A., (2001) Mortgage Fraud, The Impact of Mortgage Fraud on Your Company's Bottom Line, Mortgage Bankers Association of America.

Rezaee, Z. (2004), Causes, consequences and deterrence of financial statement fraud, Critical Perspective on Accounting, in press, .

Samociuk, Martin and Iyer, Nigel (2003) Fraud Resistance, A Practical Guide, SIRCA 01-2003, Standards Australia International Limited ISBN 073375028 1. Journal of Economic Crime Management . Volume 2, Issue 2

The Nilson Report, (December, 2000) Credit Card Fraud Losses 1980 through 2000, Issue # 730 Oxnard, CA.

Valentine, W. (2010).*Use biometrics to tackle ATM fraud*. [Online] Available: http://234next.com/csp/cms/sites/Next/Money/Business/5544853146/story.csp (June 30, 2010)

Whatley, E. (2008). Card Security and Fraud Prevention Source Book.Faulkner and Gray. New York.

Wole, M. O., and Louisa, J. I. (2009). The adoption of automatic teller machines in: An application of the theory of diffusion of innovation. *Issues in Informing Science and Information Technology*, Vol. 6, :374-393.

Young M .R. (2002) Accounting Irregularities and financial fraud.Pp 1-9 Publishers: Aspen law and Business, Aspen Publishers Inc. NY.

APPENDICES

Appendix 1: Introduction letter

DamarisKarimiMwabu

P.O. BOX

Nairobi.

Dear Respondent,

RE: REQUEST FOR PARTICIPATION IN A RESEARCH STUDY

I am a final year Master of Arts student at the University of Nairobi, specializing in project planning and management. I am currently undertaking a research on "FACTORS INFLUENCING ELECTRONIC FRAUD IN THE BANKING INDUSTRY IN KENYA".

I will be grateful if you could spare sometime from your busy schedule and fill in the questionnaire. All the information provided will be purely used for academic purposes and your identity will be treated with utmost confidentiality.

Thank you for your cooperation.

Yours faithfully,

DamarisKarimiMwabu

Appendix 2: Questionnaire

DEMOGRAPHIC INFORMATION

1) Please indicate your gender

Female [ ] Male [ ]

2) Your age bracket (Tick whichever appropriate)

Below 24 Years	[ ]	25 - 30 Years	[ ]
31 - 34 years	[ ]	35 - 40 years	[ ]
41 - 44 years	[ ]	45 - 50 years	[ ]
Over- 51 years			

3) What is your highest education level? (Tick as applicable)

Diploma/certificate	[ ]	Bachelors' degree	[ ]
Postgraduate degree	[ ]	Others-specify……………………………	

4) For how long have you worked with the bank?

Less than 3 years	[ ]
4 to 6 years	[ ]
7 to 9 years	[ ]
Above 10 years	[ ]

QUALITY MANAGEMENT

5) To what extent does quality of management influence electronic fraud in the banking industry?

To a very great extent	[ ]	To a great extent	[ ]
To a moderate extent	[ ]	To a little extent	[ ]
To no extent	[ ]		

6) What is the extent to which the following affect electronic fraud in the banking industry?

	Very great extent	Great extent	Moderate extent	Low extent	Not at all
Fraud detection capabilities among the management staff					
Monitoring capacity for suspicious behavior					
Pre-employment screening process					
Lack of knowledgeable programmers and security experts					
Post-hiring employee monitoring					
Integration of risk management into operational decisions and business processes					
Insincerity of bank staff					
Work load of the staff					
Lack of experience					

SECURITY CONTROLS

7) To what extent does security controls influence electronic fraud in the banking industry?

To a very great extent [ ] To a great extent [ ]

To a moderate extent [ ] To a little extent [ ]

To no extent [ ]

8) What is the extent to which the following affect electronic fraud in the banking industry?

	Very great extent	Great extent	Moderate extent	Low extent	Not at all
E-identity and authentication mechanisms (KYC)					
Business rule management systems					
Network failure					
Lack of standardized online identity verification and authentication tools					

Investments cost of fraud prevention tools					
Phone verification and notification products					
Two-factor authentication procedure for online banks					
Transaction monitoring programs for debit and credit card					
Using a similar international online identity solution for all payment types					
Protection of customer privacy (account information)					
Manual checks					
Statistical profiling					

SALARIES AND REMUNERATION

9) To what extent does salaries and remuneration influence electronic fraud in the banking industry?

To a very great extent [ ]   To a great extent [ ]

To a moderate extent [ ]   To a little extent [ ]

To no extent [ ]

10) What is the extent to which the following affect electronic fraud in the banking industry?

	Very great extent	Great extent	Moderate extent	Low extent	Not at all
Poor basic pay compared to market rate					
Rapid promotion for inexperienced hands					
Allowances					
Retirement benefits					
Insurance cover					
Bonuses					

LEVEL OF AWARENESS OF THE CUSTOMER

11) To what extent does level of awareness of the customer influence electronic fraud in the banking industry?

To a very great extent [ ] To a great extent [ ]

To a moderate extent [ ] To a little extent [ ]To no extent [ ]

12) What is the extent to which the following affect electronic fraud in the banking industry?

	Very great extent	Great extent	Moderate extent	Low extent	Not at all
Customer ignorance on identification procedures					
Disclosure of password or PIN					
Stolen or cloned card					
Fraudster use of imaging techniques, cameras and other gadgets					
Phishing (using fake emails and/or fake websites)					
Trojan horse (embedding a computer virus type software program onto the customer's PC)					
Identity theft					

ELECTRONIC FRAUD IN THE BANKING INDUSTRY

13) What is the trend of the following in your bank for the last five years?

	Greatly Increased	Increased	Constant	Decreasing	Greatly decreased
Card fraud					
Identity theft					
Misrepresentation					
Money laundering					
Fraudulent deposits					

THANK YOU

Appendix 3: Required Size for Randomly Chosen Sample

N	**S**	**N**	**S**	**N**	**S**	**N**	**S**
10	10	140	103	550	226	4500	354
15	14	150	108	600	234	5000	357
20	19	160	113	650	241	6000	361
25	24	220	140	700	248	7000	364
30	28	230	144	750	254	8000	367
35	32	240	148	800	260	9000	368
40	36	250	152	1200	291	10000	370
45	40	260	155	1300	297	15000	375
50	44	270	159	1400	302	20000	377
55	48	280	160	1500	306	30000	380
60	52	290	165	1600	310	50000	381
65	56	300	169	1700	313	100000	384
70	59	320	175	1800	317		
75	63	340	181	1900	320		
80	66	360	186	2000	322		
85	70	380	191	2200	327		
90	73	400	196	2400	331		
95	76	420	201	2600	335		
100	80	440	205	2800	338		
110	86	460	210	3000	341		
120	92	480	214	3500	346		
130	97	500	217	4000	351		

Source: Krejie and Morgan (1970). N=Population size

S=Sample size