ELECTRONIC FRAUD ANDPERFORMANCE OF RETAIL BANKING IN UGANDA: A CASE STUDY OF CENTENARY BANKLIMITED MAPEERA HOUSE

BY

MATOVU LUBEGA ABDU
2016/AUG/MBF/M220699/WKD

A DISSERTATION SUBMITTED TO THE SCHOOL OFBUSINESSADMINISTRATION

IN PARTIAL FULFILLMENT OF THEREQUIREMENTS FORTHE AWARD OF

THEMASTER OF SCIENCE IN BANKING AND FINANCE OF

NKUMBA UNIVERSITY, ENTEBBE UGANDA

OCTOBER 2018

DECLARATION

I, Matovu Lubega Abdu, hereby declare that this dissertation is an original work resulting from my own research efforts and has never been submitted to any other institutions for any award. Where ideas have been borrowed from other scholars, due acknowledgement has been made.

Signature: -------------------------------- **Date: -------------------------------------**

MATOVU LUBEGA ABDU

STUDENT

APPROVAL

This study titled “Electronic fraud and Retail Banking Performance in Retail banks in Uganda: A Case Study of Centenary Bank, Mapeera house Kampala” has been written under my supervision and has been submitted in partial fulfillment of the requirements for the award of the degree of a Master of science degree in Banking and Finance of Nkumba University, with my approval.

Signature --------------------------------------- Date ---------------------------------------

Mrs. Violet Asiimwe

Supervisor

ACKNOWLEDGEMENTS

I wish to extend my sincere heartfelt gratitude to all those who have been instrumental and points of emulation to make it possible for me to accomplish the great task of this study through the list cannot be exhausted, below are those whose contribution deserves special acknowledgment.

My first special thanks giving glory is contributed to Allah for all the provision, care, love and his sovereignty to me.

I acknowledge my Dad Hajji Bruhan Kizza, and Mum Mastula Kizza (Mrs), for all kinds of support, tolerance, courage, endurance and love extended to me through all the joyous and tough moments. May the almighty God bless or award you abundantly.

I am particularly grateful to my supervisor Madam Asiimwe Viola for her professional, academic and parental guidance given to me for accomplishment of this work.

I would like to acknowledge all the support from my friends especially those whom I met at Nkumba University specifically Victor, Andrew, Scholar A, and other friends may God bless you abundantly.

Lastly, I thank the staff of Centenary Bank Mapeera House – main branch for their support and for providing the necessary information that has led to the successful completion of this work.

Otherwise, without you parents, relatives and friends I would not have made it to this extent. I love you all my Allah keep blessing you now and always.

DEDICATION

I would like to dedicate this report to my beloved father, mother and my immediate family who **.**

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

LIST OF ABBREVIATIONS

ATM - Automated Teller Machines

CEO - Chief Executive Officer

CRDT - Centenary Rural Development Trust

DFCU – Development Finance Company of Uganda

EFT - Electronic Fund Transfer

PIN - Personal Identification Number

SME – Small and Medium Enterprises

SPSS - Statistical Package for Social Sciences

ABSTRACT

The purpose of the study was to investigate the influence of Electronic Fraud and Performance in Retail Banking in Uganda, a case of Centenary Bank Uganda Limited. The study was guided by the following specific objectives; The effect of ATM fraud on retail banking performance ;The effect of internet fraud on retail banking performance; and The effect of mobile fraud on retail banking performance at Centenary bank.

Using a phenomenological approach, a highly descriptive and explanatory research was carried out and responses were collected from 179 respondents with the help of self-administered questionnaires as well as face to face interviews. Data on the population sample was determined using Krejie and Morgan’s table characteristics and objectives was analyzed according to frequency tabulations and Pearson correlation matrix respectively and regression analysis was used to examine the predictive power of electronic fraud on retail banking performance.

From the findings: ATM fraud with R square = .384, internet fraud with R square = .320 and mobile fraud with Rsquare = .331 had positive significant relationships on retail banking performance showing that electronic fraud had a positive and significant effect on the retail banking performance of Centenary bank. Results from regression analysis showed ATM fraud, internet fraud and mobile fraud were strong predictors of retail banking performance with Adjusted R Square = .351). In conclusion Electronic fraud has a positive significant relationship with centenary bank

The study recommended that; the management of the bank should develop a very strong risk management team as well as security systems coupled with effective strategies inclined to retail banking performance enhancement. The strategies will help foster proper management and control of electronic fraud which will in turn enhance efficiency, growth in customer base and brand equity.

CHAPTER ONE

INTRODUCTION

Overview

This study examined ‘The Effect of electronic fraud on Retail Banking Performance Retail Banking using Centenary Bank as a case study. The independent variable of the study was electronic bank fraud whereas the dependent variable of the study was retail-banking performance. This introductory chapter presents the background to the study, the statement of the problem, and the purpose of the study. Also presented in this chapter are the objectives of the study, the research questions, scope and significance of the study.

1.1 Background to the study

Technological developments in the banking sector started in the 1950s with the installation of the First automated book keeping machine at banks. Automation in the banking sector became widespread over the next few decades as bankers quickly realized that much of the labor-intensive information handling processes could be automated with the use of computers (Musara and Fatoki, 2010). Electronic banking can be traced in the early 1970s. During this time, some banks had started looking for alternatives and supplements to the traditional banking functions (Mobarek, 2007).

The term electronic banking became popular in the early 1980s, by then, the term referred to the use computers to access banking services. In 1981, electronic banking was welcomed and offered by major banks in the New York City such as Citibank, Chase, Manhattan, Chemical and Manufactured Hanover. From the United States, electronic banking was welcomed in United Kingdom in 1983 (Shannak, 2013).

Full development of electronic banking came about in 1995 when a number of banks allowed bank accounts to be opened online. By the year 2000, 80% of the American banks offered electronic banking. A number of Ugandan commercial banks considered the role of electronic banking and its efficiency as an improvement in the banking sector. In 1997, electronic banking was introduced in Uganda when standard chartered bank introduced the use of ATM. In the same year, the Bank of Uganda introduced Electronic Fund Transfer (EFT) (Abaasa, 2007; Daily monitor, 16th, August, 2004). The history of electronic banking fraud is not well documented.

However, the rapid popularity and of electronic banking invited security threats (Keivani, Jouzbarkand, Khodadadi, &Sourkouhi, 2012).

Shannak (2013) defines Fraud as the deliberate deception to secure unfair or unlawful, or to deprive the victim their legal right to gain from their finances, classified as a civil wrong. McEwan (2000) defines Electronic fraud as one that is committed by means of electronic gadgets like computers, telephones and other electronically aided medium.

According to Hermanson (1990) and Cressey (2000), fraud has been associated with human organization from recorded history. Investigating and detecting fraud is not an easy task and requires thorough knowledge about the nature of fraud, how it can be committed and concealed. Forensic Accountants are increasingly being asked to play an important role in helping organizations investigate, prevent and detect fraud. Electronic banking fraud can be traced after the adaptation of electronic banking in the industry (European ATM Crime Report, 2007).

Similarly, Wisdom (2012)) revealed that the increase of electronic banking has led to increase of fraud resulting in financial loses. For example, it is estimated that in 2009 to 2010 there was 93% increase in electronic banking fraud and a 30% increase in 2012 to 2013. According to a study by retail banking researchers in 2011, electronic banking fraud costs US $8.6 billion annually. This was anticipated to increase in the next years. Banking industry includes a number of businesses such as corporate banking, investment banking, wealth management, capital market and others. Retail banking is another segment of the banking industry. Retail banking has been the new focus of the banking industry across the world. Retail banking offers services like account opening, credit card, debit card, ATM, internet banking, phone banking, insurance and stock broking and many others.

This study was guided by the Fraud Triangle model by Cressey (2000)which was later modified by the Fraud Diamond model by Hermanson (2004).Cressey, a criminologist researched about what drives people to commit fraud and he discovered three factors: "*Pressure/ Motive, Opportunity and Rationalization."*To add to that*,* Hermanson introduced the Fraud Diamond model in order to add to the three factors that cause fraud. The model adds a fourth variable *"capabilities"* to the three of the fraud triangle: motive / pressure", "Opportunity" and "Rationalization". The factors highlighted above are not exceptional to the reasons why one seemingly honest person would not hesitate to commit ATM, Internet and Mobile fraud respectively.

According to Roger's (1983), Electronic banking is the use of electronic and telecommunication networks to deliver a wide range of value added products and services to bank customers. Steven (2002) further says that, the use of information technology in banking operations is called electronic banking. Ovia, (2001) argued that Electronic banking is a product of e-commerce in the field of banking and financial services. Banks are also offering payment services on behalf of their customers who shop in different e-shops. It is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution, (FinCen, 2000).

According to Swaminathan and Ananth (2010), electronic banking is the automated delivery of new and traditional banking products and services directly to the customer through the electronic communications like computers, ATMs and internet websites. Daniel (1999) defines electronic banking as "distribution of information and services by banks to their customers through differently delivery platform that can be used with a personal computer, telephone or automated teller machine (ATM)." From the definitions given, internet banking, telephone banking and ATM banking are the most referred to aspects of electronic banking.

ATM is an electronic computerized telecommunication device that allows a financial institution's customers to directly use a secure method of communication to access their bank accounts.

E –banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution. The following are the Indicators of e banking when used by customers and commercial banks: personal computer (PC) Banking, Internet banking, virtual banking, online banking, home banking, remote electronic Banking and phone banking. Personal computer banking and Internet, mobile banking or online banking are the most frequently used designations. It focus strictly on consumer market providing a wide range of personal banking service, for example, savings, check account, bill payment services, ATM, mortgages and personal loans.

According to Ongkasuwan and Tantichattanon, (2002) internet banking allows customers to access and perform financial transactions on their bank accounts from web-enabled computer that have internet connections to the bank. Fraud is defined by the advanced learner's dictionary as an act of pretending aimed at deceiving in order to get money or good illegally. Therefore, electronic banking fraud is an act of compromising internet , ATM and telephone banking in order to illegally tap into their accounts illegally to steal their money or/and goods. For purposes of this study, electronic banking fraud will be operationalized as ATM bank fraud, internet bank fraud and mobile phone bank fraud.

Darlington (1999) defines retail banking as banking services that are geared primarily toward individual consumers. Retail banking generally refers to the provision of products and services that banks provide to personal customers and businesses, including SMEs, through a variety of channels including branches, internet and mobile technology. Banks typically organize their retail banking activities either by the type of customer served (such as, personal versus business), Products offered (such as mortgages, credit cards) or size (such as small versus large businesses). The main functions of retail banks (sometimes referred to as 'high street banks') include accepting deposits, making loans and providing payment services. Retail banking includes Production Code Administration (PCA) and Small and Medium Entrepreneur (SME) banking services, the reference products for our investigation, but also other products such as residential mortgages, personal loans and insurance. Many large UK retail banks have separate retail banking divisions or business units, with their own management and reporting structures, although there are differences in the way these banks define, organize and describe their retail activities.

2.3. Electronic Banking overview.

The term electronic banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive Communication channels (Buchanan, 2010). E-banking for this particular study includes the systems that enable financial transactions modes of payment used by customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Automated Teller Machines (ATMs) used alongside the Personal Identification Number (PIN) , Internet banking and Mobile Banking,(Jacob, 2009). There are five basic services associated with e-banking: view account balances and transaction histories; paying bills; transferring funds between accounts; requesting credit card advances; and ordering checks for more faster services that can be provided by domestic and foreign bank. E banking reaps benefits for both banks and its customers.

From the banks' perspective, e-banking has enabled banks to lower operational costs through the reduction of physical facilities and staffing resources required, reduced waiting times in branches

16 resulting in potential increase in sales performance and a larger global reach (Ihejiahi, 2009). From the customers' perspective, e banking allows customers to perform a wide range of banking transactions electronically via the bank's website anytime and anywhere. In addition, customers no longer are confined to the opening hours of banks, travel and waiting times are no longer necessary, and access of information regarding banking services are now easily available (Mudiri, 2014). Despite the barriers associated with E-banking and the internet, the advancements and benefits of E-banking to consumers as well as banking institutions are irreplaceable. From the consumer's perspective, E-banking has provided them with the ability to pay bills, manage accounts, and shop all from the convenience of their homes. This alternative has also reduced cost for the banking institutions that offer the service, an online transaction costs the bank much less than a face-to-face interaction with a bank's teller (Akindele, 2010).
In an attempt to remain on the cutting edge in the evolutionary world, banks and bank managers are challenged by the new technology and software systems used to make sure the finance world runs smoothly. Along with the benefits attached to the e- banking, the inherent security issues in terms of confidentiality, integrity and privacy have always been a challenging factor stalling the advancement of its progress (Hoffman &Birnbrich, 2012).

These security issues seem to be an open-ended list of issues, prominent among them are; confidentiality of information exchanged, authentication of the relevant instructions, integrity of the e-banking platform, etc. All these security issues, no doubt, are also related and sometimes complementarily overlapping. Secure transactions must possess integrity, meaning the transaction was not altered while being transmitted. Without integrity, there is no guarantee that the message your customer sent to the bank matches the message that the bank actually received (Idowu, 2009). Secure transactions must also possess confidentiality, that is, the content of messages remains private as they pass from the customer through the internet to your bank. Without confidentiality, anyone can view the transaction message and gain private information, inevitably leading to electronic bank fraud as discussed in the proceeding sections.

In context Centenary bank was founded in 1983 as a credit trust, Centenary Rural Development Trust (CRDT), by six individuals: (a) Simeon Lutaakome (b) Hugh Francis Pulle (RIP) (c) PaulKateregga (d) Vincent Kirabokya Maria (e) Emmanuel Mpande(RIP) and (f) John Ogutu

(RIP).The bank's vision is "To be the best provider of Financial Services, especially Microfinance in Uganda." And the mission statement is "To provide appropriate financial services especially microfinance to all people in Uganda, particularly in rural areas, in a sustainable manner and in accordance with the law." The values held by the bank are superior customer service, integrity, teamwork, professionalism, leadership, excellence, competence. In 1985, CRDT began to provide financial services to the public. Centenary Bank became a fully licensed commercial bank in 1993, after receiving a banking license from the Bank of Uganda, Uganda's central bank.

As of December 2011, Centenary Bank was the 6th largest commercial bank in Uganda, with an asset base estimated at US$381.3 million (UGX: 944 billion), representing approximately 7% of all bank assets in the country at that time. Centenary Bank is the second-largest indigenous Ugandan bank, behind Dfcu Bank. Centenary Bank has its headquarters in Kampala. As of August 2012, the bank has moved into its new headquarters building, Mapeera House, on Kampala Road opposite City Square. Centenary Bank has a network of 60 bank branches together with 115 linked automated teller machines in Central, Western, Northern and Eastern Uganda. The bank boasts of over 1,100,000 deposit customers. Centenary Bank has the second-largest branch network in Uganda, behind Stanbic Bank. The majority of the bank's branches are in rural areas and the bank plans to open more branches in future. As of October 2013, the branches of the bank include the following locations, arranged alphabetically.

Like any other growing bank, centenary has engaged in the setting up of new technologies to match the trends of time. Many businesses have embraced technology in their operations as they seek to improve efficiency and remain competitive in today's cutthroat business environment. However, there is growing fear among players in the banking industry about the risks that the advancement and adoption of new technology is posing to the industry. In February 2012, Mr Fabian Kasi, the Centenary Bank managing director, told Daily Monitor in an interview that fraud was emerging as a big challenge for the industry, costing the sector millions of shillings annually. It is estimated that about Seven (7) per cent of an average organization's annual revenue is lost to fraud while financial institutions and telecoms in Uganda lose between 15-20 per cent of annual revenue to fraudsters (Monitor, February 29, 2012, Faridah Kulabako).

1.2 Statement of the Problem

Electronic banking is intended to offer a wide range of advantages and opportunities in the banking sector to ensure that their work is carried out effectively and efficiently. Brücher, Scherngell et al. (2003) had an opinion that electronic banking adoption would improve three critical domains which are efficiency, quality, and transparency in any banking institution**.**

However, Wisdom (2012)) revealed that the increase of electronic banking has led to increase of fraud resulting in financial losses. For example, it is estimated that in 2009 to 2010 there was 93% increase in electronic banking fraud and a 30% increase in 2012 to 2013. According to a study by retail banking researchers in 2011, elelectronic-banking fraud costs US $8.6 billion annually. This was anticipated to increase in the next years. The Bank of Uganda Financial Stability Report (2015 - 2016) revealed that the total customer base of Centenary bank declined by 11.4%, customer deposit declined by 7%, total credit slowed down by 12% and customer complaint due to electronic fraud increased by 6.3%.

A 2012 survey by Deloitte indicated that Ugandan banks lose up to sh12b annually to electronic fraud while UGS118b was lost by banks in the East African region. In October 2015, Centenary Bank cancelled all Personal Identification Numbers (PINs) which implied that customers could not make any withdrawals over automated teller machines (ATM). Withdrawals were limited to UGS100,000. Some customers said they were only able to access shs50,000 before the ATM cards were cancelled, as a result many left the bank due to inconvenience.(15th October 2015, New Vision Samuel Sanya).

According to Centenary Bank Report (2015), In 2012 a group of Bulgarians was convicted of defrauding many ATM users. Centenary bank was one of the most affected banks and this led to the cancellation of ATMs card PINs aimed at calming down the general public. With even this and other measures, consumers continue to report complaints of electronic fraud at Centenary Bank (Summit Business Review, 2015). According to the Financial Crimes Report (2014), the fact that most of the time, these cases go unnoticed or remain unreported implies that the extent and effect of such crimes on retail bank performance remains un-quantified. Consequently, Centenary Bank incurs substantial operating costs by refunding customers' monetary losses, which greatly affects financial performance, while its clients experience considerable time, and emotional losses. If delete such electronic fraud causes are not managed by commercial banks, they may not only be distressed, but also will eventually collapse in future.

1.3 Purpose of the Study

The study examined the effect of electronic fraud on performance of retail banking in Uganda performance in Centenary Bank Limited.

1.4 Specific Objectives of the Study

The study specifically sought to address the following objectives

i) To find out the effect of ATM fraud on performance of retail banking in Centenary bank.

ii) To establish the effect of Internet fraud on performance of retail banking in Centenary bank.

iii) To examine the effect of Mobile fraud on performance retail banking in Centenary bank.

1.5 Research Questions

i) What is the effect of ATM fraud on retail banking performance in Centenary bank?

ii) What is the effect of Internet fraud on retail banking performance in Centenary bank?

iii) What is the effect of Mobile fraud on retail banking performance in Centenary bank?

1.6 Study Hypothesis

Electronic fraud has not significantly affected retail banking at centenary bank

H1: There is no significant relationship between electronic fraud and retail banking

Performance in Centenary bank.

H0: There is a significant relationship between electronic fraud and retail banking

Performance in Centenary bank.

Electronic fraud has significantly affected retail banking at centenary bank

1.7 Scope of the Study

1.7.1 Content Scope

The researcher acknowledged that electronic fraud in the banking sector takes on different forms. However, in this study the researcher examined the independent variable with three forms of electronic bank fraud namely; ATM fraud, Internet fraud and mobile fraud as well as the dependent variable: retail bank performance with constructs efficiency, growth in customer base, quality service, transparency, brand equity, to mention but a few.

1.7.2 Geographical Scope

The study was carried out among the staff and clients of Centenary bank, not excluding the ICT department, Mapeera House in Kampala Capital City. Kampala is Uganda's capital city and therefore it is not only the home of the headquarters of Centenary bank but also has one of the greatest number of bank branches and ATM outlets. Besides, the presence of a number of internet hotspots and easy accessibility to other forms information technology makes Kampala more ideal for electronic bank fraud. More to that, Centenary bank is one of the few banks so far offering mobile money through mobile banking.

1.7.3 Time Scope

The time scope of the study was 2012 to 2017. This period is selected as representative of the time when Centenary bank is experienced a number of such electronic frauds in its retail-banking sector. The researcher acknowledged that electronic products like ATMs have existed long enough at Centenary bank; Electronic Funds Transfer is a commonly used mode of transaction as well as mobile banking.

1.8 Significance of the Study

It is hoped that this study may quantify the existence of electronic banking in Centenary Bank and hence suggest ways in which this fraud can be prevented, detected or dealt with. This may help the management of Centenary bank to expand their electronic banking services to more areas in the country thus enhancing the growth and development of the bank.

The findings of this study shall bring more insight to policy makers in the financial services sector to come up with proper financial control systems and regulations aimed at preventing financial loss through electronic fraud. The researcher anticipates that the findings of this study may act as a reference point for researchers who wish to study electronic banking in the banking sector in particular but more generally in the financial services sector as a whole.

The study may also add value to the body of existing knowledge and perhaps lead to new ventures in the field. This may provide knowledge that may be the basis of research and suggesting further areas for research in banking technology.

CHAPTER TWO

STUDY LITERATURE

2.0 Introduction

The researcher sought the contribution of other scholars on the two variables considered in this study. Therefore, this chapter is focuses to the review of the related literature. The chapter has three basic parts namely; theoretical review, conceptual framework and actual review presented according to the study objectives.

2.1 Literature survey.

A number of studies have been carried out in the field of Electronic Banking ICT and Electronic Banking ICT related fraud, however there remain some grey areas as explained below.
Namirembe (2004) carried out a study on the effect of electronic banking ICT innovations on the Banking Industry, taking a case study of Dfcu bank. The study looked at customer's attitudes to technological innovation, friendliness of the electronic innovations and the effectiveness of the electronic innovations. She discovered that, that much as Electronic Banking ICT carries several benefits in Dfcu bank, it seems to create a number of threats especially related to electronic fraud, that ATMs in particular wastes a lot of time and seems no different from the former way of withdrawing funds from the banks. However, Namirembe's study did not explain at all whether the ICT innovations affected retail-banking performance in one way or another.

Tabaza (2009) also carried out a study on ATM fraud and customer turn over in commercial bank in Uganda, a case study of Stanbic bank. According to Tabaza (2009) not much literature has been circulated on the magnitude of customer turn over related to ICT electronic fraud within Stanbic bank. The results of this study were quiet about the other causes of customer turnover.

Tunanukye and Oluwafemi (2012) further carried out a study on Impact of information technology on the Ugandan finance and investment industry. A case of Alliance investment house. They stated that, as Information Technology is vital in banking today, it becomes imperative for banks to realize its impact on operational performance in order to justify capital investments. The objective of their work was just to examine how the adoption of Information Technology affects the operations of commercial banks in terms of effectiveness, efficiency, competitiveness, customer base and globalization. However, just like Namirembe and Tabaza , the study but did not look at ICT related fraud as a problem to the performance of retail banking.

Kizito and Mugole (2015) sought to establish the effectiveness of mobile banking services in selected commercial banks in Uganda. Research findings revealed that mobile banking services inthe selected commercial banks were generally effective. The least effective item under mobile banking services was noted in security measures and privacy, followed by time management, convenience and financial risk measures respectively. This study also found out that there were significant differences in the effectiveness in mobile banking services among selected commercial banks. Relating to the security challenges associated with mobile banking the study reported that the present and single biggest challenge to the trust reposed in banks by customers is electronic fraud. Besides the risk of losing customers, direct financial impact for banks is also a significant factor. Upon reporting of a fraudulent transaction by a customer, the bank is liable for the transaction costs and has to refund the client. Additionally, fraud invites fines from the regulatory authorities. All these continue to affect the effectiveness of mobile banking as an enhancer of retail banking performance.

2.2 Literature Review

This study was guided by the Fraud Triangle Model by Cressey (2000) and the fraud diamond model by Hermanson (2004). Hermanson introduced the "fraud diamond model" in order to add to the factors cause fraud. The model adds a fourth variable "capabilities" to the three of the "fraud triangle": motive / pressure", "Opportunity" and "Rationalization".

Why people commit fraud was first examined by Cressey Donald, a criminologist in 1950. His research was about what drives people to violate trust. He interviewed 250 criminals over a period of 5 months whose behaviors met two criteria:

(i) The person must have accepted a position of trust in good faith, and

(ii) He must have violated the trust (Rasha and Andrew, 2012).

Cressey was especially interested in the circumstances that lead to otherwise honest people to get overcome by opportunity and temptation to commit fraud when the environment is ripe for fraud.

He found that three factors must be present for a person to violate trust and was able to conclude that: "trust violators when they conceive of themselves as having a financial problem which is non-sharable, have knowledge or awareness that this problem can be secretly resolved by violation of the position of financial trust and are able to apply to their own conduct in that situation, verbalization which enable them to adjust their misconceptions of themselves as users of the entrusted funds and property " (Rasha and Andrew 2012).

The three factors were non-sharable financial problem, opportunity to commit the trust violation, and rationalization by the trust violators, Cressey (1987) as cited by Coenen (2005). When it comes to non-sharable financial problem (pressure), Cressey (1987) as cited by Rasha and Andrew (2012) noted that "persons become trust violators when they conceive of themselves as having incurred financial obligations which are considered as non-socially-sanction able and which, consequently, must be satisfied by a private or secret means."

He also mentioned that perceived opportunity arises when the fraudster sees a way to use their position of trust to solve the financial problem, knowing that they are unlikely to be caught. As for rationalization, Cressey as cited by Rasha and Andrew (2012), believed that most fraudsters are first-time offenders with no criminal record. They see themselves as ordinary, honest people who are caught in a bad situation. This enables them justify the crime to themselves in a way that makes it acceptable or justifiable. Cressey as cited by Rasha and Andrew (2012) found that: In the interviews, many trust violators expressed the idea that they knew the behavior to be illegal and wrong at all times and that they merely kidded themselves into thinking that it was not illegal.

Over the years, Cressey's hypothesis has become well known as "the fraud triangle" as shown in figure 2.1 below. The first side of the fraud triangle represents a pressure or motive to commit the fraudulent act, the second side stands for perceived opportunity, and the third side represents a rationalization (Wells, 2011).

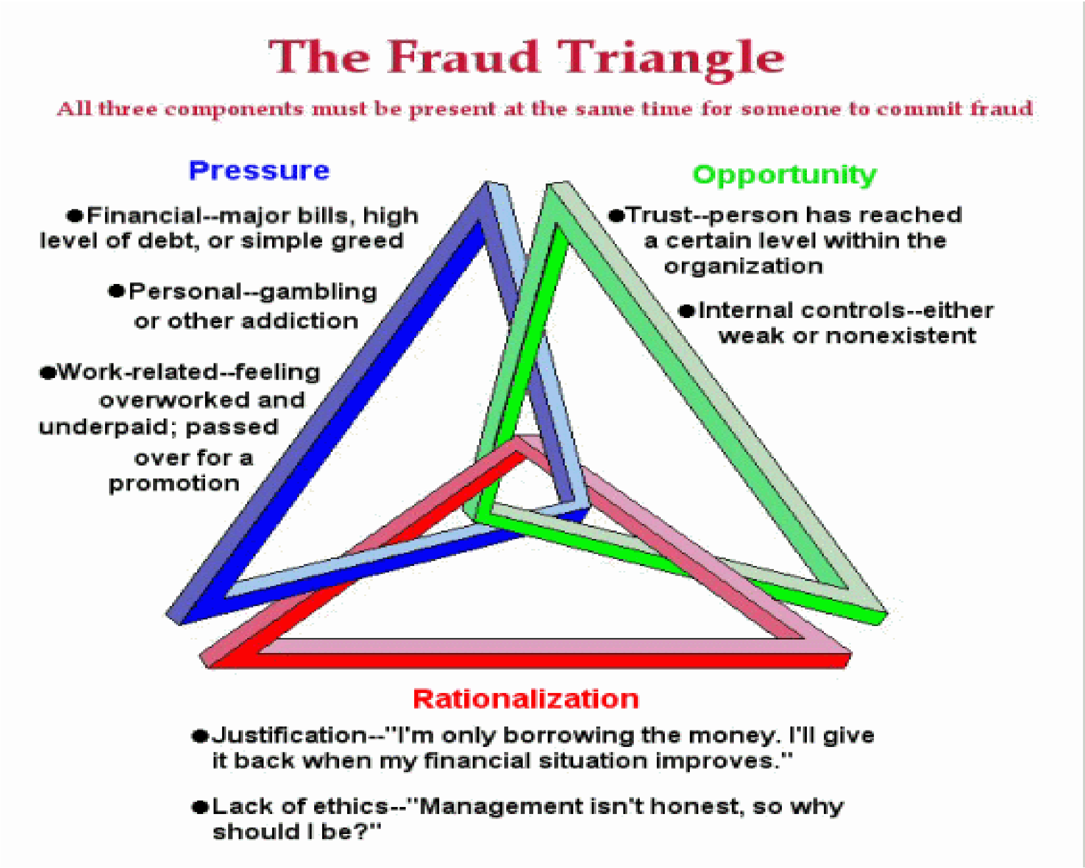
The Fraud Triangle
All three components must be present at the same time for someone to commit fraud
Pressure
●Financial--major bills, high level of debt, or simple greed
●Personal--gambling or other addiction
●Work-related--feeling overworked and underpaid; passed over for a promotion
Opportunity
●Trust--person has reached a certain level within the organization
●Internal controls--either weak or nonexistent
Rationalization
●Justification--"I'm only borrowing the money. I'll give it back when my financial situation improves."
●Lack of ethics--"Management isn't honest, so why should I be?"

Figure 2.1: Fraud Triangle

Source: Cressy And Wells (2000, 2011)

Cressey as cited by Wells (2011), Pressure/ Motive is divided into the non-sharable financial problems into six categories: difficulty to payback debt, problems resulting from personal failure, political pressure, business reversals (incontrollable business failures such as inflation or recession), physical isolation (a trust violator is separated from people who can help him), status gaining (living beyond one's means) and employer-employee relations (employer's unfair treatment).

Researchers in the audit literature defined differently the components of the fraud triangle and gave different examples for each. For instance, Lister (2007) defined pressure/motive to commit fraud as "the source of heat for the fire" but he believed the presence of these pressures in someone's life does not mean he or she will commit fraud. He also added there are three types of motivation or pressure: personal pressure to pay for lifestyle, employment pressure from continuous compensation structures, or management’s financial interest, and external pressure such as threats to the business financial stability, financier covenants, and market expectations.

Lister (2007) saw opportunity, which is the second side of the fraud triangle as “the fuel that keeps the fire going” and he believed even if a person has a motive, he or she cannot perpetrate a fraud without being given an opportunity. He also gave some examples of opportunities that can lead to fraud like high turnover of management in key roles, lack of segregation of duties, and complex transactions or organizational structures. As for the third component of the fraud triangle “rationalization” Lister (2007) defined it as “the oxygen that keeps the fire burning.” Although, forensic accountants may not be able to assess the personal value system of each individual in the organization, they can assess the organizational culture.

On the other hand, Vona (2008) believed the motive to commit fraud is often associated with personal pressure or corporate pressure on the individual. The motive to commit fraud may be driven by the pressures influencing the individual, by rationalization, or by sheer opportunity. He believed a person’s position in the organization contributes to the opportunity to commit fraud. He also believed there is a direct correlation between opportunity to commit fraud and the ability to conceal the fraud. Thus, understanding the opportunity for fraud to occur allows forensic accountants to identify which fraud schemes an individual can commit, and how fraud risks occur when the controls do not operate as intended by management.

Mudrock (2008) also argued that pressure can be a financial pressure, non-financial pressure or political and social pressure. Non-financial pressure can be derived from a lack of personal discipline or other weaknesses such as gambling, drug addiction. While political and social pressure occurs when people feel they cannot appear to fail due to their status or reputation. However, Rae and Subramaniam (2008) said pressure relates to employee’s motivation to commit fraud as a result of greed or personal financial pressure, and opportunity refers to a weakness in the system where the employee has the power or ability to exploit, making fraud possible, while rationalization as a justification of fraudulent behavior as a result of an employee’s lack of personal integrity, or other moral reasoning.

Albrecht, Albrecht and Albrecht (2008, 2010), however, mentioned pressure/motive can be financial or non-financial and they gave examples of perceived financial pressures that can motivate fraud like: personal financial losses, falling sales, inability to compete with other companies, greed, living beyond one's means, personal debt, poor credit, the need to meet short-term credit crises, inability to meet financial forecasts, and unexpected financial needs. They also gave example of non-financial pressure such as: the need to report results better than actual performance, frustration with work, or even a challenge to beat the system. They believed that even with very strong perceived pressure, executives who believe they will be caught and punished rarely commit fraud.

They also mentioned some examples of rationalizations that executives can use to commit fraud like: "we need to keep the stock price high", all companies use aggressive accounting practices or it is for the good of the company. As for the perceived opportunities to commit fraud examples include; a weak board of directors, lack of or circumvention of controls that prevent / detect fraudulent behavior, failure to discipline fraud perpetuators, lack of access to information and lack of an audit trial.

It can be concluded from the above that motives/pressures were classified differently. Some researchers classified them as personal, employment or external pressure, while others classified them as financial and non-financial pressures. However, it can be noticed that both classifications are somehow related. For instance, personal pressure can come from both financial and non-financial pressure. A personal financial pressure in this case could be gambling addiction or sudden financial need, while a personal non-financial pressure can be lack of personal discipline or greed. By the same token, employment pressure and external pressure can come from either financial or non-financial pressures. As for the third component of the fraud triangle "rationalization" Lister (2007) defined it as "the oxygen that keeps the fire burning." Although, forensic accountants may not be able to assess the personal value system of each individual in the organization, they can assess the organizational culture.

On the other hand, Vona (2008) believed the motive to commit fraud is often associated with personal pressure or corporate pressure on the individual. The motive to commit fraud may be driven by the pressures influencing the individual, by rationalization, or by sheer opportunity. He believed a person's position in the organization contributes to the opportunity to commit fraud. He also believed there is a direct correlation between opportunity to commit fraud and the ability to conceal the fraud. Thus, understanding the opportunity for fraud to occur allows forensic accountants to identify which fraud schemes an individual can commit, and how fraud risks occur when the controls do not operate as intended by management.

Second, the “fraud diamond model” by Hermanson (2004), adds a fourth variable “capabilities” in order to add to the factors that cause electronic fraud. To this became the four causes,:“ pressure/ motive ”, “Opportunity”, “Rationalization” and “ capabilities”.

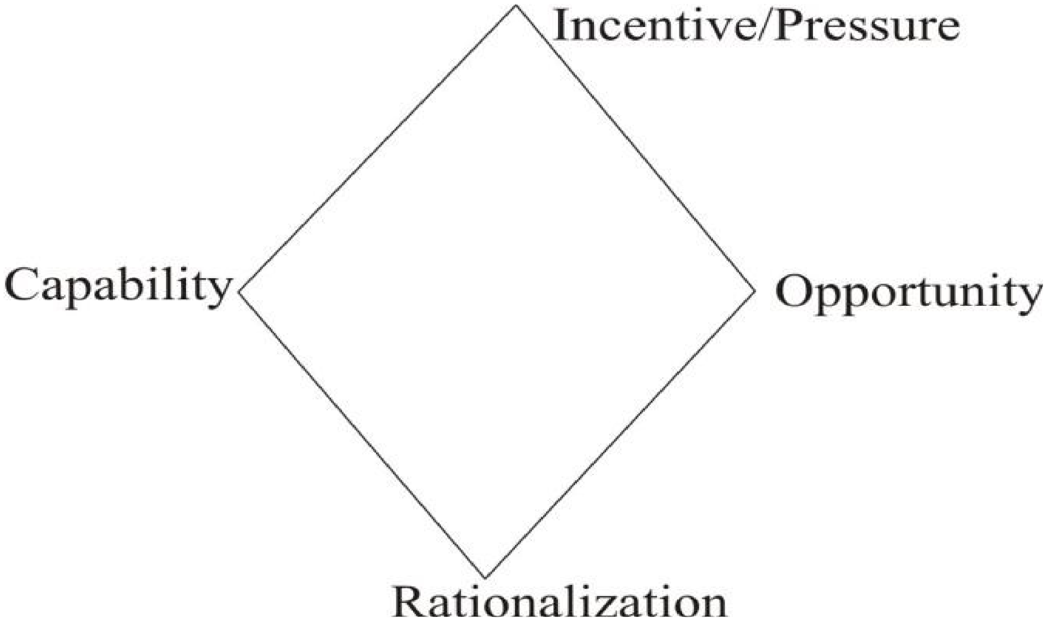

Fig 2.2 The Fraud Diamond model
Source: Hermanson (2004)

Just like a “diamond” the four faced model explains further in addition to ‘pressure’, ‘Opportunity’ and ‘ Rationalization’, ‘ Capabilities’, is another element that absolutely applies to the circumstances that lead to otherwise honest people to become by opportunity and temptation to commit fraud, when the environment is ripe for fraud. All the four must be present before electronic fraud must be committed within the bank especially using Automated Teller Machines, the Internet as well as mobile banking.

2.3.1 Effect of ATM banking Fraud Retail banking performance

Bank customers in Uganda had a collective sign-of-relief when the Automated Teller Machines (ATM) was introduced as an instrument to aid banking operations in 1988, starting with Standard Chartered Bank. The introduction of the ATMs by financial institutions all-over the world changed the face of banking but with some inherent challenges.(Obiano 2009)

The introduction and use of Automated Teller Machine (ATM) is not only safe but also convenient. However, this has been lessened by the frauds that are perpetrated by ATM fraudulent (Onuorah and Ebimobowei, 2012). Since the introduction of ATM in the early 1970s, perpetrators have been working hard to find ways of how to steal cash from the machines (Kanu & Okarafor, 2013). In 2000, a report on global ATM fraud identified the various ATM fraud which included; shoulder surfing, Lebanese loop, using stolen cards, card jamming, using fake cards and card swapping. According to Wilhem (2004), ATM fraud and fraudulent activities greatly affects the banking sector. He estimated that ATM fraud cost US $1.2 billion annually.

The banking system with all its complexities, challenges and opportunities touches virtually all aspects of the daily lives. Using a credit card to make a purchase, writing a personal or business check, paying bills and moving funds online or accessing funds through an automatic teller machine (ATM) are just a few examples of how people may participate daily in the banking system. Even the micro-finance banks provides banking-related services such as loans and check cashing in communities where those services are either not readily available or where consumers perceive the micro finance bank to be their best or only-banking alternative.

The techniques of managing of banking industries through the use of Automated Teller Machine (ATM) towards improving banking industry performance is a basket full where every financial institution is expected to pick that which is applicable to it. According to the Fannie Mae Foundation, automated teller machine as used in banking sector serve approximately 420 million transactions annually for a total of $3.3 billion in gross annual revenues. In this article, we will address a number of topics including the types of services provided by full service banks, technological changes and the use and important of automated teller machine and fringe banking services.

ATMs are known by various other names including automatic banking machine (or automated banking machine particularly in the United States) (ABM), Automated Transaction Machine, Cashpoint (particularly in the United Kingdom), Money Machine, Bank Machine, Cash Machine, Hole-In-The-Wall, Autoteller (after the Bank of Scotland's usage), Cashline Machine (after the Royal Bank of Scotland's usage), MAC Machine (in the Philadelphia area), Bankomat (in various countries particularly in Europe and including Russia), Multibanco (after a registered trade mark, in Portugal), Minibank in Norway, Geld Automaat in Belgium and the Netherlands, and All Time Money in India.

Rose (1999) cited by Aditi (2013) , describes ATMs as follows: “an ATM combines a computer terminal, record-keeping system and cash vault in one unit, permitting customers to enter the bank’s book keeping system with a plastic card containing a Personal Identification Number (PIN) or by punching a special code number into the computer terminal linked to the bank’s computerized records 24 hours a day”. Once access is gained, it offers several retail banking services to customers. They are mostly located outside of banks, and are also found at airports, malls, and places far away from the home bank of customers. They were introduced first to function as cash dispensing machines. However, due to advancements in technology, ATMs are able to provide a wide range of services, such as making deposits, funds transfer between two or accounts and bill payments. Banks tend to utilize this electronic banking device, as all others for competitive advantage.

Using an ATM card, a debit card, or a credit card, bank patrons can electronically access their accounts and withdraw or deposit funds, make payments, or check balances. ATMs have eliminated the need to enter a bank for basic transactions and allow access to accounts at machines throughout the United States. Financial institutions started charging fees to use their ATMs in the mid-1990s, making the transactions very profitable for the host banks. The use of ATMs has cut service staff in traditional banks, impacting employment in the industry. As many machines are now commercially owned and leased in public venues, a technical industry for cresting, leasing, and maintaining the machines has developed.

However, the advantages of safety and convenience of ATM has unfortunately been lessened by the frauds that are perpetrated by ‘plastic money’. The increase in number of customers using ATM has also increased the propensity to fraudulent practices by the ATMs fraud perpetrators.

Ihejiahi (2009)expressed concern about the lack of cooperation among banks in the fight to stem the incidence of ATM related frauds now plaguing the industry. He expressed that the silence among banks on ATM frauds makes it difficult for banks to share vital information that will help curb the menace.

Muhammad (2009) postulates that the level of ATM fraud tend to have overshadowed the improvements which it has brought into the service delivery systems of Nigerian financial institutions. Similarly, he adds that despite the reality that the introduction of ATM terminals as a banking instrument was lauded by several customers as an alternative to the frustrating queues that characterized the country's banking hall, the situation today has changed drastically; it has become a source of worry to users and providers (banks) because the function it was meant to provide has been eroded seriously.

Obiano (2009) blamed the menace of ATM frauds on indiscriminate issue of ATM card without regard to the customer’s literacy level. According to him one of the frequent causes of fraud is when customers are careless with their cards and pin numbers as well as their response to unsolicited e-mail and text messages to provide their card details. Omankhanleu(2009) opined that the current upsurge and nefarious activities of Automated Teller Machine (ATM) fraudster is threatening electronic payment system in the nation’s banking sector with uses threatening massive dumping of the cards if the unwholesome act is not checked.

As with any device containing objects of value, ATMs and the systems they depend on to function are the targets of fraud. Fraud against ATMs and people’s attempts to use them takes several forms. These include: Shoulder Surfing; Lebanese Loop; Using Stolen Cards; Card Jamming; Use of Fake Cards; Duplicate ATMs; Card Swapping: Diversion; and ATM Burglary (A Report on Global ATM Frauds, 2007). Some if not all are found in the Ugandan banking environment which ultimately undermined the effectiveness of ATM facility. ATM fraud is now a recurrent decimal that speaks ill of the Ugandan financial system which ought to be checkmated.

Furthermore, Owolabi (2010) noted that the problem of ATM fraud in the retail banking sector is not limited to any economy, nation, continent or environment. These kinds of losses pose a significant threat to banks considering their roles in the economy. The relationship between banking efficiency and the use of ATM is complex. The overall level of efficiency and

productivity greatly influence the organization overall success. The achievement, goals, profit and attainment of retail banking sector depend largely on proper management and technology like ATM (European ATM Crime Report, 2007). Adepofu and Alhassan (2010) opined
that bank customers in Nigeria initially cherished the use of ATM and their convenience. However, recently there has been a proliferation of ATM fraud that has impacted electronic banking negatively. According to the study by Abdul Rasheed, Babaitu and Yunisa (2012) among Nigerian banks, it was revealed that there is a strong and significant negative relationship between fraud and bank profits. In addition, a study by Kanu and Okarafor (2013) on "Nature, Extent and Economic Impact of ATM fraud", found out that there is a largely positive relationship between bank deposit and fraud in the Nigerian bank industry. Extensive studies on ATM fraud have been carried out among Nigerian banks. Fraud is one of the prominent features which brought about reforms in the banking sector. Fraud is regarded as the most fatal of all risks confronting banking in Nigeria (Chiezey, 2013).

Bank frauds erode public confidence in the banking sector. This brings various setbacks to the efforts of promoting the banking culture. Similarly, Rasheed, et. al., (2012) urged that frauds bring about financial losses to the banks and shareholder depriving honest among applicants. Basing on the research findings by Nwankwo (2013) it was inferred that it is important to emphasize that management and regulation of bank fraud was quantitatively important in the performance of banks. In the same study, electronic banking fraud was found to have a positive effect on the performance of commercial banks in Nigeria. The study concluded that the level of ATM bank fraud over the years have indeed negatively affected insignificantly on the performance of banks in Nigeria.

In a study by Idolor (2010) about the causes effects and possible remedies of ATM fraud in Nigeria, it was found out that loss of customer confidence was the most prominent effect followed by loss of revenue, loss of patronage , distress and loss of corporate image. The study also revealed that response of most of the banks to fraud needs improvement in order to avoid putting the burden to customers. In addition, Ihejiahi (2009) was concerned about the lack of cooperation among banks in the fight to stem the incidence of ATM related fraud plaguing the industry. Akindele(2010) found out that lack of adequate training, communication gap and poor leadership skills were the greatest causes of ATM fraud. Furthermore, Idowu (2009) pointed out that poor management, policies and procedure, inadequate working conditions, bank staff overstaying on particular jobs and staff's feeling frustrated as a result of poor remuneration.

2.3.2 Effect of Internet Banking fraud on retail banking performance.

Internet banking involves conducting banking transactions such as account enquiry printing of statement of account; funds transfer payments for goods and services, etc on the internet using electronic tools such as the computer without visiting the banking hall. E-commerce is greatly facilitated by internet banking and is mostly used to effect payment. Internet banking also uses the electronic card infrastructure for executing payment instructions and for final settlement of goods and service over the internet between the merchant and the customer, currently the most common internet payments are for consumer bills and purchase of air ticket through the websites of the merchants (Littler, 2006).

Berney (2008) states that nowadays, customers rely heavily on the web for their banking business, leading to an increase in the number of fraudulent online transactions. Fraudsters react to these changes as the internet provides them with more opportunities to attack customers (Gates and Jacob, 2009). On the web, customers are not physically present to authentic the transactions, which facilitates fraud (Malphrus, 2009; Gates and Jacob, 2009). Orad (2010) even claims that the internet allows criminals to organize as a network, supporting each other in their attacks. Fraudsters are particularly interested in accessing customers' online bank accounts. A common practice to steal access data are "phishing," where an e-mails from an allegedly credible source are sent to bank customers requesting sensitive information such as their user name or password.

During recent years, phishing has become a significant threat to online security (Bergholz, et. al., 2010). Since (credit) cards have become a major payment instrument for web -based transactions, they have attracted great attention of fraudsters (Malphrus, 2009). Despite an inability to provide exact numbers on card fraud because of differences in bank's' fraud tracing and lack of customer reporting, worldwide card fraud likely exceeded $10 billion in 2009
(ACI Payment Systems, 2009).In general, fraud, either online or offline, hurts retail banks' operating performance, and increases their costs of operation (Gates and Jacob, 2009).According

to Greene (2009), the true economic costs are about 150 percent of the actual fraud loss. Retail banking fraud entails any attempt of criminals to "achieve financial gain at the expense of legitimate customers or financial institutions through any transaction channel, such as credit cards, debit cards, ATMs, online banking, or checks" (Sudjianto, et. al., 2010). Recent literature categorizes fraud by the person conducting it and differentiates between first-party and third-party fraud. In first-party fraud, a legitimate customer betrays the bank, where as in third-party fraud, the customer becomes a victim of criminals who steal identities, use lost or stolen cards, counterfeit cards, or gain unauthorized access to customer accounts by other means (Gates and Jacob, 2009; Greene , 2009). This study focuses on third-party fraud. Third-party fraud can be subdivided into different classes. Most common is differentiation between payments fraud and identity theft.

Payments fraud refers to "any activity that uses information from any type of payments transaction for unlawful gain" (Gates and Jacob, 2009). It occurs when fraudsters gain access to customer accounts and use these accounts for their own financial benefit (Sullivan, 2010; Malphrus, 2009). Identity theft may also comprise fraudsters illicitly gaining access to customer accounts (Hartmann-Wendels, et. al., 2009), but usually refers to opening new accounts in the customer's name (Malphrus, 2009). This study focuses on payments fraud in general and on card fraud in particular, since it is of rising importance globally (Worthington, 2009). As the Internet becomes more important for commerce, Internet Web sites are playing a more central role in most companies' business plans. An especially elegant case has been made for the ''Internet-only'' business model in the banking industry.

Overhead expenses can be reduced by jettisoning physical branch offices. Banks can use the resulting savings to reduce their loan interest rates or increase their deposit interest rates, attracting new customers without sacrificing earnings. The web-based distribution focus allows banks to enter new geographic markets without the costs of acquiring existing banks or starting up new branches, further increasing growth potential. Nearly half of all U.S. banks and thrifts were operating transactional Internet Web sites at the beginning of 2002 (A transactional Web site allows customers access to banking services without leaving their homes or offices. The most basic transactional Web sites allow customers to check account balances and transfer funds between accounts. More-advanced Web sites allow customers to open new accounts, apply for loans, manage investments, receive bills, and pay bills. The point estimate of ‘‘nearly half of all U.S. banks and thrifts’’ is based on the 49.7% Internet Web site adoption rate at national banks as of 2001: Q4 (Office of the Comptroller of the Currency staff). But most of these firms have adopted a ‘‘click-and-mortar ’’ business model in which an Internet Website is used to complement existing brick and mortar branches. Only a few dozen banks and thrifts have adopted a pure Internet-only strategy that eschews physical branches entirely; by-and large, these firms have generated sub-par earnings. For every Internet-only bank or thrift that has achieved marginal levels of profitability, another has exited the market through liquidation or acquisition or has abandoned the pure Internet-only business model and established physical branches. Government regulators have become increasingly risk averse with banks and thrifts that deploy, or wish to deploy, this business model.

A confidential transaction requires a transaction to be authenticated, meaning you have to know who sent the transaction. Authentication is one element of confidentiality. And without good authentication techniques, you have no way to be sure that the person sending the instructions is the person they say they are (Kanu & Okoroa for, 2013). There exists numerous threats on online banking; financial services providers are faced with complex challenges that directly affect their bottom line and, potentially, their very survival in a high-churn market. Protecting sensitive and critical data, no matter where it resides, and ensuring that only the appropriate persons have access to that data is a core requirement of every company’s security strategy (Ojo, 2008). With the rising incidence of threats to sensitive data, and increasing requirements to protect that data, banks must focus squarely on their security infrastructure. Obtaining safe and secure environment of computer technology is the most important concern for all financial service organizations.

Security of online banking transactions is one of the most important challenges to the banking sector (Idowu, 2009).Billions of financial data transactions are conducted online every day, and bank cyber-crimes take place every day by skilled criminal hackers through manipulating the bank’s online information system (Ojo, 2008). Threats can come from inside or outside the system, which threatens customers’ information and transactions, where bank administrators must ensure that banks have the appropriate practices in place to guarantee the confidentiality of customers' data, as well as the integrity of the e-banking system and the transactions conducted (Hoffman &Birnbrich, 2012).

Fraud is defined as any behavior by which one person intends to gain a dishonest advantage over another. Fraud is an act which intends to cause wrongful gain to one person and a loss to the other, either by a way of concealment of facts or otherwise. Based on an empirical analysis performed on real world transaction datasets, Akindele (2010) concluded that a large number of different e-banking accounts were accessed by a single fraudster, which included small value transactions with a total value larger than a single account fraud are common based on the increased number of password failures that open doors for fraudulent behaviors. The objective of an attacker may vary. Attacker may try to exploit vulnerabilities in particular operating systems, or they may try repeatedly to make an unauthorized entry into a website leading to denial of service to customers(Ojo, 2008).

Hackers or attackers have many different ways that they can try to break the system through. However, the problems in information systems today are inherit within the setup of communication and the computer itself. Hence, banks and service providers need to guard against various types of online attacks to achieve secure communications over the channels of information systems.

Ihejiahi (2009) reported that the main threats or attacks to security of e-banking platforms are the following denial of service, illegitimate use, disclosure of information, and repudiation. Other research presented a classification for the common attacks against online banking systems. Akindele (2010) proposed a hierarchy of causes that includes three major categories; legitimate access, device control and credentials theft. In practice, existing online bank fraud detection systems are rule based, in which the rules are generated according to domain knowledge. Consequently, these systems usually have a high false positive rate, this means that the detection rate of fraud is low. The identification of the access devices is made by a component that must be downloaded in client devices, and already used by the actual online banking system (Kanu & Okoroafor, 2013). This component generates a fingerprint of the access device, and sends it to the bank website as part of each transaction. The observation of user's global behavior plays a major role in fraud detection.

A large number of different accounts accessed by a single device, or the occurrence of login fail over many accounts using a single trial password are examples of global behavior that infer a fraud (Mudiri, 2014). Monitor uses counters to verify transactions which they updated for each transaction. Kanu and Okarafor (2013) also investigated fraud detection in e-banking, and reported three main types which include credit card fraud detection, computer intrusion detection and telecommunication fraud detection. In addition, they proposed and implemented an online banking fraud detection system, which takes advantage of domain knowledge, mixed features, multiple data mining methods and multiple layer structure for a systematic solution. Their approach and system were tested in a major bank, and showed that it is particularly effective in detecting fraud in large volume of extremely imbalanced data (Akindele, 2010). Also, it performed better than existing fraud detection methods in both efficiency and accuracy. In addition to fraud prevention methods used in e-banking domain, many national regulators have already amended their regulations to ensure safety and soundness of the domestic banking systems, protect customer rights, and achieve public trust among them (Berney, 2008).

Licensing, verifying an individual’s identity, capacity planning, adaptation, legalization, harmonization and integration are all policies that can be used to achieve and enhance safety and security of e-banking.

2.3.3. The Effect of Mobile banking fraud on retail banking performance

Mobile banking involves the use of mobile phone for settlement of financial transactions. It supports person to person transfers with immediate availability of funds for the beneficiary. Mobile payments use the card infrastructure for movement of payment instructions as well as secure Short Message Service (SMS) messaging for confirmation of receipt to the beneficiary. Mobile banking is meant for low value transactions where speed of completing the transaction is key. The services covered under this product include account enquiry, funds transfer, recharge phones, changing of passwords and bill payment which are offered by few institution (Sathye, 1999). Mudiri (2014) maintains that the introduction of mobile money services has greatly changed the dynamics of the industry, bringing financial services closer to the public. Financial institutions such as commercial banks and microfinance institutions are also investing in the provision of mobile financial services. Consistent with this, Munyoki (2015) states that mobile banking offers millions of people a potential solution in emerging markets that have access to a cell phone yet remain excluded from the financial mainstream.

Mobile banking has the advantage of making basic financial services more accessible by minimizing time and distance to the nearest retail bank branches as well as reducing the banks' own transaction costs (Lee and Kim, 2007). According to Nyango, Mbabazize and Shukla (2015), mobile banking involves the use of mobile phone for settlement of financial transactions. It supports person to person transfers with immediate availability of funds for the client. Ogwal (2014) reports that the rate of mobile money account ownership outstrips bank account ownership, which stood at 3.6 million bank accounts in 2013. He argues that the massive uptake of mobile money has also promoted new forms of frauds.

Uganda mobile money market has been a playground for fraudsters with an average of at least 100 mobile money users losing money every week. In Agreement a survey by Agent Network Accelerator in Uganda conducted by the Helix Institute of Digital Finance (2013) revealed that one of the biggest challenges of mobile financial services is the high risk of fraud. Despite the many advantages of mobile banking, the innovation suffers from a number of challenges.

Mudiri (2014) defines mobile banking fraud as the intentional or deliberate action undertaken by players in the mobile financial services ecosystem aimed at deriving gain (in cash or e-money) and /or denying other players revenue and/or damaging the reputation of the other stakeholders. He goes on to categorize mobile banking fraud into: consumer driven fraud, agent driven fraud, business partner related fraud, mobile financial service provider fraud.

Consumer driven fraud refers to fraud that is initiated by fraudsters posing as customers and is the most common type of mobile fraud. Agent driven fraud is perpetuated from within the agent network and it is initiated and operated by agents or their employees. Business partner driven fraud describes the fraudulent activities perpetrated by bank staff on the bank, bank staff on customers or bank staff on mobile money operator.

Mobile financial services provider fraud refers to a range of fraudulent activities perpetrated by the mobile financial service providers' employees. This fraud could target the service provider, agents or customers (Mudiri, 2014). As mobile fraud might ultimately affect customer relationship quality and customer loyalty, fraud prevention and its communication are important aspects for retail banking performance. Although mobile fraud is continuously becoming a challenge in the mobile financial services sector, limited academic efforts have been undertaken to explain the reasons for this trend. Ogwal(2014) argues that the growing fraudulent cases in the mobile banking services can be attributed to the sophisticated nature of the fraud mechanisms employed by fraudsters. The approaches to fraud executed by the con-men demonstrate their thorough understanding of mobile money system. This is made worse by Uganda's weak Know Your Customer (KYC) norms. It is reported that the ease of securing and registration of a phone SIM card makes it difficult to trace fraudsters. Most fraudsters acquire SIM cards for purposes of committing fraud. Additionally, Mudiri (2014) reports that the key enablers of mobile banking fraud include but not limited to: weak regulation, low consumer awareness levels and poor communication with the main players. For example the inability of regulators to monitor the mobile money ecosystem, to set guidelines for different stakeholders increases the likelihood of fraud associated with mobile banking.

Similar views are also shared by Ojo (2008) in highlighting the following as the institutional factors responsible for the increasing mobile banking fraud. These factors include: weak accounting and internal control system, inadequate supervision of subordinates and the banks' reluctance to report fraud due to the perceived negative publicity or image. This is capable of engendering more fraud. As maintained by Lee and Kim (2007) mobile banking fraud has a number of far reaching effects on retail banking performance. These range from the credibility of the bank, brand equity, the growth in the number of clients to affecting the prospects of rolling out the mobile banking services across the country. Although most scholars have not explicitly studied how mobile banking fraud affects retail bank performance, the available literature relating to the effect of mobile banking on performance of financial institutions highlights mobile banking fraud as a key challenge in e-banking. For example, Nyango, et. al., (2015) examined the contribution of E-Banking towards the performance of banking institutions in Rwanda. The findings of their study revealed that E-Banking greatly affected the banks' performance in terms of increase in profitability, reduction in the costs of operations, increase in the bank's assets and bank's efficiency. The findings of their study further revealed that mobile banking technology still lacks in security. They argue that it is easier for fraudulent personnel to carry out their fraudulent activities without being detected. This in the long run affects negatively the performance of the banking sector. In line with Nyango, et. al., (2015), the study by Hoffman and Birnbrich (2013) revealed similar findings. The two scholars examined the impact of fraud prevention on bank-customer relationships in the retail banking in the Netherlands. The purpose of their study was to establish a conceptual as well as an empirical link between retail banks' activities to protect their clients from third party fraud, the quality of customer relationships and customer loyalty. The results of this study found out that there is a positive association between customer familiarity with and knowledge about the bank's fraud prevention measures and customer relationship quality.

Customer relationship in turn, positively affects customer loyalty intention. The implication of this is that banks which have instituted mobile banking fraud prevention mechanisms are able to build trust among their customers. On the contrary banks that do not have such measures in place Experience performance related challenges. Gates and Jacob (2009) state that mobile banking fraud hurts both banks and their clients. Banks incur substantial operating costs by refunding customers' monetary losses while bank clients experience considerable time and emotional losses. They have to detect the fraudulent transactions, communicate them to their bank, initiate the blocking and re-issuance or re-opening of a card and dispute the reimbursement of their monetary losses (Douglass, 2009). Similarly Hoffman and Birnbirch (2012) state that becoming a fraud victim may also impact the customers' perception of feeling secure and protected at their bank. Thus fraud may damage the bank-customer relationship because of shattered trust and confidence. This in turn may negatively affect customer loyalty and stimulate switching behavior (Gruber, 2011), thereby hurting the banks' reputation and impeding of new customers (Buchanan, 2010).

2.4 Electronic fraud and Retail Banking Performance.

Retail banking also known as consumer banking is the provision of services by a bank to individual consumers, rather than to companies, corporations or other banks (Darlington, 1999).
Services offered include savings and transactional accounts, mortgages, personal loans and credit cards. The term may also be used to refer to a division or department of a bank dealing with retail customers. Retail banking provides financial services for families and small businesses. The three most important functions are credit, deposit and money management (Idowu, 2009). Credit allows people to spend future earnings now. Retail banks also offer small business loans to entrepreneurs.

These small companies create up to 65 percent of all new jobs as they grow. Retail banks use the depositors' funds to give out loans. They make money by charging higher interest rates on loans than they pay on deposits. Retail banking remains an essential part of the financial services industry, accounting for 45% of all banking revenues. But while the sector has recovered from the2007-2008 financial crises, the growth picture globally is mixed. To place the importance of performance management for retail banks in its appropriate context, itis necessary to consider the process of setting the bank's strategy. Strategy in retail banking involves devising a unique value proposition and market position and preserving it by creating a culture of customer care (Gates and Jacob, 2009).

This customer focus is facilitated by the 3Psthus, professional and ethical people, efficient processes and innovative products. The implication of this strategy statement is that competitive advantage is created and preserved by an emotional bond between customer and bank. The emphasis on the role of customer-centricity for bottom-line success means that bank executives and, in particular, HR experts must take action to align divisional, team and individual performance with the bank's strategic objectives (Idowu, 2009).Banks are seeing a return to pre-crisis levels of revenue expansion, but economic, demographic, competitive, and technological changes will continue to exert downward pressure through the end of the decade (Darlington, 1999). Indeed, despite concerted efforts to stabilize performance, many retail banks are still plagued by long cycle times, inconsistent channel experiences and generic customer propositions. Unless they make deeper, bolder changes, profitability and competitiveness will suffer. Banks can make these changes and substantially improve performance by more efficiently and effectively fusing digital functionality with personalized, human interaction in other words, by becoming more bionic (Gates and Jacob, 2009). A bionic transformation includes blending digital and personal interactions to create a more responsive and cost-effective distribution model, articulating a value proposition that combines human judgment with data power, and adopting a customer journey mindset with end-to-end processes that are supported by robotics and machine learning.

The introduction of universal banking practice and the adoption of electronic banking by deposit Money banks have offered increased services to customers with attendant increase in customer risk exposure (Sullivan, 2010; Malphrus, 2009). The changing environment of bank management has impacted much on the number of services and risk which banks face. Electronic banking is the conduct of banking business electronically which involves the use of information communication technology to drive banking business for immediate and future goals (Douglass, 2009). The revolution in the banking industry started with the advent of electronic devices to assist in the discharge of quality services to bank customers. The introduction of these electronic devices has increased competition in the industry which has gone a long way to reducing customers' waiting time for banking transactions. This innovation is brought in by the use of computers and other networking gadgets.

E-banking appeal as well its product development is rapidly growing, and the global acceptance has strongly encouraged its penetration. The success of e-banking is contingent upon reliable and adequate data communication infrastructure. Similarly Hoffman and Birnbirch (2012) posit that It is efficient for banks to invest in online transactions through the creation of networks. Most banks today have electronic systems to handle their daily voluminous tasks of information retrieval, storage and processing (Gruber, 2011). Irrespective of whether they are automated or not, banks by their nature are continually involved in all forms of information management on a continuous basis. The computer is of course an established tool for achieving a competitive edge and optimal resource allocation. The most obvious application of computers in the banking industry is in the area of customer services, information management and control (Douglass, 2009).

Computerized banks respond immediately to requests from customers for statement of accounts, Balance and account activity enquiries. With signature and image verification systems, the time take to offer typical cashier services like receiving and paying out of cash is minimized (Sullivan, 2010). Also with the advent of automated Teller machines (ATM), banks are able to serve customers outside the banking hall all round the clock (Mudiri, 2014). E-banking can be classified into three basic types. These include Internet banking, Smart card banking and Mobile/telephone banking. Hoffman and Birnbirch (2012) posit that the rate of adoption of a new innovation is related to (perceived) relative advantage. The greater the perceived related advantage, the faster the adoption. Secondly, the desire to improve organizational performance is seen to be an enabler for technological change.

However, the benefits of electronic banking encompass a broad range of functions and include electronic mail (e-mail) improves communication between individuals and the bank, within the bank, with the bank and external parties and between banks (Sullivan, 2010;Malphrus, 2009). The availability of online information provides bankers and customers with a powerful vehicle

for research. Banks can provide information and services online which customers can pay for and receive. Banking processes are made more efficient and cost effective by integrating other aspects of banking operations such as management and financial control. Lee and Kim (2007) posit that on-line banking services have now become a birth right of the customer as the customer demands the flexibility of operating an account in any branch of a bank irrespective of which branch the account was domiciled (Mudiri, 2014).
With internet banking, customers would enjoy sitting in the comfort of their homes and offices and with a Personal Computer, log onto their banks' servers and transact banking activities (Douglass, 2009). Each financial institution should apply guidelines based on its scope and level of sophistication in e-banking technology. Typically, electronic banking amplifies the scale of exposure of banks to traditional risks, such as transaction, strategic, reputation and compliance risk, among others.

As information systems become more connected and interdependent, the risk of computer intrusion will increase. Arguably, this is the single most challenging aspect of the "new" electronic delivery system. Banks with weak physical and system security substantially increase their exposure to a plethora of risks, many of which could lead to collapse (Lee and Kim, 2007). Potential consequences include direct currency loss, change reputation, improper disclosure, and law suits or regulatory sanction. Bank consolidation as most Central Banks think, may not only be the solution to bank distress and collapse (Gruber, 2011). But exposure to global risk due to the adoption of electronic banking can in a moment throw a bank into oblivion. The security of payment cards from the view point of the holder is another area of concern. The danger of invasion of the system by fraudsters to corner and divert funds is ever present and a successful invasion could result in jumbo scale diversion of funds. Another security problem of payment cards as noted by Mudiri (2014) is the consequence of any break down even momentarily and for whatever reasons, couldbe devastating. Therefore, banks deploying this technology should have an eagle eye to monitor occurrence of breakdown and good maintenance culture.

Therefore, e-banking should be consistent with the banks overall strategic and business plans, and adequate expertise should be employed to operate and maintain such systems. It is therefore Imperative that e-banking risks be managed as part of a bank's overall risk management process

(Malphrus, 2009). The level of risks assumed by banks need to be consistent with individual bank's overall risk tolerance, and not its ability to manage and control risk (Lee and Kim, 2007). Retail banking generally refers to the provision of products and services that banks provide to personal customers and businesses, including SMEs, through a variety of channels including branches, internet and mobile technology (Chiezey, 2013). Banks typically organize their retail banking activities either by the type of customer served, products offered or size. The main functions of retail banks include accepting deposits, making loans and providing payment services.

Retail banking includes personal current account (PCA) and small and medium-sized enterprise (SME) banking services, the reference products for our investigation, but also other products such as residential mortgages, personal loans and insurance. Many retail banks have separate retail banking divisions or business units, with their own management and reporting structures, although there are differences in the way banks define, organize and describe their retail activities (Berney, 2008). Typically, individuals and small businesses constitute the core of the retail banks' customer base. According to Nwankwo (2013), some banks also have wealth management and private banking activities within their retail activities to serve high-net-worth individuals. Retail divisims of the banks tend to serve start-ups and smaller SMEs, while larger SMEs and corporates are generally served by commercial or corporate banking divisions (Gates & Jacob, 2009). Most banks categorize SMEs by annual sales turnover and/or borrowing requirements to determine which of their divisions would cater to these businesses, although the cut-off for separating SMEs and larger corporate customers varies between banks.

2.5 Conceptual framework

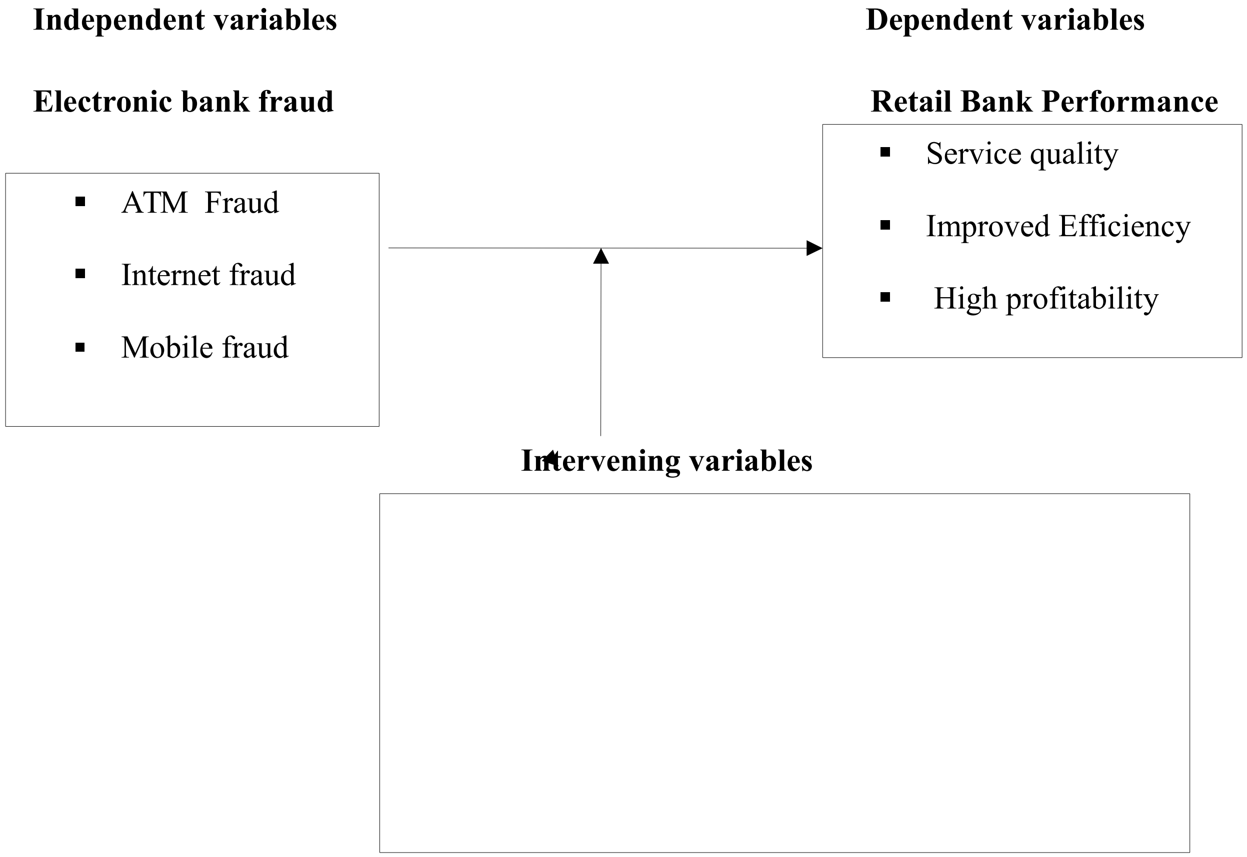

Figure 2.3: Conceptual Framework

Source: *Adopted from Swaminathan and Ananth (2010) and modified by the Researcher (2018).*

Conceptual review

As shown in the conceptual framework figure 2.1 the independent variable of the study is "Electronic fraud, broken down into; ATM fraud, internet fraud and mobile fraud respectively. The independent variable of the study on the other hand is retail bank performance whose indicators are; improved efficiency, service quality and improved profitability etc. The intervening variables are bank policies and regulations by the central bank, Know Your Customer policy and the quality of staff.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter presents and justifies the methodology that was used to answer the research questions. It comprises the research design, study population, sample size, sampling procedure, data collection methods and instruments, data quality control, procedure for data collection, data analysis plan the ethical considerations and the limitations of the study.

3.1.1 Research Design

According to Oso and Onen (2008) a research design is an outline of how an investigation is carried and indicates how data was collected, what instruments were used, and how the data was used. This study employed a cross sectional survey design.

It was used to enable the researcher to collect extensive data on the electronic banking fraud and retail banking performance of Centenary Bank at one single point in time. This researcher used questionnaires and interview guides to collect data from a case study of respondents within the same setting and at the same time.

3.1.2 Research approach

According to Kothari (2008), this means the development of a theory or a pattern of meaning on the basis of the data that they have collected. The study used a phenomenological approach. This allowed the researcher to probe the richness of emotions and motivations related to the topic, as well as beliefs and attitudes towards electronic fraud and the performance of retail banking in Centenary bank. This study therefore adopted both the quantitative and qualitative approaches.

3.1.3 Research strategy.

According to Saunders (2003), research strategy is a general plan that helps the researcher in answering the research questions in a systematic way. As such, the study used a case study of Centenary bank. This helped the researcher to find up close and deep or rather detailed information in relation to the research topic.

3.1.4 Research Duration.

The study focused on five operational years, from 2012 to 2017 and data was be collected at one single point in time. The researcher believed that this is enough time to gather reliable information about the research variables. More so, this is the period within which the bank has suffered high cases of electronic fraud.

3.1.5 Research Classification.

According to Gossa (2016) , this means understanding of a specific kind of research that was used. This study used a highly descriptive and explanatory research whose process was made easy with the use of questionnaires and interview guides as instruments of data collection.

3.2 Population of the Study.

The researcher considered an accessible population of 500 respondents that was selected from the 4 branches of Centenary bank headquarters in Kampala, Mapeera House. The research population consisted of clients and staffs from the selected case study. The staff of the bank comprised the highest percentage of respondents. The two categories of respondents were targeted for the study because they are the stakeholders and key players in the retail banking of Centenary bank.

3.3 Sample Size of the Study

The research had a sample size drawn from the two categories of people identified as part of the population. This sample size was derived from the targeted 500 elements of the population using the Krejcie and Morgan's (1970) table appended at the end of this work. According to Krejcie and Morgan (1970), with a population of 500, a sample of 217 was considered sufficient. The distribution of the population was 10 Bank departmental Managers and assistant managers, 210, front officers and 47 Information technology (IT) department staff. However, through snow ball, 3 more respondents were interviewed. These were clients of the bank whose cases were still being investigated by police.

3.4Sampling Techniques

Three sampling techniques were employed by the researcher. First, the researcher used purposive sampling technique to select the key staffs from Centenary bank like the managers and assistant managers as well as the IT department staff. The front office staffs were sampled using the simple random technique. While the three interviewees were identified through snow ball technique.

3.5 Response Rate

The study targeted 217 respondents to provide the information of the study and 217 questionnaires were distributed to the respondents while three were interviewed, these composed the sample size of the study. Out of the 217 distributed questionnaires, 179 usable questionnaires were returned giving a response rate of 82.5% which was acceptable for the study according to Sekaran (2003).

3.6 Bio Data of Respondents

This section of the study discusses the characteristics of the respondents at Centenary Bank such as gender, age group and level of education. The researcher adopted frequency tabulations to present and discuss the results of the sample characteristics below. The rationale of using frequency tabulations was to ascertain the categories of the different characteristics in relation to the responses of the respondents. In order to summarize the results, figures were used by the researcher because it was another way of presenting the results in a summarized manner.

3.6.1 Descriptive Characteristics for Respondents

Frequency tabulation was used by the researcher to present gender, age group and level of education for the respondent distribution as shown in table 3.1 below.

Table 3.1 Descriptive characteristics of the respondents

Gender	**Frequency**	**Percentage**
Male	101	56.4
Female	78	43.6
Total	**179**	**100.0**
Age group		
21-30 years	17	9.5
31-40 years	84	46.9
41-50 years	53	29.6
51 years and above	25	14.0
Total	**179**	**100.0**
Highest level of Educ.	**Frequency**	**Percentage**
Diploma	66	36.9
Bachelor's Degree	87	48.6
Others	26	14.5
Total	**179**	**100.0**

Source: Primary data 2018

The results in the table 3.1 on gender distribution showed that 56.4% of the respondents were male whereas 43.6% were female as shown in the table above. From the results it is clear that the male respondents were more responsive compared to their female counterparts.

In regard to age group distribution as per table 3.1, 46.9% of the respondents were in the age-group of 31-40 years, 29.6% were under the 41-50 years age group, 14% were in the 50 years and above age group and 9.5% were in the 21-30 years age group. This is implication that the majority of the respondents were young adults. This is the case because Uganda's population is composed of more youth than other categories of gender and therefore the youth compose the larger portion of the institution workforce. This explains the high composition of the young adults.

From the results on the table 3.1, on respondents' level of education, the results showed that 48.6%of the respondents had attained degree and 36.9% had attained diploma level of education whereas,14.5% possessed other qualifications. The results provide confirmation that information was acquired from respondents who possessed the ability to read and process the contents of the questionnaire and thereafter provided the suitable answers. Therefore, data was collected from respondents who had the capability to provide the required information for the study.

3.6.2 Empirical Findings

The findings in this study are based on the study hypotheses which included significant influence of electronic fraud on retail banking performance; ATM fraud, internet fraud banking and mobile fraud and how they significantly affect retail banking performance. The variables were measured using a five point Likert scale and the results are presented in item means of responses under each variable.

The results are further explained using the Pearson correlation matrix in order to show relationships between the study variables whereas, to study the predictive power of the dimensions of electronic banking fraud (ATM banking, internet banking and mobile banking) on retail banking performance, a regression analysis was carried out. The results from the quantitative source are compared with qualitative ones. Statistical tables were used for easier understanding and interpretations.

3.7 Sources of Data

3.7.1 Primary Data

The primary data was collected using questionnaires and interview guides.

3.7.2 Secondary Data

The researcher consulted several secondary sources such as journals, documents, newspapers, and unpublished dissertations, the internet, and any other literature on electronic banking fraud and the financial performance of retail banks.

3.8 Methods of Data Collection

The study employed two methods of data collection namely questionnaire survey and interviewing.

3.8.1 Questionnaire Survey Method

The main methodized in this study was the questionnaire survey method. This method was used to collect data from the clients of the bank. The questionnaire method was used because the purpose of the study was to find out the effect of electronic fraud on retail banking performance, thus requiring a lot of information from many respondents. Such information can best be tapped on a closed ended questionnaire which allows for easy analysis to quantify the influence of the independent variable on the dependent variables as observed by Amin (2005). Secondly the use of questionnaires allowed the respondents to fill the questionnaires at their own convenient time. It also allowed respondents to express their views and opinions without fear of being victimized as suggested by Oso and Onen (2008).

3.8.2 Interviewing

The other method that was used by the researcher was interviewing. The researcher conducted semi- structured interviews with selected staff from the selected case study. The semi-structured interviews helped the researcher in collecting systematic, comprehensive and in-depth information on how the performance of retail banking in Centenary Bank is affected by electronic bank fraud.

3.9 Data Collection Instruments

The instruments that were used in this study included self-administered questionnaires and interview guides.

3.9.1 Self-Administered Questionnaire

The researcher employed a questionnaire as a tool of data collection to collect quantitative data from the respondents. The questionnaire was divided into two parts. Part one focused on the demographic characteristics of the respondents. Part two was further subdivided into four sections. Section A was about ATM fraud, section B focused on the extent of internet fraud, section C was about the extent of mobile fraud while section Dmeasured the performance of the retail banking of Centenary bank. The questionnaires were close ended. Closed ended questions were developed to help respondents make quick decisions; in addition, a Likert scale of 1-5 (1 for Strongly Disagree, 2 for disagree, 3 for Not sure, 4 for Agree, 5 for Strongly Agree)responses helped the researcher code the information easily for subsequent analysis and narrowing down the error gap while analyzing data as observed by Sekaran (2003). The questionnaires were self-administered and were distributed to the clients by the researcher with the help of two research assistants.

3.9.2 Interview Guide

A semi-structured interview guide was constructed by the researcher to guide the process of conducting interviews with the selected bank staff. The guide had a total of nine general questions on the causes and impact of electronic fraud and retail banking performance.

3.10 Quality Management of Data

Under this section, the researcher presents the measures that were undertaken to ensure validity and reliability of the data collected for this study.

3.10.1 Validity of the Research Instrument

Validity is the property of research instruments that measures the relevance, precision and accuracy (Sarantakos, 2005). Validity refers to the extent to which a measurement procedure actually measures what it is intended to measure rather than measuring something else, or nothing at all (Amin, 2005). The researcher used content validity because it focuses on how the content corresponds to the objectives of the study. To ensure validity the research instruments were given to three experts who were requested to score the relevance of each question in providing answers to the study. After which a content validity index (C.V.I) was computed using the formula:

CVI = No. of relevant items considered relevant by all the raters
Total No of items in the questionnaire

Validity of the instrument was obtained using the Content Validity Index (CVI) as presented in the table below.

Table 3.2: Validity Test

Variable Number of Items Content Validity Index

ATM bank fraud	9.0	. 890
Internet bank fraud	9.0	.

		803
Mobile bank fraud	9.0	.829
Retail bank performance	9.0	.770

Source: primary data (2018)

The computed CVIs for the different items all of them scored above 0.7 shows that they met the acceptable standards (Amin, 2003). From the results all the Content Validity Indices ranged from .770 to .890, therefore meeting the acceptable standards.

3.10.2 Reliability of the Research Instrument

Reliability refers to the consistency or dependability of measuring instrument. In order to ensure reliability of the tool, a pre-test of the instrument was done on a total of 50 clients from Centenary Bank, Kawuku Branch. Data from the pre-test was entered into the computer and analyzed using the SPSS program to test for reliability using the Cronbach's Alpha coefficient. Cronbach Alpha Reliability Coefficient enabled the researcher to adjust the instrument for consistency. With an alpha value above 0.7, the instrument was considered reliable as suggested by Craswell (2011). This was accompanied by the guidance from the research supervisor. The instrument is valid if Cronbach Alpha Coefficient is above 0.7. The researcher used Alpha co-efficient to establish the Degree to which the questions were internally consistent.

Table 3.3: Validity Test

Variable Number of Items Cronbach Alpha Value

ATM banking	9.0	.807
Internet banking	9.0	.842
Mobile banking	9.0	.800
Retail banking performance	9.0	.793

Source: primary data(2018)

According to Cronbach (1950), coefficient alpha of 0.7 and above is considered adequate. From the results all the Cronbach alpha coefficients ranged from .793 to .842, therefore meeting the acceptable standards.

3.11 Data Collection Procedure

After approval of the proposal, the researcher obtained a letter of introduction from the School of Business administration. This letter was presented to the bank manager of Centenary bank Mapeera House in order to seek permission for carrying out the study with their clients and staff. After securing the permission from the bank managers, the selection of respondents followed. Upon identifying the respondents questionnaires were distributed and interviews conducted. The completed questionnaires were collected by the researcher as soon as they were filled to avoid loss or displacement. After collecting data, the activity that followed was data processing and analysis, which were done in line with the purpose and objectives of the research plan.

This involved checking questionnaires for completeness, coding, entry and analysis. This was essential for a scientific study and for ensuring that all data is relevant for making contemplated comparisons and analysis. As Kothari (2004) notes, processing means editing, coding, classifying and tabulation of collected data so that they were adaptable to analysis. Therefore, the researcher proceeded to process and analyzes the collected data basing on the objectives of the study.

3.12 Data Analysis

3.12.1 Analysis of Quantitative Data

The statistical package which was used for analysis of data in this study was the Statistical Package for Social Sciences (SPSS) software. The statistical techniques that were used in the analysis were descriptive statistics, and regression analysis. Simple descriptive statistics like frequency counts and percentages were used to document the demographic information of the respondents. Item means and standard deviations were used to document the existence of electronic banking and correlation analysis was used to present the results of the study objectives. Linear regression analysis was used to determine the combined effect of the dimensions used to measure electronic fraud on retail banking performance.

3.12.2 Analysis of Qualitative data

Qualitative data was analyzed using content analysis. Responses from key informants were grouped into recurrent issues. The recurrent issues which emerged in relation to each guiding question was presented in the results, with selected direct quotations from participants being offered as illustrations.

3.13 Reseach Ethical Considerations

Confidentiality was regarded very seriously in this study. The respondents were assured that all the data collected will be used for study purposes only. The researcher respected all the rights and privacy of respondents. The information received was concealed and the dignity of persons was kept in secret unless on request to be published. That is to say, the rights, interests and sensitivities of the respondents were safeguarded by the researcher. If the respondents would want to know any information from the researcher, it would be granted. There was no exploitation or harming of the respondents.

3.14 Limitations of the Study and their delimitations.

Some employees were not willing to be interviewed. However, this was solved by persuading them. There was anticipated resistance from the management of the bank because of suspicion. However, after much explanation and negotiation with the managers, they realized the research once completed would be used by them to understand the challenges of electronic fraud and how to minimize its implications. An introductory letter from the university administration was taken to the bank and permission was granted. There was a problem of scanty literature that delayed the process of the study.

CHAPTER FOUR

ATM FRAUD AT CENTENARY BANK LIMITED

5.0 Introduction

This section gives a description of research objective one: To find out the effect of ATM fraud on retail banking performance in Centenary bank. This was assessed using a variety of questions as shown in section II of the instrument. Respondent self-rated ATM fraud using 9 Likert items. The resulting summary statistics are shown in Table 4.1.

Table 4.1 Descriptive statistics on ATM Fraud a Centenary Bank

Item	**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
						N = 76	
I frequently use my ATM card and I have not encountered any problem in using it.	22 (28.9%	49 (64.5%)	5 (6.6%)	00	00	1.78	0.56
I am suspicious about my ATM account information	00	19 (25.0%)	54 (71.1%)	3 (3.9%)	00	2.79	0.50
I am aware of ATM fraud activities	5 (6.6%)	12 (15.8%)	4 (5.3%)	31 (40.8%)	24 (31.6%)	3.75	1.24
I have ever lost money to ATM fraud	3 (3.9%)	14 (18.4%)	8 (10.5%)	32 (42.1%)	19 (25.0%)	3.66	1.16
I have had complaints about ATM fraudulent from other people.	4 (5.3%)	14 (18.4%)	9 (11.8%)	30 (39.5%)	19 (25.0%)	3.61	1.20
ATM fraud is common in centenary bank	7 (9.2%)	11 (14.5%)	7 (9.2%)	28 (36.8%)	23 (30.3%)	3.64	1.30
ATM services at centenary bank are secure and safe	8 (10.5%)	10 (13.2%)	8 (10.5%)	26 (34.2%)	24 (31.6%)	3.63	1.34
Transacting bank services using ATM is risky	6 (7.9%)	10 (13.2%)	4 (5.3%)	35 (46.1%)	21 (27.6%)	3.72	1.23
When I lose my ATM I get so much worried about the safety of my money in the bank.	6 (7.9%)	9 (11.8%)	2 (2.6%)	36 (47.4%)	23 (30.3%)	3.80	1.22

Source: Primary data (2018)

The majority of respondents agreed that they were aware of ATM fraud activities (mean=3.75), they had had complaints about ATM fraudulent from other people (mean=3.61), frequently used their ATM card and had not encountered any problem in using them (mean=1.78), were suspicious about their ATM account information (mean=2.79) and had ever lost money to ATM fraudulent(mean=3.66). They also revealed that when they lost their ATMs, they got so much worried about the safety of their money in the bank (mean=3.80) and transacting bank services using ATM was risky (mean=3.72). This was also supported by some key informants who revealed that;

"ATM banking fraud is prevalent in the operations of the bank and the both the bank and customers are victims of this type of fraud."

One respondent said;

"I know about the existence of ATM banking, although the bank needed to do more to protect customers from being affected by this vice."

It was also revealed by one respondent that;

"Fraudsters were riding on the ignorance of the customers to defraud them out of ignorance and the fraudsters included staff, friends, relatives and sympathizers."

From the results, the standard deviation result of greater than 1 is proof that ATM fraud influences retail banking performance at the bank. Likewise, the standard deviation results provided evidence that the results obtained on ATM banking could be applied to the bank and therefore could be generalized on other commercial banks in Uganda. The general view from the results is that the results on ATM fraud as an electronic fraud at the bank provided confirmation that there was some level of ATM fraud at the bank. This implies that continued ATM fraud would eventually affect retail banking performance at the bank.Testing of hypothesis one: There is no significant relationship between ATM fraud and retail bank performance at Centenary Bank Ltd

Table 4.2 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.620[a]	.384	.376	5.92746

a. Predictors: (Constant), B1

The model summary table (Table 4.2) indicates that there is a significant positive relationship between ATM fraud and retail banking performance (r = 0.620). The actual contribution of ATM fraud to retail banking performance is about 38% (Adj. R Square = 0.376).

These results indicate that ATM banking as a financial service promoted the electronic services provided by Centenary bank and in the process improved the retail banking performance at the bank. Therefore, when the bank is able to enhance the level of ATM banking in the bank's electronic operations, this will enhance retail banking performance. However, with the level of fraud showed above, top executives such as the executive committee members, top managers and heads of departments must do their job to make sure that supervision and control of electronic services is effective under all levels of management of the ATM activities. They should remember that ATM banking is paramount in promoting retail banking performance in the ever changing dynamic environment, the financial sector that requires key players to have a competitive advantage so as to thrive in the global market.

Table 4.3AnovaAa

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	1622.677	1	1622.677	46.184	.000[b]
	Residual	2599.976	74	35.135		
	Total	4222.653	75			

a. Dependent Variable: C
b. Predictors: (Constant), B1

The ANOVA results show that there is significant linear relationship between ATM fraud and retail banking performance (F = 46.184, P< 0.005). This implies that the more of ATM fraud, the worse the performance of retail banking.

Table 4.4 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	8.675	2.337		3.712	.000
	B1	.407	.060	.620	6.796	.000

a. Dependent Variable: C

The coefficients table (Table 4.4) gives the model that relates ATM fraud to retail banking performance. The regression model generated was: $C = 8.675 + 0.407B_1$ (where: C= Retail banking performance and B_1 = ATM fraud).

CHAPTER FIVE

INTERNET FRAUD AT CENTENARY BANK LIMITED

Introduction

This section gives a description of research objective two: To establish the effect of Internet fraud on retail banking performance in Centenary bank. This was assessed using a variety of questions as shown in section III of the instrument. Respondent self-rated internet banking using 9 Likert items. Responses were based on Likert scale ranging from strongly disagree (1) to strongly agree (5), although these were subsequently categorized into agree and disagree sections. The resulting summary statistics are shown in Table 5.1.

Table 5.1 Descriptive statistics on internet fraud at Centenary Bank

Item	**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
						N = 179	
The bank allows customers to obtain consolidated information about their accounts status via internet	6 (7.9%)	8 (10.5%)	11 (14.5%)	35 (46.1%)	16 (21.1%)	3.62	1.17
The bank allows customers to obtain consolidated information about their non-financial accounts	9 (11.8%)	7 (9.2%)	13 (17.1%)	32 (42.1%)	15 (19.7%)	3.49	1.28
There is training offered to clients on how to use the services online	7 (9.2%)	10 (13.2%)	7 (9.2%)	35 (46.1%)	17 (22.4%)	3.59	1.23
Our bank provides on-line tutorials for new e-banking users	6 (7.9%)	12 (15.8%)	3 (3.9%)	37 (48.7%)	18 (23.7%)	3.64	1.23
Our Bank protects customers information from intruders	5 (6.6%)	10 (13.2%)	4 (5.3%)	36 (47.4%)	21 (27.6%)	3.76	1.19
The government is directly involved to manage internet banking security	4 (5.3%)	8 (10.5%)	11 (14.5%)	35 (46.1%)	18 (23.7%)	3.72	1.10
Clients are informed of the possibility of internet banking fraud	6 (7.9%)	8 (10.5%)	10 (13.2%)	35 (46.1%)	17 (22.4%)	3.64	1.17
Customers are told how to deal with Internet fraud in case it comes up	7 (9.2%)	5 (6.6%)	21 (27.6%)	31 (40.8%)	12 (15.8%)	3.47	1.13
Our Bank is able to detect fraudulent e-banking system activities	6 (7.9%)	5 (6.6%)	10 (13.2%)	39 (51.3%)	16 (21.1%)	3.71	1.12

Source: Primary data (2018)

Basing on the study results in Table 5.1, the majority of the respondents agreed that the bank allowed customers to obtain consolidated information about their non-financial accounts (mean=3.49), protected customers' information from intruders (mean=3.76), the government was directly involved in managing internet banking security (mean=3.72), clients were informed of the possibility of internet banking fraud (mean=3.64) and the bank was able to detect fraudulent e-banking system activities (mean=3.71). In line with the qualitative results on internet banking fraud above, the results from the interviews affirmed that;

"customers had access to electronic information, the bank and other stakeholders were involved in managing internet fraud, provided training to staff and clients about internet banking among other things".

On the other hand, the bank allowed customers to obtain consolidated information about their finances (mean=3.49), the bank provided on-line tutorials for new e-banking users (mean=3.64), customers were told how to deal with internet fraud in case it comes up (mean=3.47) and there was training offered to clients on how to use the services online (mean=3.59). One respondent indicated that;

"e-banking was a new phenomenon which was being gradually being embraced by customers, although this was being hampered by the availability of ICTs that support e-banking."

The research found out that e-banking was mostly used by public and private institutions to carry out transactions such as electronic funds transfer. This was supported by one of the respondent who revealed that;

"there was growing use of e-banking at the bank although the bank needed to create more awareness about e-banking so that its advantages can be appreciated by the general public. Much as globalization was forcing the business/private sector to embrace e-banking so as to be able to transact across the globe. "

This is justification that the management of the bank ensured that both clients and staff were given the required training on internet banking and how fraud could occur during work processes at the bank. From the results, the standard deviation result of less than 1 is proof internet banking determined electronic banking fraud at the bank. Likewise, the standard deviation results provided evidence that the results obtained on internet banking could be applied to the bank and therefore could be generalized on other commercial banks in the country.

Testing of hypothesis two: Electronic fraud does not significantly affect retail-banking centenary

In order to establish the exact explanation of the variation in retail banking performance due to internet fraud, correlations and regression were run and the following is a discussion of the results.

Table 5.2 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.566[a]	.320	.301	5.65843

a. Predictors: (Constant), B2

Results in the model summary table above indicate that there is a significant positive relationship between internet fraud and retail banking performance (r = 0.566). The same table shows that about 32% of the variation in retail banking performance is explained by vendor internet fraud (Adj. R Square = 0.301)

Table 5.3ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
	Regression	1853.332	1	1853.332	57.884	.000[b]
1	Residual	2369.321	74	32.018		
	Total	4222.653	75			

a. Dependent Variable: C
b. Predictors: (Constant), B2

The results in the ANOVA Table show that there is a significant linear relationship between internet fraud and retail banking performance (F = 57.884, P<0.005).

Table 5.4Coefficient

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		

1	(Constant)	-1.520	3.400		-.447	.656
	B2	.353	.046	.662	7.608	.000

a. Dependent Variable: C

The coefficients Table generates the regression model between internet fraud and retail banking performance to be: $Y = -1.520 + 0.363B_2$ (where: C = retail banking performance, and B_2 = internet fraud). Results of less than zero indicate that when the bank had the necessary procedures to promote internet banking, this would make it easy for the bank to manage electronic banking and in turn improve its retail banking performance. The results imply that if the bank put in place favorable internet banking strategies to develop the required controls in order to eliminate fraud , this would have a positive effect on its retail banking performance.

CHAPTER SIX

MOBILE FRAUD AT CENTENARY BANK LIMITED

Introduction.

This section gives a description of research objective three: To examine the effect of Mobile fraud on retail banking performance in Centenary bank. This was assessed using a variety of questions as shown in section IV of the instrument. Respondent self-rated mobile banking using 9 Likert items. Responses were based on Likert scale ranging from strongly disagree (1) to strongly agree (5), although these were subsequently categorized into agree and disagree sections. The resulting summary statistics are shown in Table 6.1

Table 6.1 Descriptive statistics on mobile fraud at Centenary Bank.

Item	**SD**	**D**	**N**	**A**	**SA**	**Mean**	**Std. Dev.**
						N = 76	
The mobile secret code or PIN number is known by me alone	2 (2.6%)	11 (14.5%)	13 (17.1%)	33 (43.4%)	17 (22.4%)	3.68	1.06
I am confident that my money is safe even if I lose my phone	1 (1.3%)	15 (19.7%)	8 (10.5%)	39 (51.3%)	13 (17.1%)	3.63	1.03
I am able to verify my account details before any transactions are made	3 (3.9%)	15 (19.7%)	14 (18.4%)	33 (43.4%)	11 (14.5%)	3.44	1.09
I have received suspicious SMS on ongoing promotions by fraudsters claiming to be bank officials	3 (3.9%)	13 (17.1%)	9 (11.8%)	34 (44.7%)	17 (22.4%)	3.64	1.13
I have received calls claiming that I have won money from the bank	1 (1.3%)	19 (25.0%)	17 (22.4%)	29 (38.2%)	10 (13.2%)	3.37	1.04
I have received messages claiming wrong transfer of money to my account	2 (2.6%)	12 (15.8%)	15 (19.7%)	35 (46.1%)	12 (15.8%)	3.56	1.02
Some bank staff collude with fraudsters to access customers' accounts	4 (5.3%)	16 (21.1%)	12 (15.8%)	33 (43.4%)	11 (14.5%)	3.41	1.13
I have ever been charged more transaction fees than the normal bank charges	3 (3.9%)	12 (15.8%)	12 (15.8%)	30 (39.5%)	19 (25.0%)	3.66	1.14
Fraudsters have ever used my transaction code to withdraw funds from my account	9 (11.8%)	11 (14.5%)	11 (14.5%)	27 (35.5%)	18 (23.7%)	3.45	1.32

Source: Primary data (2018)

From the results in Table 6.1, there was agreement that the respondents were confident that their money was safe even if they lost their phones (mean=3.63), some bank staff colluded with fraudsters to access customers' accounts (mean=3.41) and they had received suspicious SMS on ongoing promotions by fraudsters claiming to be bank officials (mean=3.64). In support of the above results, some heads of departments attested that;

"Mobile money was used by customers to make transactions whether banking, payments or drawing money off accounts by customers. However, much as it made transactions more convenient, it also came with a lot of risks which fraudsters used to defraud customers".

The results further revealed that their mobile secret codes or PIN numbers were known by them alone (mean=3.68), they were able to verify their account details before any transactions were made (mean=3.44), had received calls claiming that they had won money from the bank (mean=3.37) and received messages claiming wrong transfer of money to their accounts (mean=3.56). In line with the quantitative results on mobile banking fraud above, the results fromthe interviews affirmed that;

"Fraudsters sent wrong information to customers through suspicious SMS on ongoing promotions, received calls claiming that they had won money from the bank and received messages claiming wrong transfer of money to their accounts".

This is capable of engendering more fraud. From the results, the standard deviation results of greater than 1 provided evidence that the results obtained on mobile banking applied to the bank and therefore could be generalized on other commercial banks that offer financial services in the country.

Testing of hypothesis three: There is no significant relationship between mobile fraud and retail banking performance

In order to establish the variation in retail banking performance that is explained by mobile fraud, correlation and regressions were run and the following is a discussion of the results.

Table 6.2 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.576[a]	.331	.312	5.49573

a. Predictors: (Constant), B3

The model summary table indicates that there is a significant relationship between mobile fraud and retail banking performance (r = 0.576). The Adjusted R Square of 0.312 indicates that about 31% of the variation in retail banking performance is explained by mobile banking and the associated fraud.

Table 6.3 ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1987.628	1	1987.628	65.809	.000[b]
	Residual	2235.025	74	30.203		
	Total	4222.653	75			

a. Dependent Variable: C
b. Predictors: (Constant), B3

The ANOVA table indicates that there is a significant linear relationship between mobile fraud and retail banking performance (F = 65.809, P<0.005). This means that at Centenary bank electronic fraud associated with the use of mobile phones as relatively high. Such fraud is committed mainly to the unsuspecting customers from either the bank fraudsters or even fellow customers who take advantage of the available information from their victims.

Table 6.4 Coefficient

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.075	3.000		.025	.980
	B3	.309	.038	.686	8.112	.000

a. Dependent Variable: C

The coefficients Table results imply that one unit increase in retail bank performance is contributed by 0.86 units, basing on the equation: C = 0.075 + 0.309B_3 (where: C = retail banking performance and B_3 = mobile fraud).This is indicative of the fact that proper management of mobile banking is essential for a corresponding improvement in retail banking performance. And when this is done, therefore, a positive change in mobile banking will enhance retail banking performance at Centenary bank. This position was also shared by top executives such as the executive committee members, top managers and heads of departments who revealed that mobile banking at the bank was paramount in promoting efficiency, growth in customer base and brand equity.

CHAPTER SEVEN

HARMONIZATION OF ELECTRONICFRAUD AND RETAIL BANK PERFORMANCE OF CENTENARY BANK LIMITED

7.0 Introduction

This section explains whether there is a relationship between electronic fraud and retail bank performance at Centenary Bank. A model summary, analysis of variance and a multiple regression table were used to test the general hypothesis of the study. A discussion on the findings of the study is also done under this section in relation to the available literature reviewed in chapter two, the theories and models as well as personal critiques for and against the existing literature. It is from here therefore that areas for further research are drawn

Table 7.1 Electronic fraud AND RETAIL BANKING PERFORMANCE

Statement	**Strongly agree**		**Agree**		**Not sure**		**Disagree**		**Strongly disagree**	
	Freq	**%**	**Freq**	**%**	**Freq**	**%**	**Freq**	**%**	**Freq**	**%**
Customer's numbers keep increasing	10	33.3	15	50	1	3.3	2	6.7	2	6.7
Customers trust the bank that they are free from fraud.	13	43.3	11	36.7	00	00	3	10	3	10
There are always deposit services in all branches of the bank.	17	56.7	8	26.7	2	6.7	3	10	00	00
There are always withdraw services in all the branches of the bank.	9	30	11	36.7	1	3.3	5	16.7	4	13.3
The bank's mobile technology is always up to date.	11	36.7	12	40	4	13.3	2	6.7	1	3.3
Customers access all they need at the time they need the services.	10	33.3	13	43.3	5	16.7	1	3.3	1	3.3

Source: *Primary Data 2018*

Table 7.1 shows that 33.3% strongly agreed that, 50% as the majority agreed, 3.3% were not sure, 6.7% disagreed, and 6.7% strongly agreed. This implies that the bank, always experience a steady increase in the level of customers opening accounts at the bank.

According to the findings, 43.3% of the respondents strongly agreed that, 36.7% agreed, 10% disagreed, and also 10% strongly agreed. This implies that the bank always benefits from the trust entrusted in them by their customers regarding their safety.

The findings show that the majority of respondents (56.7%) strongly agreed, 26.7% agreed, 6.7% were not sure, and 10% disagreed. This strongly implies the bank has continually provided deposit services to its customers in all the branches.

According to table 7.1, 30% of the respondents strongly agreed that, 36.7% agreed, 3.3% were not sure, 16.7% disagreed, and 13.3% strongly disagreed. This implies that the bank has continually provided withdraw services to its customers in all the other branches of the bank.

Table 7.1 above shows that 36.7% of the respondents strongly agreed, 40% agreed, 13.3% were not sure, 6.7% disagreed and 3.3% strongly disagreed. This implies that the bank ensures that it updates its technology on behalf of its customers all the time.

The table also shows that 33.3% strongly agreed, 43.3% agreed, 16.7% were not sure, 3.3% disagreed, and 3.3% strongly disagreed. This implies that the bank makes sure all its customers continue accessing its services whenever they need to transact business with the bank. This practice indicates a steady increase in the level of profits due to service availability.

7.1 Testing of the general hypothesis:H1- There is no significant relationship between Electronic fraud and retail bank performance at Centenary Bank Limited

In order to establish the combined effect of the three constructs of e-banking fraud (i.e. ATM fraud, internet fraud and mobile banking fraud) on retail bank performance, multiple correlation and regression analysis was run and the following is a discussion of the results.

Table 7.2 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.648[a]	.420	.392	5.07920

a. Predictors: (Constant), B1, B2, B3

The model summary table indicates that there is strong positive relationship between electronic fraud and retail bank performance (R = 0.648). About 39% of the variation in retail banking performance is explained by e-banking fraud, implying that 61% of the variation in retail banking performance is explained by other factors that were out of the scope of this study like poor customer care, a weak risk management team at Centenary Bank, high levels of electronic illiteracy with the customers, failure to name, shame and punish the culprits, to mention but a few. The above does not differ from the Fraud Triangle Model by Cressey (2000) and the fraud diamond model by Herman son (2004). The authors of the model argue that, in order to add to

the factors that cause fraud. The variables of pressure/ motive, opportunity rationalization and capabilities, mainly by the staff of the bank, fuel the urge to commit bank fraud. In addition;
why people commit fraud was first examined by Cressey Donald, a criminologist in 1950. His research was about what drives people to violate trust. He interviewed 250 criminals over a period of 5 months whose behaviors met two criteria:

(iii) The person must have accepted a position of trust in good faith, and

(iv) He must have violated the trust (Rasha and Andrew, 2012).

Cressey was especially interested in the circumstances that lead to otherwise honest people to get overcome by opportunity and temptation to commit fraud when the environment is ripe for fraud.

He found that three factors must be present for a person to violate trust and was able to conclude that: "trust violators when they conceive of themselves as having a financial problem which is non-sharable, have knowledge or awareness that this problem can be secretly resolved by violation of the position of financial trust and are able to apply to their own conduct in that situation, verbalization which enable them to adjust their misconceptions of themselves as users of the entrusted funds and property. If these are not taken care of in the banking sector, performance will not be revamped.

Table 7.3ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	2365.176	3	788.392	28.360	.000[b]
	Residual	1857.477	72	25.798		
	Total	4222.653	75			

a. Dependent Variable: C

b. Predictors: (Constant), B3, B1, B2

The ANOVA results indicate that there is a significant positive relationship between e-banking fraud and retail banking performance (F = 28.360, P<0.005). Therefore, the null hypothesis that there is no significant relationship between electronic fraud and retail banking performance is rejected and the alternative was accepted.

This is in agreement with Darlington (1999). He says that; indeed, despite concerted efforts to stabilize performance, many retail banks are still plagued by long cycle times, inconsistent channel experiences and generic customer propositions. Unless they make deeper, bolder changes, profitability and competitiveness will suffer.

Banks can make these changes and substantially improve performance by more efficiently and effectively fusing digital functionality with personalized, human interaction in other words, by becoming more bionic (Gates and Jacob, 2009). A bionic transformation includes blending digital and personal interactions to create a more responsive and cost-effective distribution model, articulating a value proposition that combines human judgment with data power, and adopting a customer journey mindset with end-to-end processes that are supported by robotics and machine learning.

Table 7.4 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-2.173	3.154		-1.323	.190
	B1	.152	.069	.242	2.289	.025
	B2	.102	.062	.285	2.440	.017
	B3	.113	.056	.323	2.616	.011

a. Dependent Variable: C

The coefficients table gives the multiple regression model generated from the survey: $C = -2.173 + 0.152B_1 + 0.102B_2 + 0.113B_3$ (where: C = Retail banking performance; B_1 = ATM fraud; B_2 = internet fraud; and B_3 = mobile fraud).

According to Table 7.4, the most significant predictor of retail banking performance was ATM fraud (0.152) followed by mobile fraud (0.113) and then followed by internet fraud (0.102). The findings revealed that ATM banking, internet banking and mobile banking were strong predictors of retail banking performance. Providing evidence that for the bank to attain desirable efficiency, growth in customer base and brand equity there was need to ensure that ATM banking, internet

banking and mobile banking is reduced at the bank. This is in agreement with (Kanu & Okarafor, 2013) who argue that since the introduction of ATM in the early
1970s, perpetrators have been working hard to find ways of how to steal cash from the machines. Not to leave out the words of Owolabi (2010) who noted that the problem of ATM fraud in the retail banking sector is not limited to any economy, nation, continent or environment. These kinds of losses pose a significant threat to banks considering their roles in the economy. He adds that the relationship between banking efficiency and the use of ATM is complex. The overall level of efficiency and productivity greatly influence the organization overall success and in this particular study, the overall retail banking performance.

On the other hand, the intention with internet banking was initially that, customers would enjoy sitting in the comfort of their homes and offices and with a Personal Computer, log onto their banks' servers and transact banking activities. however, the fact that majority of the banking population have not yet trusted the use of internet, its use is still very low compared to mobile and ATM banking thus the low level of influence (Douglass, 2009). Each financial institution should therefore apply guidelines based on its scope and level of sophistication in e-banking technology in order to improve its usability to the intended customers. However, it should not be forgotten that; typically, electronic banking amplifies the scale of exposure of banks to traditional risks, such as transaction, strategic, reputation and compliance risk, among others.

CHAPTER EIGHT

SUMMARY OF FINDINGS, DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

8.0 Introduction

This chapter presents the discussion of results presented in chapters four and conclusions drawn from the presentation. The chapter presents a short summary of the purpose of the study and the research findings, followed by the set of recommendations, limitations of the study and areas of further research.

8.1 Summary of the Findings

The study sought to examine the extent to which electronic banking contributed to retail banking performance at the bank. This was carried out by unpacking the dimensions of electronic banking which are: ATM banking, internet banking and mobile banking. These were related with retail banking performance when developing the study objectives.

8.1.1 ATM Banking and Retail Banking Performance

The findings validate that, ATM banking was significant in determining retail banking performance. This was confirmed by the findings from the management staff who were the key informants and the correlation results which indicated a significant and positive relationship between ATM banking and retail banking performance.

8.1.2 Internet Banking and Retail Banking Performance

According to the findings, there was a positive and significant relationship between internet banking and retail banking performance. The positive significant relationship between internet banking and retail banking performance was confirmation that in order to realize efficiency, growth in customer base and brand equity at the bank there was need to manage internet banking during electronic banking.

8.1.3 Mobile Banking and Retail Banking Performance

The findings established that mobile banking influenced retail banking performance at bank which was implication that proper management of mobile banking was paramount in promoting retail banking performance. The positive significant relationship between mobile banking and retail banking performance was explained by the fact that in order to attain efficient retail banking performance, there was a need to ensure that there is effective control of mobile banking at the bank

8.2 Discussion of the Findings

A discussion of the findings was carried out following the study objectives. Here the researcher assessed how the findings of the study were in agreement or disagreement with extant literature that was reviewed.

8.2.1 ATM Banking and Retail Banking Performance

The findings revealed that ensuring proper ATM banking in regard to awareness of ATM fraud activities would result into improved retail banking performance at the bank. This is supported by Onuorah and Ebimobowei (2012) who revealed that the introduction and use of Automated Teller Machine (ATM) is not only safe but also convenient. However, this has been lessened by the frauds that are perpetrated by ATM fraudulent. According to Wilhem (2004), ATM banking and fraudulent activities greatly affects the banking sector. Owolabi (2010) noted that the problem of ATM banking fraud in the retail banking sector is not limited to any economy, nation, continent or environment. These kinds of losses pose a significant threat to banks considering their roles in the economy. The overall level of efficiency and productivity greatly influence the organization overall success. The achievement, goals, profit and attainment of retail banking sector depend largely on proper management and technology like ATM (European ATM Crime Report, 2007).

This implied that emphasis on ATM banking would enhance retail banking performance at the bank.

8.2.2 Internet Banking and Retail Banking Performance

The findings showed that promoting internet banking at the bank translated into efficient retail banking performance at the bank. To promote internet banking, the bank should allow customers to obtain consolidated information about their non-financial accounts, protect customers' information from intruders and inform clients about the possibility of internet banking fraud. In support of the findings, Berney (2008) showed that customers rely heavily on the web for their banking business, leading to an increase in the number of online transactions. Fraudsters react to these changes as the inter net provides them with more opportunities to attack customers (Gates and Jacob, 2009). Orad (2010) revealed that the internet allows criminals to organize as a network, supporting each other in their attacks. This is justification that the management of the bank ensured that both clients and staff were given the required training on internet banking and how fraud could occur during work processes at the bank.

8.2.3 Mobile Banking and Retail Banking Performance

The findings showed that through provision of mobile banking service by the bank ,along with a vigilant risk management team , other factors remaining constant is likely to improve the retail banking performance of the bank. In agreement with this notion, Mudiri (2014) opines that the key enablers of mobile banking fraud include but not limited to weak regulation, low consumer awareness levels and poor communication with the main players. Mudiri (2014) maintains that the introduction of mobile money services has greatly changed the dynamics of the industry, bringing financial services closer to the public. Munyoki (2015) states that mobile banking has the advantage of making basic financial services more accessible by minimizing time and distance to the nearest retail bank branches as well as reducing the banks' own transaction costs. Lee and Kim (2007) posit that mobile banking has a number of far reaching effects on retail banking performance.

8.3 Conclusions

The conclusions were drawn basing on the research objectives of the study. The findings substantiate that effective management of ATM fraud was vital in promoting retail banking performance of the bank. This implies that when proper ATM banking structures are put in place to curb the fraud associated with it, this would result improved efficiency, growth in customer base and brand equity. This is confirmation that reduction in ATM banking was vital in improving retail banking performance at the bank.

The findings on objective two revealed that there were still lapses in the management of internet Banking and its associated fraud at the bank. The positive significant relationship between internet fraud and retail banking performance is justification that to ensure efficiency, growth in customer base and brand equity during retail banking performance management, there was need to adhere to effective risk management in order to reduce internet fraud.

The findings validate that a reduction in mobile fraud was principal in promoting retail banking performance at the bank**.**

This implies that a positive change in mobile banking management and control would translate into improved retail banking performance. This is justification that proper control of mobile transactions was vital in improving the bank's effectiveness and efficiency.

In conclusion, the findings validate that proper management of electronic fraud and its associated risks regarding ATM transactions, internet transactions and mobile transactions was essential for the improvement of retail banking performance at the bank. This justified by the correlation findings which were in line with regression analysis findings confirming that electronic banking determined the efficiency, growth in customer base and brand equity at the bank.

8.3 Recommendations

In light of the research findings, the following main recommendations were made:

8.3.1 ATM fraud and Retail Banking Performance

The findings revealed that ATM fraud had a positive effect on retail banking performance at the bank. It is recommended the management of the bank should strengthen the existing ATM fraud channels by putting in place effective internal and external controls to manage ATM transaction risks. The implemented structures should be able to promote customer privacy and security by ensuring that customers' private information cannot easily be accessed by second parties (fraudsters) and also secure the ATM machines where the customers carry out the transactions. Customers should be clearly sensitized on how to operate the machines and the dangers of sharing their private information such as PIN numbers, secret codes with second parties so that they do not become victims of fraudsters.

8.3.2 Internet Banking and Retail Banking Performance

The findings revealed that internet fraud had a positive influence on retail banking performance. The findings of this study suggest that internet banking in bank operations was vital to the performance of the bank and therefore, there was need to put in place effective internal controls to monitor fraud arising from internet banking and being able to deter it so as to enhance the efficiency of the bank. Likewise, the management of the bank should put in place structures and procedures backed up by the required policy framework to identify causes of internet banking challenges so as cub its manifestation in electronic banking operations at the bank. Management should carry out regular updates of banking software and hardware so as to eliminate the possibility of fraudsters taking advantage of the loopholes in the old operating systems to defraud the bank or customers.

8.3.3 Mobile Banking and Retail Banking Performance

From the findings on mobile fraud and retail banking performance, it was revealed that putting in place the relevant structures to manage mobile banking and its associated risks was vital in promoting retail banking performance. The researcher recommends that the management of Centenary Bank should develop and put in place, procedures, systems and mechanisms that should be followed during the management and control of mobile banking as these will promote efficient and effective retail banking at the bank. This framework should have active participation from stakeholders and should be adhered to by management and staff as a means of creating a sense of responsibility among staff.

8.4 Areas for Further Study

The researcher only focused on four components, that is; ATM banking, internet banking and mobile banking not considering other dimensions used by other researchers to measure electronic banking. Each of these components has broad areas which can be researched on in relation to retail banking performance. Proposed areas for further research are;

Risk electronic banking and performance of corporal banking
Customer care and retention and the competitive advantage of commercial banks in Uganda
Internal controls and the profitability of commercial banking in Uganda.

REFERENCES

A Report on Global ATM Frauds (2007).
A Report on Global ATM Frauds (2007). Available online at http://www.icmrindia.org/casestudies/catalogue/Business%20Reports/BREP041.htm.

Abaasa F. (2007). Banking in Uganda Gone High Tech, Kampala Uganda.

Adeoti, J. A. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *Journal of Social Sciences*, 27(1): 53-58.

Adeoti, J.A. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *Journal of Social Sciences*, 27(1): 53-58.

Adepoju, A. and Alhassan, G. (2010).Challenges of automated teller machine (ATM) usage and fraud.

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

Aditi, O. (2013). Working of Automated Teller Machine (ATM). Available at http://www.techs24x7.com/blog/working-of-automated-teller-machine-atm/.

Akindele, R. I. (2010). Fraud as a negative catalyst in the Nigerian banking industry; *Journal of European Journal of social Sciences*, Vol. 10 (4)

Amin, E. M. (2005). Social Science Research Conception, Methodology and Analysis.Makerere University Printery: Kampala.

Asif Khan, M. (2011). An Empirical Study of Automated Teller Machine Service Quality and Customer Satisfaction in Pakistani Banks. *European Journal of Social Sciences*, 13 (3): 333-344.

Bank Limited. A Study of Ghana Commercial Bank Ltd, Ho Poly Technic Branch, Ph.D. Thesis, Institute

behaviour towards innovative retail services: the case of Internet banking. *Journal of Retailing and*

Buchanan, R. (2010). Banks on Guard.Latin Trade. Vol. 18 No. 5, pp. 58-60.

Cabas, M. G. (2001). A History of the Future of Banking: Predictions and Outcomes. Retrieved September 2, 2012, from http://www.hass.berkeley.edu/finance /CMWpaper.pdf.

case of Bank of Kigali. *European Journal of Accounting, Auditing and Finance Research*.Vol.3 No.4 pp.

Case Study of Selected banks in Minna Metropolis. *Journal of Internet Banking and Commerce* (JIBC),

Channel for Delivering Banking Services in Nigeria. *International Journal of Business and Management*, 7(4)68

Chung, W.C.C., A.Y.K. Yam, M.F.S. Chan. (2004). Networked enterprise: A new business model for global sourcing. International Journal of Production Economics 87 267-280.

Consumer Services. Vol. 13 (6), 431–443

Craswell, J. W. (2011). Educational Research: Planning, Conducting and Evaluating Qualitative and Quantitative Research. (4th edn). Boston: Pearson Inc.

Cressey D. (2000) Computer and Crime. 2nd Edition, Irwin McGrawHill Publication

Dapo, A. A. (2008). The impact of ICT on professional practice in the Nigerian construction industry.*The*

Dapo, A. A. (2008). The impact of ICT on professional practice in the Nigerian construction industry. The Electronic Journal of Information Systems in Developing Countries. 24(2), p1-19.

Douglass, D. B. (2009).An examination of the fraud liability shift in consumer card-based payment systems.*Economic Perspectives*. Vol. 33 No. 1, pp. 43-49.

Ebiringa, O. T. (2010). Automated Teller Machine and Electronic Payment System in Nigeria: A Synenthesis of the Critical Success Factors. *Journal of Sustainable Development in Africa*, 12 (1): 71-86.

Electronic Journal of Information Systems in Developing Countries. 24(2), 1-19.

Empirical Investigation in retail banking. *International Journal of Bank Marketing*.Vol.30 No. 5 pp. 390-407.

European ATM Crime Report (2011) The European ATM Security Team.

European Scientific Journal, Vol.9(7), pp.239-263

Gates, T. and Jacob, K. (2009). Payments fraud: perception versus reality – a conference summary. *Economic Perspectives*. Vol. 33 No. 1, pp. 7-15.

Giddens, E. (2008). A first look at communication theory. New York: McGraw Hill

Global ATM Market (2011). Retail Banking Research.BrochurePg 2.

Gruber, T. (2011). I want to believe they really care: how complaining customers want to be treated by frontline employees. *Journal of Service Management*. Vol. 22 No. 1, pp. 85-110

Harcourt, Nigeria. *Asian Journal of Business Management*, 4(2).

Herman son W. (2004) Internet and Online Crime .3rdEdition .Irwin McGraw Hill Publiation.

Hoffman, A. O. I. and Birnbrich, C., (2012). The impact of fraud prevention on bank-customer relationships: An

Idowu (2009). An assessment of fraud and its management in Nigeria commercial banks, occurrence in Nigeria-A

Ihejiahi R 2009. How to fight ATM fraud online. *Nigeria Daily News,* June 21, P. 18.

Ihejiahi, R. (2009). How to fight ATM fraud online. Nigeria Daily News, June 21, P. 18.

International Journal of Asian Social Science, 2(4), 35-45.

International Proceedings of Economics Development & Research, 43

ISSN: 2321-5933, p-ISSN: 2321-5925. Vol 2, Issue 3.

James, A. (2009). Boosting Payment Solution with visa Cards. Daily Champion, P.A.12.

James, O. (2009). E-payment and its Challenges. Daily Champion, P.A. 13.

Journal of Economic Crime Management Spring, 2004.2 (2).

Journal of Management.Vol.2 No. 98.Pp.1440-1457.

Kamara, T. R. and Bitek, O. P. (2011) Macroeconomics (Money, Banking and Public Finance), V.K. Global Publication, New Delhi.

Kanu, S. I. and Okoroa for, E. O. (2013). The Nature, Extent and Economic Impact of Fraud on Bank Deposit in

Keivani, F.S., Jouzbarkand, M., Khodadadi, M. and Sourkouhi, Z. K. (2012). A General View on the E-banking,

Kizito S. andMugole P.(2015) The Effectiveness of Mobile Banking Servises in Selected commercial Banks in Uganda; Uganda Bankers Institute.

Kizito, M.I. and Mugole, N.M. (2015). Effectiveness of Mobile banking services in Selected Commercial banks in Uganda. Makerere Univesity.

Kothari, C. R. (2008). Research Methodology: Methods and Techniques (2nd ed.). Delhi: New Age International (P) Ltd.

Kulabako Faridah (2012) The Monitor News Paper February 29th 2012

Lee, K. S. and Kim, S.Y. (2007). Factors Influencing the adoption behaviour of mobile banking: a South Korean

Littler, D. and Melanthiou, D. (2006).Consumer perceptions of risk and uncertainty and the implications for commercial banks.

Lovelock, C. H. (2000). Functional integration in service: understanding the links between marketing, operations, and human resources. In Swartz, T.A. and Iacobucci, D.

Maiyaki A. U. and Mokhtar S. S. M (2010) Effects of electronic banking facilities, employment sector and age – group on customers choice of banks in Nigeria. *Journal of Internet Banking and Commerce*, Vol. 15(1), April.

Mc Ewan (2000) Fraud by Wire and Access Devices.New York McGraw Hill.

Microsave: blog.microsave.net.

Mitroff, I. I. (2003). Do not Promote Religion under the Guise of Spirituality. *Organization*, 10(2), 375-377.

Mobarek, A. (2007). E-Banking Practices and Customer Satisfaction - A Case Study in Botswana, 20th Australasian Finance & Banking Conference.

Moutinho, L. and Smith, A. 2000. Modeling bank customer satisfaction through mediation of attitudes toward human and automated banking, *The International Journal of Bank Marketing* 18(3): 124.

Mudiri, J. L. (2014). Fraud in Mobile Financial Services. Microsave Publications: Kampala.

Muhammad, A. K. (2009). An empirical study of automated teller machine service quality and customer satisfaction in Pakistani banks. *European Journal of Social Sciences*, Vol. 13 No.3, pp. 333-344.

Munyoki, K.S., (2015). Effect of mobile banking on the Financial Performance of Banking Institutions in Kenya.

Namirembe.E. (2004) The Effect of ICT Innovations on the Banking Industry; A case odDfcu Bank, Unpublished Edition.

Nigeria. *Interdisciplinary Journal of Contemporary Research in Business*, 4(9), 253-264.

Nyango, A., Mbabazize, M. and Shukla., J. (2015). E-Banking and performance of commercial banks in Rwanda. A

Obiano W 2009. How to fight ATM fraud. online Nigeria *Daily News,* June 21, P. 18

of Distance Learning, Kwame Nkrumah University of Science and Technology.

Ogbuji, C. N. et al. (2012). Analysis of the Negative Effects of the Automated Teller Machine (ATM) as a Channel for Delivering Banking Services in Nigeria. International Journal of Business and Management 7, No. 7; April 2012.

Ogbuji, C. N., et. al., (2012). Analysis of the Negative Effects of the Automated Teller Machine (ATM) as a

Ogwal, I. (2014). Survival of the Fittest: The Evolution of Frauds in Uganda’s Mobile Money Market (part I).

Ojo, J. A., (2008). Effect of Bank Fraud on Banking Operations in Nigeria.*International Journal of Investment and Finance*.Vol.1 No. 1 pp.23-32.

Omankhanlen Odidison 2009. ATM fraud rises: Nigerians groan in Nigeria. *Daily News*, Sunday, June 21, pp. 8-10.

Onuorah, S. and Ebimobowei, D. (2012). Fraudulent activities and forensic accounting services of banks in Port

Oso, Y. W. and Onen, D. (2008). A General Guide to Writing Research Proposal and Report: A Handbook for Beginning Researchers, (2nd ed). Kampala: Makerere University Printery.

Paul, D.R. (1998). Towards a more efficient use of payment instruments. Available online at http://www.econ.kuleuven.ac.be/ew/academic/intecon/Degrauwe/PDG.

Perspective.*Journal of Internet Banking and Commerce*.Vol.12 No.2 pp.34-42.

Podder, B. (2011). Determinants of Profitability of Private Commercial Banks in Bangladesh: an Empirical Study.

Rasheed, A. S., Babaitu, D. and Tinusa, G. (2012).Fraud and its implications for bank performance in Nigeria.

Ravinder D. and Muskula, A (2013). Financial Analysis–A Study.*IOSR Journal of Economics and Finance e-*

Rose, P. S. (1999). Commercial bank management. Boston, Irwin/McGraw-Hill.

Rwanda. *Journal of Applied Economics and Business*.Vol.3 No 3 pp.49-60.

Sathye, M. (1999). Adoption of Internet banking by Australian consumer: An empirical investigation. International.

Sekaran, B. (2003). Basic Research for Social Scientists. (2ndedn). London: Macmillan Publishing.

Shannak, R.O. (2013). Key Issues in E-Banking Strengths and Weaknesses: The Case of Two Jordanian Banks,

Siyanbola, T.T. (2013). The effect of cashless banking on nigerian economy. *eCanadian Journal of Accounting and Finance,* 1(2): 9-19.

Tabaza B. ATM Fraud ans Customer Turnover in Commercial Banks in Uganda.Makerere University.

Thakor, A. V and Olazabal, N. (2002) Banking: The IT Paradox. *McKinsey Quarterly* 1(1): 45-51.

The Bank of Uganda Financial Stability Report (2015-2016).

Tunanukye V. and OluwafemiC.The Impact of Technology in the Uganda Finance and Investment Industry.A case of Alliance Investment House.The Banker .Vol 3.

Ugwu, E. (2008). CBN, banks to tackle ATMs' hitches. Retrieved April 25, 2013, from http://www.guardiannewsngr.com.

Wilhelm, W. K. (2004). The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management.

Wisdom, K. (2012).The Impact of Electronic Banking on Service Delivery to Customers of Ghana Commercial Bank.

APPENDIX I

QUESTIONAIRE

Dear Sir/Madam,

I am a student of Nkumba University pursuing a Master of Science Degree in Banking and Finance. I am carrying out a study entitled "Electronic Bank Fraud and Retail Bank Performance: A Case Study of Centenary Bank Headquarters Mapeera House. This questionnaire is seeking information on the above topic. The information you give will strictly be kept confidential and only used for academic purposes. You are not supposed to write your name on the questionnaire. Kindly spare some minutes to answer the questions and provide the valuable information following the directions in the questionnaire.

Section A: Background Information

i) Age group (please tick)

21-30 years
31- 40 years
41-50 years
50 years and above

ii) Level of Education (please tick)

Certificate

Diploma

Bachelors

Others

………..

iii) Gender(please tick)

Female

Male

For the questions in section B and section C, tick the number that best indicate your opinion on the question using the following scale.

Strongly Agree (SA) Agree (A) Not Sure (NS) Disagree (D) Strongly Disagree (SD)

543 2 1

SECTION B :ATM BANK FRAUD

	Statement	**1** **S** **D**	**2** **D**	**3** **NS**	**4** **A**	**5** **SA**
1	I frequently use my ATM card and I have not encountered any problem in using it.					
2	I am suspicious about my ATM account information					
3	I am aware of ATM fraud activities					
4	I have ever lost money to ATM fraud					

5	I have had complaints about ATM fraudulent from other people.					
6	ATM fraud is common in centenary bank					
7	ATM services at centenary bank are secure and safe					
8	Transacting bank services using ATM is risky					
9	When I lose my ATM I get so much worried about the safety of my money in the bank.					

SECTION C: INTERNET BANK FRAUD

	Statement	**1**	**2**	**3**	**4**	**5**
		SD	**D**	**NS**	**A**	**SA**
1	The bank allows customers to obtain consolidated information about their accounts status via internet					
2	The bank allows customers to obtain consolidated information about their non-financial accounts					
3	There is training offered to clients on how to use the services online					
4	Our bank provides on-line tutorials for new e-banking users					
5	Our Bank protects customers information from intruders					
6	The government is directly involved to manage internet banking security					
7	Clients are informed of the possibility of internet banking fraud					
8	Customers are told how to deal with Internet fraud in case it comes up					
9	Our Bank is able to detect fraudulent e-banking system activities					

SECTION D: MOBILE BANK FRAUD

	Statement	**1**	**2**	**3**	**4**	**5**
		SD	**D**	**NS**	**A**	**SA**

1	The mobile secret code or PIN number is known by me alone					
2	I am confident that my money is safe even if I lose my phone					
3	I am able to verify my account details before any transactions are made					
4	I have received suspicious SMS on ongoing promotions by fraudsters claimingto be bank officials					
5	I have received calls claiming that I have won money from the bank					
6	I have received messages claiming wrong transfer of money to my account					
7	Some bank staff collude with fraudsters to access customers' accounts					
8	I have ever been charged more transaction fees than the normal bank charges					
9	Fraudsters have ever used my transaction code to withdraw funds from myaccount					

SECTION E: ELECTRONIC BANK FRAUD AND RETAIL BANK PERFRORMANCE

	Statement	**1** **SD**	**2** **D**	**3** **NS**	**4** **A**	**5** **SA**
1	Customers' numbers keep on increasing					
2	Customers trust the bank that they are safe from fraud					
3	There are always deposit services in all branches					
4	There are always withdrawal services for customers in all branches					
5	The bank's mobile technology is the current/up-to-date one					
6	Customers access all they need to access at the time they need to					
7	Customers are contended with the banks services					
8	The bank conducts training to address fraud issues					
9	The bank has ATM machines in all places where its customers are located					

APPENDIX II

INTERVIEW GUIDE

Introduction to Respondent

I am a student Nkumba University pursuing a Master of Science Degree in Banking and Finance. I am carrying out a study entitled "Electronic Banking and Retail Banking Performance: A Case Study of Centenary Bank Headquarters, Mapeera House.

This interview guide is seeking information on the above topic.

The information given will strictly be kept confidential and only used for academic purposes. Kindly spare some minutes to answer the questions asked which include:

1. What is the effect of ATM banking on retail banking performance of Centenary bank?
2. What is the effect of Internet banking on retail banking performance of Centenary bank?
3. What is the effect of Mobile banking on retail banking performance of Centenary bank?
4. In what ways does the institution monitor customer accounts to ensure that they are in line with the customer's financial/business profile as understood by the institution?
5. What category of the clients uses mobile banking for their transactions?
6. Have you received cases of mobile banking fraud through:
    a) Abuse of passwords by system administrators
    b) Creation of fake and non-existent users on mobile banking platform
    c) Individual users with multiple rights
    d) Fraud on multiple access channel
7. What has been your experiences of ATM banking at centenary bank
8. How common are the following ways of ATM banking fraud:

a) Using fake ATM cards

b) Using stolen ATM cards

c) Card swapping

d) Card jamming

e) Shoulder surfing

9. What are some of the retail banking services that the bank offers?

APPENDIX III: KREJCIE & MORGAN'S TABLE FOR DETERMINING SAMPLE SIZE

N	S	N	S	N	S
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	3000	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	214	5000	357
100	80	500	217	6000	361
110	86	550	226	7000	364
120	92	600	234	8000	367
130	97	650	242	9000	368
140	103	700	248	10000	370
150	108	750	254	15000	375
160	113	800	260	20000	377
170	118	850	265	30000	379
180	123	900	269	40000	380
190	127	950	274	50000	381
200	132	1000	278	75000	382
210	136	1100	280	1000000	384