THE RELATIONSHIP BETWEEN ICT UTILIZATION AND FRAUD LOSSES IN COMMERCIAL BANKS IN KENYA

BY

CECILIA NGALYUKA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE IN MASTER OF BUSINESS ADMINISTRATION, UNIVERSITY OF NAIROBI

OCTOBER 2013

DECLARATION

STUDENT'S DECLARATION

This research project is my original work and has not been presented for a degree at any other university.

Name: CECILIA NGALYUKA D61/72625/2012

Signatureé é é é é é é é é Dateé é é é é é é é é é é é

SUPERVISOR'S DECLARATION

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

Name: Dr. JOSIAH ADUDA

Signatureé é é é é é é é é é Dateé é é é é é é é é é é é .

ACKNOWLEDGEMENTS

I am deeply grateful to the Almighty God who makes all things possible and for giving me strength, good health and sound mind throughout the study period.

I would like to extend my appreciation to my supervisor, family, friends and all the respondents who contributed tremendous inputs towards the successful completion of this research project.

Special gratitude and appreciation go to my Supervisor, Dr. Aduda, and moderator, Mr. Mirie Mwangi, for their patience, guidance, support and dedication throughout the study.

Secondly, I am grateful to my loving husband James, children Staycy, Joan and Joy for their support and encouragement.

Thirdly, I am grateful to the director and staff of the Banking Fraud Investigation Unit who provided invaluable data and information that made this research work a success. I couldnót have done it without them.

DEDICATION

I dedicate this research project to my loving mum, Bernadette.

ABSTRACT

The purpose of this study was to establish the relationship between ICT utilization and fraud losses in commercial banks in Kenya. Secondary data was collected from reports at central bank, Banking Fraud Investigation Unit and audited financial reports of the 43 commercial banks in Kenya. Data was analyzed using SPSS through correlation analysis and regression analysis. The findings were presented in tables and graphs. The major findings of the study indicated that total values transacted through EFT, RTGS and ATM had a positive correlation with the total fraud costs of commercial banks. The level of staff wages also had a positive correlation with fraud losses.

The main conclusions were that ICT utilization has exposed commercial banks in Kenya to more fraud. This is due to the speed of execution of transactions. Adoption of ICT tends to increase the chances of Identity theft due to the fact that transactions are online and real time. The levels of staff wages are also a motivation for fraud from the employee side.

The researcher recommends more robust fraud mitigation practices and policies to ensure that all elements of fraud are captured in the adoption of ICT. Banks should consider increasing their staff costs to mitigate frauds. Bank employees have access to all information relating to customer accounts hence should be well rewarded and motivated in order to prevent them from falling into traps of fraud. The researcher suggests that a similar study be carried out targeting MFIs to get their perspective of the effect of ICT utilization on fraud losses.

Table of Contents

ABBREVIATIONS AND ACRONYMS

ANOVA-Analysis of variance

ATM-Automated Teller Machine

CBK-Central Bank of Kenya

EFT-Electronic Funds Transfer

ICT-Information Communication Technology

KYC-Know Your Customer

LAN-Local Area Network

MIS-Management Information System

R^2-Coefficient of determination

RTGS-Real Time Gross Settlement

SMS-Short Message Service

SPSS-Statistical Package of Social Sciences

TRA-Theory of Reasoned Action

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Fraud has been in existence throughout history and has taken many different dimensions. Bank fraud has grown with advent of the banking industry, and has been facilitated by the technological innovations and the widespread use of the Internet. According to the fraud triangle (Cressey, 1973), for fraud to occur the three factors; pressure, rationalization and opportunity should be present. Bank employees have knowledge of the systems as well as classified and confidential information which together with technological advancement can give them the opportunity to commit frauds. All they need is some pressure and the rationalization and that way they become part of fraud cartels that are fleecing millions of shillings from the banks.

According to a report by consultant firm, Deloitte Kenyan banks were victims of more than half the Sh4.1 billion ($48.3 million) fraud that hit East African banks in 2012 as technology made the crime easier. At least Ksh1.5 billion ($17.64 million) was stolen from Kenyan banks in the past one year, in schemes hatched by technology-savvy bank employees. This can be attributed to failure by both the bank processes and the employees to detect and control fraud. Security experts say the amounts reported reflect only a small portion of the real losses suffered since banks prefer internal disciplinary measures in cases involving thieving employees (Kimani, 2013).This means that banks should be on an alert and should also revise their controls to keep up with fraud and technology.

1.1.1 Information Communication Technology

Information technology has been around for a long, long time. Basically as long as people have been around, information technology has been around because there were always ways of communicating through technology available at that point in time. ICT has transformed the lives of people as well as organizations .It is no surprise that ICT revolution has proven a powerful source for creative vision by utopian thinkers the world over. The reach ICT around the world has been expanding for decades. The recent past has seen particularly rapid rollout of access to communication facilities like telephones and the Internet, as technology advance has driven

down costs (Nyokabi, 2012). Like other countries Kenya has recognized the potential and enabling element of ICT as a tool for social and economic development.

ICT is increasingly seen as a means of enabling other developmental needs rather than as an end in itself hence some types of financial innovation are driven by improvements in ICT. Woherem, (2000) claimed that only banks that overhaul the whole of their payment and delivery systems and apply ICT to their operations are likely to survive and prosper in the new millennium. He recommends that banks should re-examine their service and delivery systems in order to properly position them within the framework of the dictates of the dynamism of ICT.

1.1.2 Fraud

Fraud is an intentional deception made for personal gain to damage another individual. It is a crime and is also a civil law violation. Many hoaxes are fraudulent, although those not made for personal gain are not technically frauds (Wanemba, 2011). According to The American Heritage Dictionary, (Second College Edition), fraud is defined as ña deception deliberately practiced in order to secure unfair or unlawful gainò. In a nutshell, ñFraud always involves one or more persons who, with intent, act secretly to deprive another of something of value, for their own enrichmentò(Davia et al., 2000). Wells, (2005) also stresses deception as the linchpin to fraud. Defrauding people of money is presumably the most common type of fraud, but there have also been many fraudulent discoveries, in art, archaeology, and science.

Bank fraud on the other hand, is the use of fraudulent means to obtain money, assets, or other property owned or held by a financial institution (Glaessner and Mass, 1995). Bank fraud is a crime that has been around for as long as banks have been in operation. Anytime there is a large amount of money floating around, there will be people trying to figure out ways of getting it. Fraud can be committed through many methods, including mail, wire, phone, and the internet (computer crime and internet fraud). The difficulty of checking identity and legitimacy online, the ease with which hackers can divert browsers to dishonest sites and steal credit card details, the international dimensions of the web and the ease with which users can hide their location, all contribute to making internet fraud the fastest growing area of fraud. Estimates are that just twenty percent of frauds are exposed and made public. The remaining frauds are either undetected or discovered and not made public because of reputation risk (Bartlett and Ballantine,

2002). Leuchtner, (2011) identified the common fraud schemes in banks as general ledger fraud, identity theft, account takeover and collusion with external criminals.

Apoorva and Juhi , (2007) defined bank fraud as a deliberate act of omission or commission by any person carried out in the course of banking transactions or in the books of accounts, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank. They concluded that bank frauds are the failure of the banker and mentioned the major elements responsible for the commission of frauds in banks; active involvement of the staff-both supervisor and clerical either independent of external elements or in connivance with outsiders, failure on the part of the bank staff to follow meticulously laid down instructions and guidelines and external elements perpetuating frauds on banks by forgeries or manipulations of cheques, drafts and other instruments. There has been a growing collusion between business, top banks executives, civil servants and politicians in power to defraud the banks, by getting the rules bent, regulations flouted and banking norms thrown to the winds.

1.1.3Effect of ICT Utilization on Fraud

The banking industry has witnessed tremendous changes linked with the developments in ICT over the years. The ICT infrastructure used in banks includes internet access, internal networks and automated payment systems e.g. Automated Teller Machine (ATM), Real Time Gross Settlement (RTGS), Electronic Funds Transfer and cheque truncation. Internet access is a precondition for e-Business as it is the main channel for e-banking. The general availability of Internet allows for the analysis of overall ICT-readiness in the Banking Industry. Products that rely on the internet include both internet and mobile banking.

The application of networks is also vital part of an effective ICT-enabled system, which is especially true in the case of banks with a branch network. Local Area Network (LAN) may also be seen as a basic indicator of the minimum infrastructure required to enable banks to conduct e-banking at a substantial level. Wire-based LAN is currently the dominating technology. Wireless LAN is a relatively new technology in the Banking Industry, and is used to permit bank employees to access network resources from nearly any convenient location. Instant notification of transactions made is another innovation brought by ICT through the use of smart phone in

conjunction with the internet facility in the Banking Industry. There has also been the digitalization of formerly paper-based processes. Electronic mail is increasingly being applied for especially non-legal correspondence like account statements, marketing and sales (Agboola, 2001).

The security issue which is the basis of ICT related fraud is of special concern in the Banking Industry, as banking is highly based on trust from its customers. The risk of hackers, denial of service attacks, technological failures, breach of privacy of customer information, and opportunities for fraud created by the anonymity of the parties to electronic transactions can be managed by enhancing security of information. Depending upon its nature and scope, a breach in security can seriously damage public confidence in the stability of a financial institution or of a nation's entire banking system. By introducing the appropriate security measures and putting security concerns at ease, banks might be able to attract the segments among consumers who previously were not inclined to use e-banking. Furthermore, it is also in the banksô own interest to improve security, as digital fraud can be costly both in financial losses, and in terms of the damage it does to the brand of the bank in question. The common concern among users of e-banking is related to the authentication of users and data connections. This includes the use of digital signatures, PIN codes and encryption (Agboola, 2001).

1.1.4 Commercial Banks in Kenya

A commercial bank is a type of financial intermediary and a type of bank. Commercial banking is also known as business banking. It is a bank that provides checking accounts, savings account, and money market accounts and that accepts time deposits. It raises funds by collecting deposits from businesses and consumers via checkable deposits, savings deposits, and time (or term) deposits. It advances loans to businesses and consumers. It also buys corporate bonds and government bonds. Commercial banksô primary liabilities are deposits, and the primary assets are loans and bonds.

The banking industry in Kenya is governed by the Companies Act, the Banking Act, the Central Bank of Kenya Act and the various prudential guidelines issued by the Central Bank of Kenya (CBK). The CBK, which falls under the Minister for Financeôs docket, is responsible for formulating and implementing monetary policy and fostering the liquidity, solvency and proper

functioning of the financial system. The CBK publishes information on Kenyaôs commercial banks and non-banking financial institutions, interest rates and other publications and guidelines. The banks have come together under the Kenya Bankers Association (KBA), which serves as a lobby for the banksô interests and also addresses issues affecting its members. (Central Bank of Kenya, 2013)

There are forty-three banks and non-bank financial institutions, fifteen micro finance institutions and forty-eight foreign exchange bureaus. Six of the major banks are listed on the Nairobi Securities Exchange. The commercial banks and non-banking financial institutions offer corporate and retail banking services but a small number, mainly comprising the larger banks, offer other services including investment banking. (http://www.centralbank.go.ke).

1.2 Statement of the Problem

Bank fraud has grown with advent of the banking industry, and has been facilitated by the technological innovations and the widespread use of the Internet. The main driver of financial innovations in banks is adoption of ICT. It enables banks to develop sophisticated products, implement reliable techniques for control of risks and to reach geographically distant and diversified markets. On the other hand, a pre-condition for ICT adoption is proper risk management including fraud risk. The risk management framework cannot fully address the risk of fraud because it involves collusion between several parties. As technology advances fraudsters have also become technologically savvy. The speed at which some bank transactions are effected has rendered it almost impossible to detect fraud. Banks are rapidly adopting the Real Time Gross Settlement (RTGS) which processes amounts above one million shillings on a real time and gross basis. This may be a challenge because fraud on such transactions is noticed after it has occurred.

Scholars have different opinions on IT and fraud. Kariuki, (2005) agreed that ICT has positive impacts on the banking performance in commercial banks in Kenya. However, Apoorva and Juhi, (2007) were of the opinion that the losses sustained by banks as a result of frauds exceed the losses due to robbery, burglary and theft-all put together. Kenyan banks have not been spared as theft in banks has shifted from robbery and burglary to the technology related fraud. Such

fraud is perpetrated by employees within the bank, outsiders or even both employees and outsiders in collusion.

Wanjiru, (2012) studied the strategic responses to increasing fraud related risks while Wanemba, (2010) tried to establish the challenges of fraud faced by commercial banks in Kenya and to identify the strategies that commercial banks use to combat fraud. Sitienei, (2012) carried out a study to determine the factors influencing credit card fraud in the banking sector. No study has been done on the effect ICT utilization on fraud losses. This research sought to answer the question; what is the relationship between ICT utilization and fraud losses in commercial banks in Kenya?

1.3 Objective of the Study

The objective of the research was to examine the relationship between ICT utilization and fraud losses in commercial banks in Kenya.

1.4 Significance of the Study

The study will open up and increase the knowledge in the area of bank fraud. It is an important topic especially in Kenya because it will help the banking sector to realize that the technological advancement in the country calls for advancement in fraud control and detection skills especially in banks that can be said to highly computerized. Such technology has increased fraud in banks hence the need to invest more in detecting and deterring it instead of trying to suppress the number of fraud and theft-related cases that they file at the High Court.

Other commercial organizations can rely on the results to identify how they can enhance their control environment. Since ICT cuts across the whole economy, other organization will understand that as ICT advances, there is need to focus on fraud prevention, detection and control in order to reap the positive benefits of ICT.

Researchers and scholars can use the findings from this study as a basis for future research on the fraud and ICT challenges.

The government can rely on the findings of this study to formulate the relevant laws relating to fraud. It can also set up the legislation relating to adoption and implementation of ICT.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents a review of literature related to ICT and fraud.

2.2 Review of Theories

Three theories have been reviewed to help understand both ICT and fraud .These theories are the theory of the fraud triangle, the fraud scale theory and the theory of reasoned actions.

2.2.1The theory of the fraud triangle

Donald Cressey developed the theory of the fraud triangle. One leg of the triangle represents a perceived non-shareable financial need which can be a source of pressure. The second leg is for the perceived opportunity, and the final is for rationalization (Cressey, 1973).He concluded that individuals commit fraud when three factors are present: (1) a financial need that cannot be shared, (2) a perceived opportunity for illicit gains, and (3) a personal rationalization of the act. Perceived pressure relates to the motivation that leads to unethical behaviors. Every fraud perpetrator faces some type of pressure to commit unethical behavior. Albrecht, Howe, and Romney, (2006) pointed out that the word perceived is important due to the fact that pressure does not have to be real; if the perpetrators believe they are being pressured, this belief can lead to fraud. Perceived pressure can result from various circumstances, but it often involves a non-sharable financial need. Financial pressure has a major impact on an employeeôs motivation and is considered the most common type of pressure. Specifically, about 95% of all cases of fraud have been influenced by financial pressure (Albrecht et al., 2006). Motivations are so natural to human beings that no special forces are necessary to explain law-breaking (Jensen, 2003).

Opportunity is created by weaknesses in the systems that allow an individual to commit fraud; in the accounting field, this is called weak internal control. The concept of perceived opportunity suggests that people will take advantage of circumstances available to them (Kelly & Hartley, 2010). Perceived opportunity is similar to perceived pressure in that the opportunity does not have to be real; the perpetrator must simply believe or perceive that the opportunity exists. In

most cases, the lower the risk of getting caught, the more likely it is that fraud will take place. Other factors related to perceived opportunity can also contribute to fraud, such as the assumption that the employer is unaware, the assumption that employees are not checked regularly for violating company policies, the belief that no one will care, and the belief that no one will consider the behavior to be a serious offense (Sauser, 2007).

Rationalization refers to the justification that the unethical behavior is something other than criminal activity. If an individual cannot justify unethical actions, it is unlikely that he or she will engage in fraud. Some examples of rationalizations of fraudulent behavior include ñI am only borrowing,ò ñthe organization can afford it,ò and ñit is not really a serious matter.ò It is important to note that rationalization is difficult to observe, as it is impossible to read the perpetratorôs mind. Bank employees have knowledge of the systems as well as classified and confidential information which together with technological advancement can give them the opportunity to commit frauds. All they need is some pressure and the rationalization and that way they become part of fraud cartels that are fleecing millions of shillings from the banks (Jensen, 2003).

2.2.2 The Fraud Scale Theory

The fraud scale theory was developed by Albrecht, Howe, and Romney, (1984) as an alternative to the fraud triangle theory. The fraud scale is very similar to the fraud triangle; however, the fraud scale uses an element called personal integrity instead of rationalization. This personal integrity element is associated with each individualôs personal code of ethical behavior. Albrecht et al., (1984) also argued that, unlike rationalization in the fraud triangle theory, personal integrity can be observed in both an individualôs decisions and the decision-making process, which can help in assessing integrity and determining the likelihood that an individual will commit fraud. This argument is consistent with other research. Experts agree that fraud and other unethical behaviors often occur due to an individualôs lack of personal integrity or other moral reasoning (Dorminey et al., 2010; Rae & Subramaniam, 2008), as moral and ethical norms play essential roles in an individualôs decisions and judgment.

2.2.3 Theory of Reasoned Actions (TRA)

This theory originates from social psychology and was developed by Ajzen and Fishbein in 1975. They developed TRA to define the links between the beliefs, attitudes, norms, intentions,

and behaviors of individuals in their intention to use ICT. The theory assumes that a personôs behavior is determined by the personôs behavioral intention to perform it, and the intention itself is determined by the personôs attitudes and his or her subjective norms towards the behavior. The subjective norm refers to ñthe personôs perception that most people who are important to him think he should or should not perform the behavior in questionò Fishbein and Ajzen, (1980). In TRA rational considerations determine the choices and behaviors of individuals, and individual intentions determine behavior. Intentions refer to individualsô plans and motivations to commit a specific act. Intentions also reflect individual attitudes and the extent to which individuals perceive a specific act as desirable or favorable. The theory suggests that human behavior is governed by personal attitudes, but also by social pressures and a sense of control.

2.3 Review of Empirical Studies

Irungu, (2012) carried out a research to ascertain the influence of ICT on the performance of the aviation industry in Kenya with the case of Kenya Airways ï Kenya office. The objectives of the research was to study the influence of communication networks on the performance of an airline, to establish the influence of mobile phone technology on the performance of an airline, to investigate the influence of handheld devices on the performance of an airline and to study the influence of Internet applications on the performance of an airline. The findings showed that ICT which includes communication networks, mobile phone technology, handheld devices and Internet and computer applications influence the performance of the aviation to a large extent by assisting to improve on faster passenger handling and increased revenue generated from improved access to information. The recommendations were that the company should align itself to using ICT at a strategic level and to these strategies are cascaded to all levels of the hierarchy.

Nyokabi, (2012) carried out a study aimed at examining the role of information technology in empowering the local community through project implementation on the case of projects funded by Musoni Kenya Limited. The study sought to analyze the progress and achievement by the local community, their constraints, recommendations and possible solutions to improve their weaknesses. The researcher concluded that efficiency and quality service is enhanced through improved service delivery by use of ICT in project implementation within local community. The study also found that the mobile money transfer has enhanced communication within the Rural

Area. The ICT technology used by Musoni Kenya Ltd has facilitated faster access of Information and greatly impacted on group communication. The researcher also noted that security was improved and fraud was reduced through use of ICT.

Sitienei, (2012) carried out a study to determine the factors influencing credit card fraud in the banking sector. The study established that the factors that were considered important in influencing credit card fraud in the banking sector included credit card skimming, technology, system security, proper card management and systems integration. The study found out that in terms of factors that influence credit card fraud all the five factors were found to be significant and contribute to the credit card frauds. The study recommended that all banks adopt smart credit cards as their main mode of operation; smart credit cards operate in the same way as their magnetic counterparts, the only difference being that an electronic chip is embedded in the card which can be loaded with customer's biometric details.

Wanjiru, (2011) did a case study at Equity Bank of Kenya Limited with the aim of getting detailed information regarding the strategic responses to increasing fraud related risks. The study concluded that fraud is very sensitive and that customers have immense fear of fraud and it impacts negatively on banks profitability where income lost through fraud would have been reinvested to foster growth. The study also concluded that the worst fraud risk is identity theft where identification documents are easy to reproduce, fraudsters make parallel passports, IDs and driving licenses then use them to takeover accounts. The study further concluded that cheque fraud is a common type of fraud mainly because customers with cheque books are not careful in ensuring that their books are kept in safe custody. The Bankôs IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The study also revealed that a whistle blowing facility is existent in the Bank. The researcher recommended that there should be reforms in the police. This could help reduce the fraud related risks in the bank. The study also recommended that review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti-fraud laws. The study also recommended that review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank.

Wanemba, (2010) carried out a study with an objective to establish the challenges of fraud faced by commercial banks in Kenya and to identify the strategies that commercial banks in Kenya use to combat fraud. The study concluded that itôs necessary for a bank to have an anti-fraud unit that employs various strategies to curb fraud. The researcher suggested that banks should invest in advancing their technology in order to prevent fraud. The KYC (Know Your Customer) strategies are also equally important, and if applied together with regular auditing, will be able to curb cases of fraud. The internal controls within the banks should also be looked at keenly to ensure that they are in line with fraud prevention.

Beck et al, (2007) assessed the bright and dark sides of financial innovation. They used regression analysis to analyze bank, industry and country level data for 32 mostly high income countries between 1996 and 2006.They concluded that financial innovation is associated with higher growth volatility among industries more dependent on external financial innovation and with higher idiosyncratic bank fragility and higher bank losses.

Kariuki, (2005) carried out a study that showed that there were positive impacts of ICT on the banking performance. The study used bank turnover and profits as measure of performance. He established that banks with high profit growth are more likely to be using greater numbers of advanced ICTs. He concluded that e-banking leads to higher profits though in long-term but not in short-term due to high ICT investment cost.

Batavia, (1999) conducted an analysis of financial performance of Kenyan commercial banks and found out that risk management is central to any commercial bankós ability to register consistent profits and higher shareholders órreturns.

Tufano, (1989) did a research on financial innovation and first mover advantages. The objective of the study was to determine whether financial products innovators enjoy first mover advantages. The researcher concluded that the innovators that created new financial products did not charge higher prices in the period before imitative products appear and in the long run charged lower than rivals hence leading to losses. The researcher underscored the need for a robust risk management framework for all functions of the organization including marketing and promotion.

2.4 Information and Communication Technology

Commonly used information and communication technologies include management information systems (MIS), automated teller machines (ATMs), mobile phones, and smart cards (Ssewanyana, 2008). MIS is important to banks as it is the back office and backbone of any ICT innovation for banking services. It can effectively support loan portfolio, transactions, operational growth, decision making, transparent and quality services to the client, time management, and increased outreach (Turaga, 2004).

ICT offers various benefits to clients and banks in various countries. The benefits to clients have been identified as access to banking services, more convenient services, and faster loan processing and less time in queues. Benefits to the banks are reduced transaction costs, less fraud, improved quality of financial information, increased outreach, reduction in operational costs, and increase in customer satisfaction and loyalty (Hishigsuren, 2006).

ICT has been used to create branchless banks through mobile banking, automated teller machines (ATM), and point-of-sale networks among others where clients can access various financial services. Rogers, (2007) examined the role of ICT and in particular mobile phones in the delivery of financial services.

Mavungo, (2012) evaluated the ICT strategy adopted by Standard Chartered Bank Kenya Limited on the bankôs performance. He concluded that effective exploitation of technology is essential for the bank to increase their efficiency and effectiveness levels and reform agenda and all the firms should be incorporating and taking advantage of the technology to increase their growth through the adoption of the technologies.

Rogony, (2012) carried out a study with the objective of assessing the effect of adoption of real-time gross settlement system on interbank settlement efficiency in the Kenyan banking industry. The study concluded that the adoption of real-time gross settlement system has improved the efficiency of interbank settlement in the Kenyan banking industry. The real-time gross settlement system has led to increased volumes of processed payments, while decreasing the volumes of Cheques and EFT through the Automated Clearing House. The study findings serve as stimuli to policy makers to understand the industry better and to acknowledge that embracing technology, particularly in the banking sector will bring benefit both in the micro and macro economy.

Agboola, (2001) studied the impact of computer automation on the banking services in Lagos. He discovered that Electronic Banking has tremendously improved the services of some banks to their customers in Lagos.

2.5 Fraud Detection

Concerns of fraud should not be just how to detect fraudulent activities but how to prevent them from taking place (Jesper, 2008). This aspect is more directed towards the internal control systems which banks set up in order to detect and prevent fraudulent behavior from occurring.

Fraud can be detected through internal audits, external audits and anonymous fraud hot lines. Internal and external audits would indicate control weaknesses e.g. a lack of segregation of duties and lack of oversight through continuous, automated monitoring of journal entries. Leuchtner, (2011) suggests that bank fraud can be deterred and detected through having sufficient technology and security to safeguard the customersô information. Such technology can record internal user activity across the bank and replay it for later investigation. Others include restricting access to customer data to prevent identity theft and continuous monitoring of employee behavior and transactional activity to help uncover warning signs of internal fraud.

Ndiritu, (2010) researched on the use of technology to reduce international fraud in the banking industry with reference to the case of Kenya's banking industry and use of chip and pin technology for the period 2004-2009.The objectives of the study was to examine the use of chip and PIN technology in the banking sector by establishing the nature and extent of card fraud, accessing the impacts of the technology on fraud and the level of awareness in the banking industry and among the policy makers. The findings of the study were that chip and PlN technology has helped to reduce card fraud in countries that have adopted the technology, however very few commercial banks in Kenya have adopted the technology. The banks sighted the high investment cost as a setback despite the numerous counterfeit cards being used on their payment systems that result to losses from chargeback's received from issuing banks. The study concluded that there is need to Create more awareness on the benefits of technology in minimizing fraud losses in the industry as the fraudsters are now targeting countries such as Kenya that are still using the magnetic stripe technology. In addition, the optic fibre cables that have landed in Kenya recently have exposed the country to international hackers who are highly

sophisticated in using sensitive information from firms. A complete overhaul of the systems currently in use is encouraged if banks are to avoid potential losses.

Appelbaum and Shapiro, (2006) felt that top management plays a major role in fraud control. They concluded that the concept that is stressed by those in positions of authority will determine how workers react to situations that have ethical implications, thus the message of zero tolerance to fraud has to flow downwards from the top. Hollman, et al, (2003) suggested that every organization should have a manual that should clearly define behavior expectations, i.e., what activities are unacceptable, the internal controls in place to prevent fraud, and the punishment for those who do not comply. This ethics policy should become operative at the time of new hire orientation and continue until the employee separates. However various conditions may exist within an organization or business which can give an individual that feeling of opportunity. If an organization has a lack of policy to control various activities which could allow an individual to take part in fraud and espionage activity then the offender can become embolden to take part in a criminal action because of the lack of a formal written policy as a means of authority for enforcement (ACFE, 2008). Policies should be viewed as a social fabric which provides guidelines to hold the organization together.

According to the Journal of Economic Crime Management, 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 is prevention which involves actions and activities to prevent fraud from occurring. In detection, which is 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, for example. The next stage analyses losses that occurred despite deterrence, detection, and prevention activities are identified and studied to determine the factors of the loss situation, using methods such as root cause analysis. The sixth stage of the Fraud Management Lifecycle,

policy, is characterized by activities to create, evaluate, communicate, and assist in the deployment of policies to reduce the incidence of fraud. Balancing prudent fraud reduction policies with resource constraints and effective management of legitimate customer activity is also part of this stage. The seventh stage, involves obtaining enough evidence and information to stop fraudulent activity, recover assets or obtain restitution, and to provide evidence and support for the successful prosecution and conviction of the fraudster(s). Covert electronic surveillance is a method used in this stage. The final stage of prosecution is the culmination of all the successes and failures in the Fraud Management Lifecycle. There are failures because the fraud was successful and successes because the fraud was detected, a suspect was identified, apprehended, and charges filed. The prosecution stage includes asset recovery, criminal restitution, and conviction with its attendant deterrent value. (Wilhelm, 2004)

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. He concluded that when fraud management professionals fail to balance the various stages of the Fraud Management Lifecycle successfully, and do not integrate new technologies into each of the Lifecycleôs stages, they expose the companies they represent to unnecessary fraud losses and/or excessive expenses, and create a negative externality effect on society.

A whistle blower line provides an avenue for early detection of fraud. It also acts as an avenue for a concerned employee to anonymously voice his or her concerns. The existence of a hotline may not be enough hence management should also consider conducting periodic evaluations to determine whether the whistleblower hotline is effective, including benchmarking analysis against competitors. Banks should consider the use of an experienced outside agency managing the whistleblower hotline to enhance the perception of confidentiality. The policy can simultaneously create an incentive program for associates who uncover misconduct. (Kelly, 2008)

2.6 Conclusion

The chapter has explored the various views on ICT and fraud risk management concepts. Apart from the attempts to define and describe the concepts, the scholars and practitioners contend that ICT is a business enabler as it improves efficiency by cutting down costs. The key elements of a

robust adoption of ICT as a business enabler is proper fraud risk management framework. Overall, the studies have exposed the strategies adopted by banks to combat fraud, the role played by ICT in improving efficiency in banks and the fraud management cycle. From the discussion above, it is clear that adoption of ICT can either impact positively or negatively on the profitability of commercial banks.

No known studies by the researcher have been carried out on ICT utilization and the challenge of fraud. To my best knowledge not much has been done in Kenya to establish the fraud challenges that can originate from ICT utilization. Therefore there is a gap in literature that the present study seeks to bridge. This study therefore examines the effect of ICT utilization on fraud losses in commercial banks in Kenya.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The chapter provides an outline for conducting the study. It identifies research design and data collection procedures. It also describes the technique for data analysis and methods for data presentation and checking for validity and reliability of the findings.

3.2 Research Design

A design is used to structure the research, to show how all of the major parts of the research project, the samples or groups, measures, treatments or programs, and methods of assignment, work together to try to address the central research question (Mugenda and Mugenda, 1999). The research design used is a descriptive survey. This is because a broad range of information regarding utilization of ICT and fraud in commercial banks in Kenya was required for this study. Surveys are flexible in the sense that a wider range of information can be collected and since they are standardized, they are relatively free from several types of errors. A survey provides the kind and nature of information that is useful for comparison and generalization across banks with different demographics. It is also good for making comparisons and also useful in describing the characteristics of a large population (Mugenda and Mugenda, 1999).

3.3 Population

According to Curvery et al., (2003) a population refers to an entire group of persons or elements that have at least one thing in common. A population is a group of individuals, objects or items from which samples are taken for measurement. The target population was made of the 43 commercial banks licensed by the Central Bank of Kenya as at 31st December 2012.These include 6 large commercial banks, 14 medium sized banks and 23 small banks.

3.4 Sample

A sample size is a number of individual selected from a population for a study in a way that they represent the larger group from which they were selected. It would then be possible to generalize the characteristics of the sample to the population. The study targeted the whole population of all the 43 banks. This is because the population is small hence may not need to be sampled.

3.5 Data Collection

Secondary data was used for this study. Data on fraud was collected from records at the Banking Fraud investigation Unit (BFIU). CBK reports were reviewed to collect data on amounts transacted through ATM, RTGS and EFT. Data on staff costs was extracted from audited financial statements of banks for the period 2008-2012.

3.6 Data Analysis

The collected data was analyzed using the Statistical Package for Social Sciences (SPSS) version 16. Regression analysis was used to quantify the relationship between the dependent variable and the independent variables. The technique assisted in coming up with estimated coefficients in the empirical equation that measure the change in the value of the dependent variable for each one-unit change in the independent variable, holding the other independent variables constant.

3.6.1 Empirical Model

Regression analysis was used to analyze effect of ICT utilization on bank fraud. The regression model was as follows;

$Y= a + b_1X_1 + b_2 X_2 + b_3X_3 + b_4X_4 + \text{y}$

In order to measure the dependent variable (Y) the researcher used the annual amount lost through fraud in commercial banks .The researcher sought to establish the relationship between the total fraud (dependent variable) and the total value transacted through ICT related payment systems (ATM, RTGS and EFT) and Staff costs being the independent variables. Staff costs were used as a control for financial pressures faced by bank employees.

The components and measurements of the variables were as follows:

Y= amount lost through fraud

a = constant (The fraud Factor that exists without any adoption of ICT related transactions)

b_1.... b_4 are co-efficient of the independent variables (X_1.....X_4) respectively.

X_1 = Total Value Transacted through ATM per month as per CBK reports

X_2=Total Value Transacted through RTGS per month as per CBK reports

X_3= Total Value Transacted through EFT per month as per CBK reports

$X_{4=}$ Staff costs (Annual wages and salaries as reported in audited statement of comprehensive income)

ε = the error term, it represents the noise effect of all variables excluded from the regression model plus the effect of measurement error in the variables included in the model.

Mean scores were appropriately used to establish how ICT utilization affects fraud in commercial banks in Kenya as was indicated by scores put against each descriptive statement. The findings of the study were presented in tabular form for ease of interpretation and reporting. SPSS output of multiple regressions was used to establish existing relationship between the dependent and independent variables. The ANOVA tables were also established to indicate the level of fitness and validity of the model with the existing set of independent variables. The correlation coefficients were used to measure the degree to which the variables are related ranging from 0 to +1 if positively correlated and 0 to -1 if negatively correlated.

CHAPTER FOUR

DATA ANALYSIS RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents analysis and findings of the study as set out in the research methodology. The study findings are presented as an evaluation of the relationship between ICT utilization and fraud losses in commercial banks in Kenya. The data was gathered exclusively from reports at CBK and BFIU and the audited financial statements being the source of secondary data in line with the objectives of the study.

4.2 Data analysis

The data was analyzed for all the 43 registered commercial banks. In the analysis, staff costs for some banks were excluded as they were not in operation for all the five years. These banks include Jamii Bora bank, First community bank, Gulf African bank, K-Rep bank and Eco bank. The data was analyzed using the statistical package for social sciences-version16.

4.2.1 Checking the regression assumption of normality of the error term

The error term conformed to the regression assumption of normality as shown by the histogram in figure 1 below. The shape of the histogram follows the shape of the normal curve.

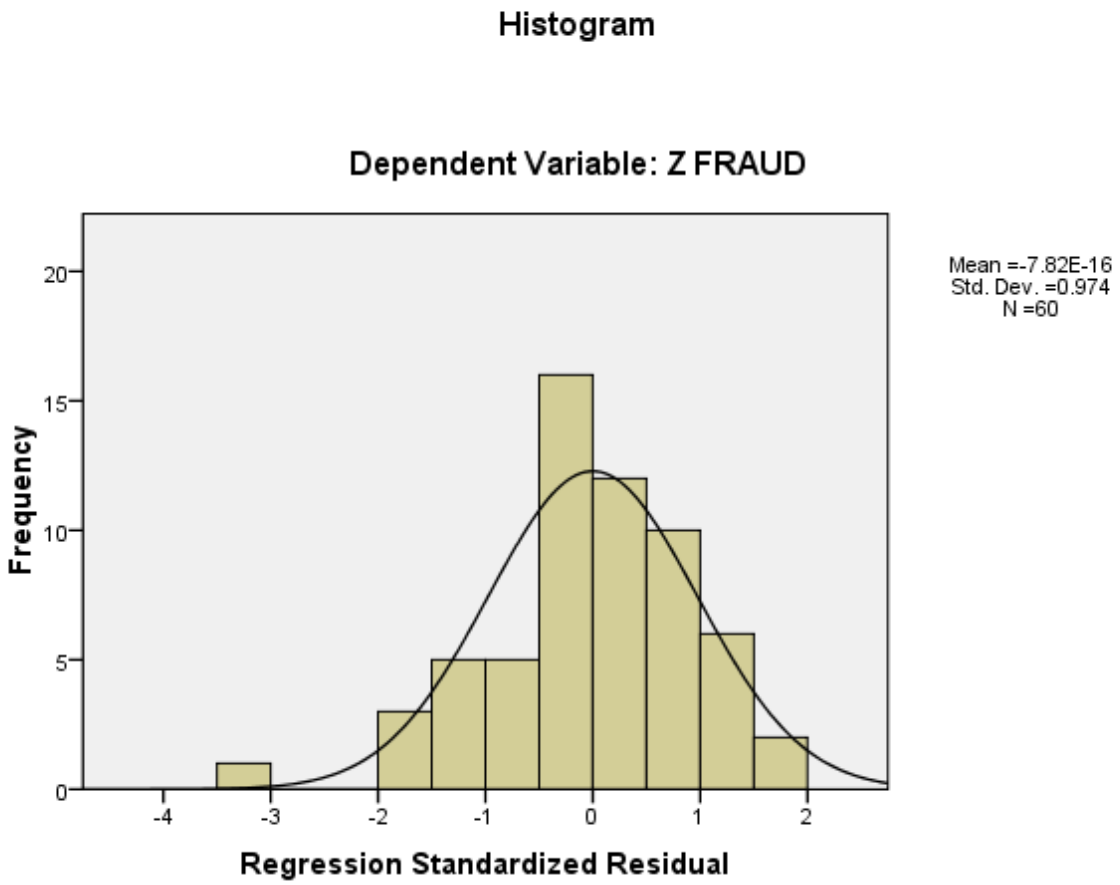

Figure 1: Histogram of the error term (Source: Analysis of research data-2013)

4.2.2 Checking Multi-collinearity

Normal regression results indicated multi-co linearity problem where independent variables i.e RTGS, ATM and EFT values were highly correlated. This was indicated by several Eigen value close to zero meaning that the predictors are highly correlated and that a small change in the data values may lead to large changes in estimated coefficients. This problem was also revealed through co linearity diagnostics by high condition indices of beyond the 15 mark considered benchmark. To fix the multi-co linearity problem, the regression was re-run using standardized values and the step-wise method of model selection. The table below shows that RTGS valueswas excluded in the overall model due to multi collinearity.

4.2.3 Variables excluded in the model due to multi-collinearity

Since the stepwise regression excluded RTGS values in the model due to multi-collinearity as shown in table 1 below, the beta coefficient for RTGS is not necessary here as a predictor of fraud losses. This means that the variables that will be in the model to predict fraud costs are ATM values, EFT values and Staff costs.

Table 1; Excluded Variables

Model		Beta In	t	Sig.	Partial Correlation	Collinearity Statistics		
						Tolerance	VIF	Minimum Tolerance
1	RTGS	.161a	3.596	.001	.430	.977	1.023	.977
	EFT	-.061a	-1.026	.309	-.135	.663	1.508	.663
	ATM	.402a	7.972	.000	.726	.448	2.234	.448
2	RTGS	.041b	1.064	.292	.141	.757	1.322	.347
	EFT	.153b	3.437	.001	.417	.482	2.075	.325
3	RTGS	.053c	1.500	.139	.198	.750	1.333	.278

4.3 Descriptive statistics

Table 1: Descriptive Statistics

This table analyzes the descriptive statistics which included the mean, standard deviation, minimum, median and maximum value for fraud losses, staff wages, EFT values, RTGs values and ATM values. The statistics were computed for 60 monthly observations.

Descriptive Statistics					
	FRAUD LOSSES	**STAFF COSTS**	**EFT VALUES**	**RTGS VALUES**	**ATM VALUES**
N	60	60	60	60	60
Mean	90.91583333	4334.145865	262300	1501146	9595.09023
Median	89.41666667	3983.768497	213000	1456240	9673.5
Mode	68.49583333	3453.131436	214000	107235	7439
Std. Deviation	18.6944243	743.3516288	95498.21189	383805.9	2778.49922
Range	55.67083333	2115.55851	276000	2510105	9745.35538
Minimum	68.49583333	3453.131436	152000	107235	5276.64462
Maximum	124.1666667	5568.689946	428000	2617340	15022
Sum	5454.95	260048.7519	15738000	90068746	575705.414

Source: Analysis of research data-2013

The difference in fraud losses in terms of highest and lowest fraud figures was ksh55.67 million. This indicates that fraud is not uniform monthly. The mean fraud losses were shs 90.9 million. The deviation from the mean monthly fraud losses was ksh 18.69 million. The minimum and maximum fraud losses were ksh68.49 million and ksh124.17 million respectively. The mean EFT, RTGS and ATM values were shs 4,334 million, shs 262,300 million, shs 1,501,146 million and 9,595 million respectively for the study period. The minimum and maximum ATM values were ksh 5276.64 million and ksh15,022 million respectively. The difference in these monthly values was ksh 9745.35 million. The difference in values transacted could be attributed to the fact that more bank customers were more comfortable with the use of ATMs as technology advances.

4.4 The Analysis of variance

In general, from table below which shows the regression results corrected for multi- collinearity indicates that about 94.6% of the variation in fraud losses can be accounted for by the model (adjusted R^2 of 0.944). The ANOVA table also shows regression sum of squares of 56.78597906 out of total variation of 60 also pointing to the fact that about 94.6% variation in bank fraud is explained by the model. In addition, the significance value of the F-statistic is less than 0.05 which means that the variation in the dependent variable explained by the model is not by chance.

The **analysis of variance**

Model		**Sum of squares**	**F**	**Significance**
	Regression	56.78597906	28.615**	0.000
	Residual	3.214	329.806	0.0000
	Total	60		
Adjusted R square	0.944			

4.5 Regression Coefficients

In order to determine the relationship between the fraud losses and the four independent variables at the commercial banks, the researcher conducted a multiple regression analysis. As per the SPSS generated table 4., the equation ($Y= a + b_1X_1 + b_2 X_2 + b_3X_3+ b_4X_4+ \varepsilon$) becomes:
$Y= 0.00000000000000022 + 0.499 X_1 + 0.153X_3+ 0.647X_4$: Where Y is the dependent variable (fraud losses), X_1 is Total Value Transacted through ATM per month as per CBK reports,
X_2 is the Total Value Transacted through RTGS per month as per CBK reports, X_3 is the Total Value Transacted through EFT per month as per CBK reports and X_4 is the annual staff costs as reported in audited financial statements.

Table 4; Regression coefficients

Coefficients					
Model		**Unstandardized Coefficients**	**Standardized Coefficients**	**t**	**Sig.**
	(Constant)	-0.00000000000000022		-0.000000000000071	1
	WAGES	0.646659124	0.646659	13.91421	0.000
	RTGS	_	_	_	_
	ATM	0.49931875	0.499319	9.210045	0.000
	EFT	0.153114573	0.153115	3.437177	0.001115

Source: Analysis of research data-2013

4.6. Summary and interpretation of findings

The stepwise algorithm chose, value transacted through ATM, EFT and staff wages as the predictors of fraud losses in banks as shown in table 4 below. As per the regression equation established, if all ICT utilization factors were taken to be constant at zero, fraud losses at the commercial banks will be 0.00000000000000022 which is almost zero. The ɓ coefficient of staff costs is positive indicating that there exist a significant positive relation between staff costs and fraud losses. The data findings analyzed also shows that if all other independent variables are taken at zero, a unit increase in the Value Transacted through ATM will lead to 0.499 unit increase in the fraud losses at the commercial banks. Further, a unit increase in the Value Transacted through EFT will lead to 0.153 increases in the fraud losses at the commercial banks and a unit increase in the annual staff costs will lead to a 0.647 increase. The results of the test show that the coefficient estimates of all the independent variables are positive conveying the message that these three independent variables (ATM, EFT and staff costs) have positive effect on the fraud losses.

From the above analysis of the betas, it can also be inferred that the level staff costs, contributes a lot on the fraud losses at the commercial banks followed by ATM transactions and EFT transactions respectively. The level of staff wages contributes to fraud losses because of the fact

that employees who are not well motivated financially will most likely fall into traps of fraud originating within the banks or even through collusion with outsiders. EFT and ATM values contribute to fraud in that as more customers transact a lot of data is exposed to identity theft. This is due to the speed of processing and the fact that the transactions are online and real time.

From the analysis the significance value of staff wages, ATM and EFT as a predictors are less than the p-value of 0.05 indicating that these variables are statistically significant in predicting fraud losses.

These findings support the theory of the fraud triangle which concluded that individuals commit fraud when three factors are present: (1) a financial need that cannot be shared, (2) a perceived opportunity for illicit gains, and (3) a personal rationalization of the act. Adoption of ICT by banks may have increased the opportunity to commit fraud. These findings are also consistent with those in studies by (Wanjiru, (2011) who did a case study at Equity Bank of Kenya Limited with the aim of getting detailed information regarding the strategic responses to increasing fraud related risks. The Bankôs IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The study also revealed that a whistle blowing facility is existent in the Bank.

The findings of this study also support findings by Wanemba, (2010) who carried out a study with an objective to establish the challenges of fraud faced by commercial banks in Kenya and to identify the strategies that commercial banks in Kenya use to combat fraud. The study concluded that itôs necessary for a bank to have an anti-fraud unit that employs various strategies to curb fraud. The researcher suggested that banks should invest in advancing their technology in order to prevent fraud. The KYC (Know Your Customer) strategies are also equally important, and if applied together with regular auditing, will be able to curb cases of fraud. The internal controls within the banks should also be looked at keenly to ensure that they are in line with fraud prevention. The findings in this study also agree with Agboola, (2001) who studied the impact of computer automation on the banking services in Lagos. He discovered that Electronic Banking has tremendously improved the services of some banks to their customers in Lagos. He also concluded that ICT improved bank efficiency but at the same time exposed banks to fraud.

The significance value of staff costs as a predictor is less than the p-value of 0.05 indicating that the variable is significant in predicting firm value. This supports the fraud scale theory developed by Albrecht, Howe, and Romney, (1984).They stressed on an element called personal integrity instead of rationalization. This personal integrity element is associated with each individualôs personal code of ethical behavior. The findings are also consisted with the study by Appelbaum and Shapiro, (2006) who felt that top management plays a major role in fraud control. They concluded that the concept that is stressed by those in positions of authority will determine how workers react to situations that have ethical implications, thus the message of zero tolerance to fraud has to flow downwards from the top.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

The objective of this study was to determine the relationship between ICT utilization and fraud losses in commercial banks in Kenya. The period under study was 2008 -2012. ICT utilization in this case was represented by the monthly values transacted through EFT, RTGS and ATM. The control factor of staff costs was used to represent motivations for fraud.

Secondary data was used for this study and was collected from CBK reports, BFIU reports and audited financial statements for all the 43 registered commercial banks in Kenya. SPSS version 16 was used to analyze data. Data was analysed through regression analysis and represented in tables.

The findings established that the commercial banks in Kenya incurred average fraud costs of kshs. 90.9 million between the years 2008 and 2012. The average values transacted through ATM, RTGS and EFT were shs 9595.09 million, khs 1,501,146 million, khs 262,300 million while the average staff costs were shs 4,334.15million, respectively within the same period. The levels of ICT utilization generally increased .EFT values increased from 214 billion in 2008 to416 billion in 2012.Fraud costs increased rapidly from 64 million monthly in 2008 to 417 million in 2012.

The regression analysis indicated that all the ICT utilization elements(Values transacted trough EFT and ATM) together with staff costs had a positive correlation with fraud losses. The coefficient of determination (R^2) indicated that the four independent variables that were studied, explained 94.6% of the relationship between ICT utilization and fraud costs of commercial banks. The ANOVA model Fóstatistic (329.8) suggested that the model was fit and valid with the existing set of independent variables.

5.2 Conclusions

From the above findings the researcher concluded that in the period between 2008-2012; commercial banks recorded great increases in both ICT utilization and fraud costs. The minimum and maximum fraud losses were ksh68.49 million and ksh124.17 million respectively. The mean EFT, RTGS and ATM values were shs 4,334 million, shs 262,300 million, shs 1,501,146 million and 9,595 million respectively for the study period. The minimum and maximum ATM values were ksh 5276.64 million and ksh15,022 million respectively. The difference in these monthly values was ksh 9745.35 million. The difference in values transacted could be attributed to the fact that more bank customers were more comfortable with the use of ATMs as technology advances.

The coefficient of determination (R2) at 94.6 % and Fó statistic at 329.8 indicated that the model was fit and valid with the existing set of independent variables. This therefore signified that ICT utilization was the main determinant of the fraud losses at commercial banks.

5.3 Limitations of the study

The study relied on secondary data collected from audited financial statements and reports at the CBK and BFIU. A limitation of this is the accuracy and reliability of the financial statements of the commercial banks. The figure of staff coats in such statements may have been inaccurate.

The integrity of the findings is affected by the fact that banks do not report all fraud to BFU. Some banks choose not to report fraud to BFIU but instead deal with such cases internally to avoid reputational risk.

Some banks were not in operation during the entire period of study. Examples include Jamii bora Bank which was licensed in 2010.

EFT, RTGS and ATM values may not have taken into account diaspora remissions which are also subject to fraud.

5.4 Recommendations

The researcher recommends more robust fraud mitigation practices and policies to ensure that all elements of fraud are captured in the adoption of ICT. Part of the investment in ICT should include fraud detection and control. Before an ICT system is adopted, it should be thoroughly tested for possibility of both internal and external fraud. In addition to this, there should be continuous monitoring of bank systems to ensure that fraud is detected and controlled at the earliest possible time.

Banks should also consider increasing their staff costs to mitigate frauds. Bank employees have access to all information relating to customer accounts hence should be well rewarded and motivated in order to prevent them from falling into traps of fraud. All bank employees should be vetted before employment and during employment. Vetting before employment will ensure that only those with high moral standards are taken in for employment. This may include background checks and recommendations from previous employers. Vetting during employment would include looking out for changes in the employeesô lifestyle that cannot be explained by their income. Management could also introduce hot lines for reporting fraud. This can be open to both bank employees and outsiders. Such a hot line can help banks in cutting down fraud costs as they can be able to control fraud once it is reported.

5.5 Suggestion for further study

The researcher suggests a similar study be conducted through a survey of the MFIs. This will allow for a comparison of the findings to come up with recommendations that be applicable to all the players in the lending business in Kenya.

Further studies could also include internal controls employed by banks and research on effect of ICT utilization on internal controls in banks.

A similar study could also be done on the relationship between ICT utilization and fraud losses in medical insurance companies.

Studies could also be conducted on the relationship of each ICT utilization factor on fraud losses in banks.

REFERENCES

Agboola, A. A. (2001). Impact of Electronic Banking on Customer Services in Lagos, Nigeria. *Ife Journal of Economics and Finance*, 5(1&2)

Ajzen, I. & Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior Englewood Cliffs, NJ: Prentice-Hall, Inc.

Albrecht, W., Howe, K. & Romney, M. (1984). *Deterring fraud: The internal auditor's perspective.:* The Institute of Internal Auditors Research Foundation. Altamonte Springs, FL

Albrecht, W. S., Hill, N. C. & Albrecht, C. C. (2006). The ethics development model applied to declining ethics in accounting. *Australian Accounting Review*, 16(1), 30-40.

Apoorva, Y. & Juhi, M. (2007). *Bank fraud in India*. National Law Institute University, Bhopal India.

Appelbaum, S. & Shapiro, B. (2006). Diagnosis and Remedies for Deviant Workplace Behaviors. *Journal of American Academy of Business*, *Cambridge*; 14-15

Cressey, R.D. (1973). *Other people's money: A study in the social psychology of embezzlement.* Montclair, NJ Peterson smith.

Glassner, T. & Mas, I. (1995). Incentives and the Resolution of Bank Distress. *The world research observer,* 10(1), 86-103

Hishigsuren, G. (2006). *Information and Communication Technology and Microfinance: Options for Mongolia.* ADB Institute Discussion Paper 42. Retrieved from http://www.adbi.org/files/2006.02.dp42.ict.microfinance.mongolia.pdf

Jensen, G. F. (2003). Social Control Theories. *Encyclopedia of Criminology*. Richard A. Wright, Fitzroy Dearborn Publishers.

Jesper F. (2008) *.occupational fraud –auditors' perceptions of red flags and internal control* Linkopingçs University, Linkoping, Sweden

Kenny, C. and Keremane, R. (2007). Toward universal telephone access: market progress and progress beyond the market. *Telecommunications Policy*, 31, 155-163

.

Kimani W. (2013). EAC Banks grapple with fraud cases. *Daily Nation*, *Smart Company* 2-3

Leuchtner, T. (2011). Four internal frauds and how to spot them. *ABA Banking Journal*, Retrieved from http://www.ababj.com/

Mugenda, O. M. and Mugenda, A. G. (1999). Research Methods: Quantitative and Qualitative Approaches. Nairobi: Acts Press.

Rogers, E.M. (2003). Diffusion of innovations (5th ed.)New York: Free Press.

Sauser, W. (2007). Employee theft: Who, how, why, and what can be done. *S.A.M. Advanced Management Journal*, 72(3), 13-25.

Ssewanyana, J.K. (2008). *The role of Free and Open Source Software in the microfinance sector in Uganda.* Conference Proceedings IST-Africa. Retrieved from http://www.IST-Africa.org/conference.

Tufano, P. (1989). Financial Innovation and First Mover Advantages. *Journal of Financial Economics,* (25), 213-240.

Turaga, J. (2004). Opportunities and challenges in India ñKuch Apru Sock aur Kuch Jugaadò: Crafting the MFI/IT Paradigm. *The Indian Experience.* Retrieved from http://www.I4donline.net/issue/jan04/opportunities-full.htm

Wells T. J. (2003) Corporate Fraud Handbook, *Introduction: Research In Occupational Fraud and Abuse*, 5-24

Wilhelm W. K. (2004). The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management. *Journal of Economic Crime Management*, 2(2), 8-10

Woherem, E. W. (2000): Information Technology in the Nigerian Banking Industry, Spectrum, Ibadan.

APPENDIX 1

List of commercial banks

1.ABC Bank (Kenya)
2. Bank of Africa
3. Bank of Baroda
4. Bank of India
5.Barclays Bank
6. Brighton Kalekye Bank
7. CFC Stanbic Bank
8. Citibank
9. Commercial Bank of Africa
10. Consolidated Bank of Kenya
11. Cooperative Bank of Kenya
12. Credit Bank
13. Development Bank of Kenya
14. Diamond Trust Bank
15. Dubai Bank Kenya
16. Ecobank
17. Equatorial Commercial Bank
18. Equity Bank
19. Family Bank
20. Fidelity Commercial Bank Limited
21. Fina Bank
22. First Community Bank
23. Giro Commercial Bank
24. Guardian Bank
25. Gulf African Bank
26. Habib Bank
27. Habib Bank AG Zurich
28. I&M Bank
29. Imperial Bank Kenya
30. Jamii Bora Bank
31. Kenya Commercial Bank
32. K-Rep Bank
33. Middle East Bank Kenya
34. National Bank of Kenya
35. NIC Bank
36. Oriental Commercial Bank
37. Paramount Universal Bank
38. Prime Bank (Kenya)
39. Standard Chartered Kenya
40. Trans National Bank Kenya

41. United Bank for Africa
42. Victoria Commercial Bank
43. Chase Bank (Kenya)

APPENDIX 2

DATA ON ICT UTILIZATION

MONTH	RTGS	EFT	ATM	fraud costs
	shs"millions"	shs"billions	shs million	shs'millions'
Dec, 2012	1,627,431	214	15,022	417
Nov, 2012	1,819,579	217	13,540	186
Oct, 2012	1,899,675	234	13,712	61
Sep, 2012	1,738,832	202	13,081	187
Aug, 2012	1,637,004	214	13,375	23
Jul, 2012	1,560,938	223	12,500	0
Jun, 2012	1,693,432	203	12,273	67
May, 2012	1,610,126	227	13,256	99
Apr, 2012	1,528,600	201	12,413	102
Mar, 2012	1,638,150	215	13,099	93
Feb, 2012	1,546,480	203	12,085	66
Jan, 2012	1,579,320	202	12,536	218
Dec, 2011	1,562,080	210	14,063	345
Nov, 2011	1,816,270	214	12,373	132
Oct, 2011	2,004,110	199	12,384	47
Sep, 2011	1,729,950	217	12,124	87
Aug, 2011	2,007,040	207	12,333	51
Jul, 2011	2,151,280	196	9,982	43
Jun, 2011				12

	2,617,340	195	11,382	
May, 2011	1,867,910	210	11,278	105
Apr, 2011	1,727,570	172	11,339	27
Mar, 2011	1,801,550	212	11,901	59
Feb, 2011	1,288,840	184	10,464	89
Jan, 2011	1,319,870	179	11,202	106
Dec, 2010	1,400,960	206	12,367	186
Nov, 2010	1,430,130	195	10,432	91
Oct, 2010	1,375,620	184	10,403	132
Sep, 2010	1,256,470	193	9,866	96
Aug, 2010	1,280,470	176	10,243	112
Jul, 2010	1,425,810	179	9,871	13
Jun, 2010	1,500,990	159	9,481	88
May, 2010	1,587,240	174	9,435	43
Apr, 2010	1,436,310	171	9,150	135
Mar, 2010	1,694,230	194	9,414	79
Feb, 2010	1,458,480	162	8,246	0
Jan, 2010	1,254,020	152	8,719	98
Dec, 2009	1,454,000	187	8,832	127
Nov, 2009	1,429,960	165	7,792	94
Oct, 2009	1,480,730	166	7,636	85
Sep, 2009	1,198,240	413	7,586	81
Aug, 2009	1,127,100	375	7,682	0
Jul, 2009				127

	1,184,970	397	7,439	
Jun, 2009	1,031,560	414	7,439	78
May, 2009	1,064,250	371	7,290	12
Apr, 2009	107,235	413	7,144	74
Mar, 2009	1,234,920	409	7,002	83
Feb, 2009	1,236,480	351	6,861	93
Jan, 2009	1,375,950	357	6,724	113
Dec, 2008	1,293,360	428	6,590	167
Nov, 2008	1,225,150	349	6,458	85
Oct, 2008	1,343,930	406	6,329	119
Sep, 2008	1,367,430	404	6,202	86
Aug, 2008	1,327,200	348	6,078	77
Jul, 2008	1,863,959	416	5,957	49
Jun, 2008	2,600,813	419	5,838	88
May, 2008	1,895,025	392	5,721	37
Apr, 2008	1,219,919	427	5,606	89
Mar, 2008	890,747	323	5,494	95
Feb, 2008	985,324	338	5,384	132
Jan, 2008	1,256,387	375	5,277	64