CARD FRAUD DETECTION TECHNIQUES ON PERFORMANCE OF COMMERCIAL BANKS IN NAIROBI, KENYA

ALLAN MAINA GAKURU
D53/NYI/PT/27635/14

A RESEARCH SUBMITTED IN PARTIAL FULFILLEMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION (MBA: FINANCE OPTION) IN KENYATTA UNIVERSITY

DECEMBER, 2016

DECLARATION

I wish to declare that this is my original work and has thereby not been submitted to any other University or institution of higher learning for examination .The research paper is a result of my own research efforts, and where other authors, researchers have been cited, they are duly acknowledged.

Signature_____ Date_____

Allan Maina Gakuru. D53/NYI/PT/27635/14

Supervisor

This research has been submitted for examination with the approval of the Kenyatta university supervisor.

Signature_____ Date_____

DR. John Mungai,

Lecturer,

School of business

Department of accounting and finance

DEDICATION

This research project was dedicated to my loving family whose support has enabled me to complete my research. Sincere thanks to my supervisors for his supervision and guidance and special thanks to God Almighty for giving life which has enabled me attain this level of my education.

ACKNOWLEDGEMENT

I would like to give special thanks to all those who contributed in one way or the other to the success of my research. I am greatly indebted to my supervisor, who was supportive in making valuable correction and contribution.

ABBREVIATION AND ACROYNAMES

ATM	Automated Teller Machine
CBK	Central Bank of Kenya
EMV	Euro Master Card and Visa
EPS	Electronic Payment System
KBA	Kenya Bankers Association
KCDA	Kenya Credit and Debit Card Association
P.I.N	Personal Identification Number
PCI DSS	Payment Card Industry Data Security Standard
PWC	Price Water House Coopers
SABRIC	South African Banking Risk Intelligence Centre
SAR	Suspicious Activity Reports
SEPA	Single Euro Payment Area

OPERATIONAL DEFINITION OF TERMS

Advanced Authorization Detection: Advance Authorization detection technique is the use of biometrics as advanced authentication tokens and biometrics proliferate, Biometrics refers to metrics related to human characteristics and it more advanced from Authentication detection technique which is the use of ID and password

Authentication Detection Technique: Authentication is the process of verifying the identity of users, applications, or devices before giving them access to sensitive data or systems. Today's authentication schemes range from a simple user ID and password

Bank regulation: A form of government regulation which subjects banks to certain requirements and restriction.

A debit card: Is a plastic payment card that provides the cardholder electronic access to their bank account(s) at a financial institution. Some cards may bear a stored value with which a payment is made, while most relay a message to the cardholder's bank to withdraw funds from a payer's designated bank account. The card, where accepted, can be used instead of cash when making purchases. In some cases, the primary account number is assigned exclusively for use on the Internet and there is no physical card.

Credit card: Is a payment card issued to users as a system of payment. It allows the cardholder to pay for goods and services based on the holder's promise to pay for them. The issuer of the card

creates a revolving account and grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user.

Card fraud: The fraudulent use of plastic card through theft of the account card number, card number, card details and personal information, through a wide variety of methods in order to perform unauthorized transactions from the comprised account.

Detection techniques: The process of extracting information or the act of discovering information which may prevent fraud from occurring.

Financial performance: Measures are intended to evaluate the effectiveness and efficiency by which organisations use financial and physical capital to create value for shareholders.

Performance: The accomplishment of a given task measured against preset known standard of accuracy, completeness

ABSTRACT

Fraud is one of the major ethical issues in the card industry. The study sought to find out card fraud detection techniques on performance of commercial banks in Kenya. The main aim of the study was to identify the different types of card fraud, and, review alternative techniques that can be used in detection of card fraud. The study defines common terms in card fraud, highlights key statistics and figures. The study reflects on how returns in the banking sectors have been eroded due to card fraud; this has made management and Shareholders of Banks to complain to the central bank which in turn has led to commercial banks analyzing card fraud. The study is likely to have beneficial attributes in terms of cost savings and time efficiency to all the relevant stake holders. The application of the techniques reviewed in the study will minimize card fraud being one of the major factors affecting performance of financial banks. The objectives of the study includes: the effects of Strong Authentication detection technique, understanding the effects of advanced authorization detection techniques, analyzing the effect of Card Fraud Management Systems detection and finally understanding the effects of (PCIDSS) Payment Card Industry Data Security Standard Compliance detection techniques on bank performance. The study adopted the descriptive research design because it enabled the researcher to summarize and organize data in an effective and meaningful way. It provides tools for describing collections of statistical observations and reducing information to an understandable form. The target population focused on the 42 banks who are members of the Kenya debit and credit card association. The study used the census study on the targeted population. The researcher used questionnaires in collecting primary data. The quantitative and qualitative analysis was analyzed using both descriptive and inferential statistical analysis. Reliability of the questionnaire was ensured by chronbach alpha which was reliable and consistent in analyzing the responses of the questionnaires. Content validity was measured by using experts in the field of study to validate the instrument. To establish the strength of the association among the variables Pearson correlation coefficient and multiple regressions was utilized. The integrity and effectiveness of the model was assessed by considering the coefficient of determination and analysis of variance. The descriptive and quantitative measure was calculated using the Statistical Package for Social Sciences (SPSS) 17.The result of the study indicated a significant relationship between strong authentications detection technique on performance of banks with the study indicating any change in strong authentication technique affected the bank performance by 35.9%. The study also indicated that Advance authentication technique significantly affects bank performance any change on the technique affects bank performance by 45.8% positively. The study also concluded that Card Management system technique had no relationship with bank performance with the study indicating 0.999 as a figure which insignificantly affects the bank performance .The study also indicated that PCIDSS compliance system significantly affects Bank performance with a change of the PCIDSS compliance system affecting bank performance by 20%. In conclusion most detection techniques affect bank performance.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Moncla & Gregory(2013) state that bank cards are issued plastic card with a magnetic stripe that holds machine readable identification code. Bank cards are used for electronic commerce with magnetic stripe readers or via Internet and for banking transactions through automatic teller machines (ATMs). Two main types of bank cards are credit cards: which allow drawing of funds up to an approved credit limit and debit cards: which allow drawing of funds up to the available balance in cardholder's account.

Bulus (2013) stipulated that fraud is an intentional deception made for personal gain to damage another individual. It is a crime and is also a civil law violation. Defrauding people of money is presumably the most common type of fraud, but there have also been many fraudulent discoveries, in art, archaeology, and science.

Sitienei, (2012) describes bank fraud on the other hand, is the use of fraudulent means to obtain money, assets, or other property owned or held by a financial institution. Cards are one of the most famous targets of fraud, Furthermore the face of fraud has changed dramatically during the last few decades as technologies have changed and developed. A critical task is helping businesses and financial institutions including banks to take

steps to prevent card fraud and to deal with it efficiently and effectively, when it does happen (Anderson, 2015).

Doody (2008) also stated that debit and credit card payments are convenient for consumers, widely accepted by merchants, and more efficient than paper forms of payments, but as cards have become the primary payment instrument in retail transaction. Awareness of identity theft and concerns over the safety of payments has increased. card fraud is a sophisticated crime carried out by tech-savvy criminals using modern technology, these fraud payments have resulted into losses therefore driving increasing efforts in card fraud prevention and detection as well as implementation of robust card risk fraud management response strategies such as the new laws which were enacted to compel banks to maintain set security standards and open the card networks to external auditors.

Sitienei, (2012) stipulate that when banks lose money because of card fraud, card holders partially pay the loss through higher interest rates, higher membership fees, and reduced benefits. Hence it is in both the banks and card holders' interest to reduce illegitimate use if credit cards, particularly when plastic are prevalent in today's increasingly electronic society. Various techniques in fraud management have been developed and are used by commercial banks to manage the menace of fraud.

Doody (2008) states that for the period of April 1, 1996 through September 30, 2002, the FBI received 207,051 Suspicious Activity Reports (SARs) for criminal activity related to card fraud. These fraudulent activities accounted for 47 percent of the 436,655 Suspicious

Activity Reports (SARs) filed by U.S. financial institutions (excluding Bank Secrecy Act violations), and equaled approximately $7 billion in losses" (U.S. Department of Justice DOJ, 2002).

According to Meridien Research(2011), without any technological investments in card fraud detection and prevention, worldwide card fraud will represent $15.5 billion in losses annually by 2015. However, if merchants adopt data mining technology now to help screen credit-card orders prior to processing, the widespread use of this technology is predicted to cut overall losses by two thirds to $5.7 billion in 2015 (Mena, 2003).

Wesley (2004) stipulated that with changing consumer spending patterns, the European card market has expanded rapidly in the last few years. According to a report sponsored by Payments, Cards & Mobile, there are approximately 322 million credit and debit cards in circulation across the U.K., Spain and France and around 92 million in Germany. In Poland, the number of credit cards tripled between 2004 and 2007. Fraudsters have spotted this growing market as an opportunity and banks have seen their card fraud losses increase substantially as a result. However, the tactics used by fraudsters and their levels of sophistication as well as the counter-measures used by financial institutions has varied widely across Europe.

Mena,(2003). States that With 82 million credit and debit cards in circulation in 2007, France is one of the pioneers of smart cards which have been rolled out en masse to

control fraud. By 1992, all French bank cards were chip-enabled and during the first year following the introduction of Chip and PIN, total card fraud losses halved and domestic counterfeit fell by 78 per cent. In France, issuers are also provided with industry fraud scores by organizations such as Carte Bleue, which has successfully helped drive down some forms of card fraud.

Anderson, (2007) stipulated that with the economic boom over the past few years, particularly in the Middle East, the total number of credit cards in the Middle East and North Africa region jumped by 24 per cent in 2006 to 6.23 million. However, this has not only drawn businesses and developers to the area, but it has also increased its attractiveness to criminals. As a result, the region is not only seeing the adoption of card usage but also consequent anti-fraud strategies usage by banks which are likely to evolve in the coming years and these countries have adopted the prevention and detection measures to combat card fraud.

Mena (2003) states that the number of unbanked consumers in Africa is still high, levels of card use are still relatively low; However Euro Master Visa(EMV) is being rolled out in places, in a bid to prevent potential card fraud. Douglas (2005) talked of card fraud in Kenya and the major campaign in the country by commercial banks with collaboration with KBA to sensitize customers on the importance of safeguarding personal information especially with the usage of ATM and ATM cards.KBA is currently running a consumer awareness programme to educate banks and the public on

the importance of safeguarding personal information at the ATM. The campaign Dubbed“KAA CHONJO! (BE ALERT!)” the ATM Safety campaign provides basic information that bank customers can follow, including areas to check out for when you are at an ATM; and tips on how to protect your PIN.(KBA 2013).

This has been done through sensitization activities including radio Public Service Announcements; and the distribution of materials with the support of faith-based organizations, universities; and other partners, including Pesa-Points.Banks are also encouraging customers who use on-line transactions to only provide the first four numbers and the last four numbers. This procedure is called masking which reduces card vulnerability to fraudsters.

1.1.2 Performance of Banks

According to Mutua (2010) Financial performance measures are intended to evaluate the effectiveness and efficiency by which organisations use financial and physical capital to create value for shareholders. Some authors have suggested the balanced scorecard which provides a framework, which encourages the use of financial and non-financial measures of performance via balancing three perspectives which include profitability, customers base and transaction volumes. (Kaplan and Norton, 1992).Zenios et al. (1999) recommended measures for financial analysis include: profitability, customer’s base and transaction volumes. Mutua (2010) further carried out a successful study which showed that bank cards affect profitability of banks.

1.1.3 Profitability of Banks

Muriu (2007) States that due to the changing banking environment, profitability is one of the most important criteria to measure performance of banks. Profitability is critical to the survival of commercial banks. Firstly, dividends are paid from profits (cash profits) and secondly, profit is an important source of retained earnings. Retained earnings are residual profits after dividends are paid. These earnings are important component of bank capital. Douglas, (2005) further states that the relevance of the study on the profitability of commercial banks therefore is based on the fact that it is the most important component in the banking industry. Thus, failure to have detection system on cards may have deep economic repercussion on banks at large. Secondly, banking sector reforms on cards are likely to affect the way banks operate and thus their performance, finally, bank profitability is an important source of retained earnings; a very important component of bank capitalisation, providing a margin of protection during recessionary periods, and enabling the banks to be more resilient against external shock. Expenditure and income of the detection technique affect profit. The cost incurred in the detection technique should be far less than the benefits realized.

1.1.4 Customer Base

Muriu (2007) and Douglas (2005) were the earliest to suggest that performance of firms are determined by increased customer base. They demonstrated that performance of firms operating in highly populated areas are significantly higher than that of firms operating in industries with lower population. Economies of scale brought about by

increased customer base will reduce the cost of gathering and processing information especially when dealing with card fraud management systems (Pavel and Binkley2007). A positive effect of increase in customer base is associated with profitability.

1.1.5 Transactional Volume

Douglas (2005) states that volume is an indicator of the market move, if markets have made strong price move either up or down the perceived strength of the move depends on the volume for the period. The higher the volume during that price move the more significant the move to the performance of an organization.

1.1.6 Card Fraud Detection Technique

Douglas, (2005) describes Issuing credit cards have turned into big business. These financial institutions that issue cards to consumers make money through outstanding balance fees, annual fees, and late payment fees. On the front end, when consumers make purchases with their cards, financial institutions make roughly 2.00% (the actual amount depends on the size of the sale).The fees that banks charge when credit cards are used for purchases are known as Interchange. The industry has come under fire during the past few years because interchange fees have risen 117% in the past five years. Interchange prices are fixed regardless of volume, which has irked many larger retailers. Cards are now an integral part of our lives with roughly 80% of all families having some type of card.

Past investigations on the card usage have acknowledged the role that the bank cards play on the financial performance of commercial banks. Odhiambo (2012) in his study a survey of the factors affecting the use of credit cards particularly in Migori town acknowledges the fact that the credit cards have a positive effect on the financial performance of the commercial banks in Kenya.

Card fraud makes banks to incur high non-interest expenses. On December 31, 2003, for instance, the average noninterest expense of bank card amounted to roughly 17 percent of the total assets. Processing card transactions is a costly operation. Bulus (2013) detail the mechanics of bank card transactions and its effects on performance. He further stated that card fraud affects the performance of banks through: The banks antifraud departments incurring cost on investigation of the frauds, investment in detection and prevention techniques.

1.1.7 Central Bank of Kenya Regulator of Commercial Banks

According to Central Bank of Kenya data, more than 13.9 million payment cards (ATM/debit cards) were in circulation by February 2015, representing a 20.9% increase over the previous year, in this period card fraud reduced by 90% as a result of the introduction of the chip and pin. KBA (2013) states that many sub-Saharan countries have yet to introduce chip cards because of the cost of upgrading their systems and infrastructure, as well as issuing the new cards, however the banking industry's migration to the EMV compliance standard has so far been successful. Nearly a year after the adoption of EMV, which introduced chip and PIN technology

as the industry wide standard for payment cards, no card skimming incidences have been reported to Kenya Bankers Association (KBA) by its member banks. KBA (2013) states that this method is effectively addressing card skimming fraud, which is promoting payment card usage. It is anticipated that the enhanced security features will spur customer confidence, resulting in more customers using payment cards not only at the ATM point but also in retail outlets and via online platforms.

1.2 Statement of Problem

Statistics from Banking Fraud and Investigations Department (BFID 2016) show that the frequency of card fraud is increasing and affecting the performance of banks. Banks are suffering huge losses due to the perpetration of card fraud. According to the CBK report of 2014 it stated that commercial banks lost 4.5 billion Kenya shillings which are more than what most banks make in a year. Management and other stakeholders of listed commercial banks expect good returns from the banks. Companies are focusing their efforts on creating yearly improvement of shareholder‘s value to survive in an increasing global competition (Moncla & Gregory, 2013). The returns in the banking sectors have been eroded due to card fraud; this has made management and Shareholders of Banks to complain to the central bank. The two have piled pressure on Central Bank of Kenya to find solution on combating card fraud. Fraud threatens the achievement of this key objective hence the need to adopt proper strategies to manage or control it.

Banks cannot take their foot off the pedal when it comes to introducing anti-fraud strategies. (KBA, 2013) Indeed, the 2009 research from data monitor into financial crime reported that despite efforts to combat fraud, the global financial crisis could accelerate a wave of financial crime with the banks being the main targets for criminals. In order to protect themselves against potential fraudulent attacks, financial institutions need to find ways of implementing effective anti-fraud strategies while maintaining efficiency and keeping costs to a minimum, but the first thing they need to do is to address the challenges they face in the fight against card fraud.

Several studies have been carried out on card fraud in the banking industry. Sitienei (2012) undertook a study on factors influencing credit card fraud in the banking sector; the case of Kenya Commercial Bank Mombasa County; however these studies have not shown how card fraud detection techniques affect the performance of commercial banks. This study therefore sought to fill the existing knowledge gap by seeking to answer the following question how card fraud detection techniques have affected the performance of listed commercial banks in Kenya.

Mutua (2012) undertook a study of prevention of cards fraud through adoption of detection techniques, however his study only focused on detection of card fraud and it did not emphasize on how detection techniques affect performance of banks. This study therefore sought to fill the existing knowledge gap especially in banks.

Siciliano (2013) study focused on how early detection of credit card fraud Spells Low Risk and High Profits. This study focuses on one element of performance of banks and it does not focus on customer base and transactional volumes. The current study covers this knowledge gap and focuses on more factors associated with performance.

1.3 Objectives of the Study

1.3.1 General Objectives

I. The purpose of this study was to establish card fraud detection techniques effects on performance of commercial banks in Kenya.

1.3.2 Specific Objectives

I. To determine the effect of Strong Authentication detection on bank performance
II. To determine the effect of advanced authorization detection technique on bank performance
III. To examine the effect of Card Fraud Management Systems detection on bank performance
IV. To measure the effect of (PCIDSS) Payment Card Industry Data Security Standard Compliance detection technique on bank performance

1.4 Research Hypotheses

The study was based on the following null hypotheses;

H_{o1}: Strong authentication does not have any significance on the performance of listed commercial banks in Kenya.
H_{o2}: Advanced authorization detection technique does not have any significance on the performance of listed commercial banks in Kenya.

H_{o3}: Card Fraud Management Systems technique does not have any significance on the performance commercial banks in Kenya.

H_{o4}: PCIDSS (Payment Card Industry Data Security Standard) Compliance detection does not have any significance on the performance commercial banks in Kenya.

1.5 Significance of the Study

This study is valuable to card fraud department managers in the payment card industry as they explore the most effective strategy to adopt in the detection of card fraud. They will be enlightened on the various strategies available in detection of fraud, how to implement them and be able to ascertain the effectiveness of these strategies this study will be beneficial to the central bank of Kenya in establishing governance policies as they relate to detection of cards fraud. This study is valuable to the criminal justice sector as it will shed light on an area that has been misunderstood and unknown by prosecutors, magistrates and lawyers. It will provide knowledge necessary to conduct productive investigations and prosecutions. To students and academicians the study will serve as a reference material for future research on related topic. It will seek to fill the knowledge gap left out by past strategies that have concentrated mainly on the general aspect of fraud.

1.6 Scope of the Study

The scope of the study was focusing on the effects of card fraud detection techniques on performance of commercial banks in Kenya. The study focused on all the banks that are members of the Kenya debit and credit card association. This is because banks incur

most of their losses perpetrated using bank cards. According to the CBK report of 2014, banks lose lots of funds in card fraud than in any other sector where cards are used.

1.7 Limitation of the Study

The respondents approached were reluctant to give information fearing that the information sought would be used to intimidate them or print a negative image about them or the bank. Some respondent turned down the request of filling the questionnaires. Bankers operate on tight schedules; some respondents were not able to complete the questionnaire in good time and that overstretch the data collection period. The researcher encountered problems in eliciting information from the respondents as the information required was subject to areas of feelings, emotions, attitudes and perceptions, which was not accurately quantified and/or verified objectively. Bank Cards have recently been introduced in the banking sector. The introduction of cards has led to the rampant card fraud been encountered, which has been attributed to lack of comprehensive research in this field. The study therefore borrowed heavily from USA and Canada who have managed to have robust detection and prevention techniques.

1.8 Study Organization

The proposal focused on card manager and risk managers who were based in the forty two commercial banks whose headquarters are based the Nairobi county. The study specifically acquired data from all officers who manage plastic card risk that is merchant managers or operation managers who were in charge of all operational risks in banks. The study focused on card mangers that are also

referred as ATM card managers and who have knowledge and information on the detection techniques used by banks.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section reviews theoretical studies and try to relate the theories with how card fraud detection techniques affect the performance of commercial banks in Kenya. It summarized the information from other researchers who have studied the field. The review covered both the theoretical and empirical reviews of the existing literature. The theoretical review helps in understanding of the current body of knowledge on the research topic while the empirical review help in understanding what other related studies have found and suggested. The reviews have been used to develop conceptual frame work.

2.2 THEORETICAL REVIEW

2.2.1 Adaptive Investment Approach

The concept of Adaptive Investment Approach, first proposed by Ma (2010, 2013, 2015), is the name given to the investment strategies that under which investors can constantly adjust their investments to reflect market conditions. The purpose of the approach is to achieve positive returns regardless of the timing in the investing environment. The underlying premise is that firms will constantly invest in various detection techniques which involve cost of upgrading systems and infrastructure, as well as issuing the new cards. Investment in the various detection techniques assist in reducing card fraud which improves performance of banks through increase transactional volume

and increase in customer base. This theory would be applicable in this study in terms of banks looking at creating a common approach to fighting the menace that faces them in the form of fraud which reduce profitability of investment done by investors.

2.2.2 Innovation Diffusion Theory

According to Dillon and Morris (1996); Rogers (1983 & 2003), the factors which influence the diffusion of an innovation include; relative advantage (the extent to which a technology offer. Improvements over currently available tools), compatibility (its consistency with social practices and norms among its users), complexity (its ease of use or learning), trial ability (the opportunity to try an innovation before committing to use it), and observe ability (the extent to which the technology's outputs and its gains are clear to see). These elements are not mutually exclusive thus unable to predict either the extent or the rate of innovation diffusion. Moore and Benbasat (1991) built on the work of Roger (1983), amongst others Tornatsky and Klein (1982) and Brancheau and Wetherbe (1990) and expanded the array of innovation characteristics to seven. Three of the seven innovation characteristics are directly borrowed from Rogers: relative advantage, compatibility, and trial ability. Specifically, the theory begins to describe the innovation decision process within organizations, the high level of innovation has attributed to the reduction of card fraud through the various detection techniques which vary from strong authentication methods to advance

authentication methods. Banks should strive to adapt to new technology in order to have relative advantage which comes as result of reduction of risks by adopting card fraud detection techniques banks performance is likely to improve by more than 75%.

2.2.3.Nadler and Tushman's Congruence Theory

Nadler and Tushman (1997) proposed the congruence theory for managing change. Their theory is based on the principle that an organization's performance is derived from four elements: tasks, people, structure (technology), and culture. The higher the congruence, or compatibility, amongst these elements, the greater the performance. For example, if you have brilliant people working for you, but your organization's does not have up to date technology, their brilliance will not shine through. Likewise, you can have the latest technology and superbly streamlined processes to support decision making, but if the organizational culture is highly bureaucratic, decisions will undoubtedly still get caught in the quagmire. According to the congruence theory, an organization should adopt the latest technology such as strong authentication, advance authorization technique which prevent and deter card fraud with the adoption of this techniques training of staff should be conducted in order to increase higher congruency and compatibility among staff and system. The congruency improves performance of banks through improve profitability and reduced risks associated by card fraud.

2.3 Empirical Literature

Several empirical studies have been conducted concerning the credit card usage and the performance of commercial banks. Muriu (2007) conducted a study on a survey of challenges facing the growth of plastic credit and debit cards in Kenya. A sample of 30 cardholders was taken. Data analysis method used was content analysis for the cardholders and qualitative analysis for card issuer manager.The study found out that marketing is limited in that products for example products like the credit card are not a mass product. Vetting of new entrants in the credit card is very restrictive. The study also found out that customers do not apply for credit cards because they fear debt, some are risk averse and others fear fraud for both credit and debit cards .

Mutua (2010) carried out a study on the key success factors and bank strategy in the credit card industry: a survey of commercial banks issuing credit cards in Kenya. He studied 12 commercial banks. The research used primary sources of data since the objective was to identify the perception of commercial banks issuing credit cards on key success factors and establish the extent to which they have a related strategy for factors identified. Descriptive statistics were used to transform the data collected into standard form for relative comparison. The study found out that the key success factors that were very important in influencing customer use of bank products and service were service quality, technology, marketing, human resources, pricing, and finance.

Williams (2007) presented a case study of credit card fraud in Tobago and Trinidad, new entry countries into the credit card market, in which a prevention activity can be improved by issuing specific laws, educating and informing the public of the various fraudulent typologies and enhancing the critical role of the banking associations in formulating *ad hoc* principles and policies to control this type of fraud. However the study did not indicate the effects of detection techniques in performance of bank.

Noka (2010) presented a case study on the strategies employed in payment card fraud. where management entail a multilayered approach to security and risk management The study indicated the strategies involved that is in minimizing fraud in the payment system by building policies and tools that help prevent fraud before it happens, protecting vulnerable card data whenever it is stored however it did not take in consideration how minimization of fraud affects performance.

2.4.1 Authentication Detection Technique

Pavel and Binkley (2007) illustrate that authentication detection technique as one critical pillar in any security system. Authentication is the process of verifying the identity of users, applications, or devices before giving them access to sensitive data or systems. Today's authentication schemes range from a simple user ID and password to multi-factor approaches that include smart cards, PINs,

mobile devices, The reason for this variety in authentication approaches is simple, applications require different degrees of assurance that users are who they claim to be and secondly, The costs associated with different forms of authentication can vary significantly. As a result, organizations are forced to make a choice between a single universal approach and a fragmented set of authentication silos designed to suit individual needs.

Douglas, (2005) also states that authentication involves processes designed to verify the legitimacy of both cardholders and the payment cards they present. Issuers conduct their authentication processes remotely while relying on merchants to conduct some authentication processes at the location where payment is made. When a customer presents a payment card to a merchant, the merchant regards possession of the card as verification that the customer owns the card account and can legitimately authorize a payment.

Douglas, (2005) futher emphasized that for a signature card payment, the merchant can do more to authenticate the cardholder by comparing the signature on the payment terminal with the signature on the back of the card. The merchant authenticates the card by verifying special attributes on the card to rule out counterfeits. The card may include attributes that counterfeiters find hard to duplicate, such as an elaborate brand logo or a hologram, or information that is repeated on the card, such as elements of the card's account number embossed

on the front and printed on the back of the card (MasterCard). Issuers also rely on merchants to screen for counterfeit cards. The PIN authenticates the cardholder in a PIN debit or an ATM transaction, but the issuer relies on the merchant to authenticate the cardholder in a signature debit or credit card transaction.

Anderson (2015) states that the transmission of encrypted information from a card payment terminal to a card issuer is a key part of the authentication process. Using cryptographic techniques, card issuers write verification codes into the magnetic stripe of each card they manufacture. When a cardholder swipes a magnetic-stripe payment card at a payment terminal, the terminal transmits the verification code to the issuer. The issuer reads the code to be sure it is consistent with the card account number and its expiration date. Any inconsistency may lead the issuer to suspect fraud and decline the transaction. Verification codes thus give merchants and issuers some degree of assurance that the card and card-holder are legitimate, examples of authentication detection technique involves Introduction of Chip and Pin Card.

Kwambukha, (2013) The introduction of the chip and pin card has been hailed as a strategy by commercial banks as a way of reducing fraud in debit and credit card transactions. Replacing the almost forty year old magnetic strip card processing method with the EMV smart card payment system which stands for

Euro, MasterCard and Visa. EMV is an open-standard set of specifications for smart card payments and acceptance devices.

The EMV specifications were developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe card (Kenya Banker, 2013).

Kenya Banker (2013) also state that the biggest benefit of EMV is the reduction in card fraud resulting from counterfeit, lost and stolen cards. EMV also provides interoperability with the global payments infrastructure – consumers with EMV chip payment cards can use their card on any EMV-compatible payment terminal.

Kwambukha, (2013) further states that EMV technology supports enhanced cardholder verification methods and, unlike magnetic stripe cards, EMV payment cards can also be used to secure online payment transactions. Skimming in highly unlikely in chip and pin cards for the customers details are stored in the chip and not in the magnetic strip behind the card. EMV cards store payment information in a secure chip rather than on a magnetic stripe and the personalization of EMV cards is done using issuer-specific keys.

Unlike a magnetic stripe card, it is virtually impossible to create a counterfeit EMV card that can be used to conduct an EMV payment transaction successfully

The Kenya Bankers Association (KBA) has mandated commercial banks to have Automated Teller Machines and cards to be chip and pin ready by September 30th 2013 (Kwambukha, 2013).Skimming in highly unlikely in chip and pin cards for the customers details are stored in the chip and not in the magnetic strip behind the card.

Kamal (2014) in the study on the effect of the electronic credit card usage on bank's profitability agrees with Odhiambo (2012) that there is a positive effect between the numbers of the bank cards, the net income from the bank cards and the profitability of commercial banks.

Muiru (2014) in his study the effects of financial innovation on financial performance of commercial banks found out that some banks in Kenya had adopted some forms of financial innovation like the cards, mobiles and agency banking and these had a great impact on the financial performance of commercial banks.

2.4.2 Advanced Authorization Detection Technique

Situma, (2012) stipulates that advanced authorization detection technique, manage and prevent suspicious and potentially costly fraudulent transactions. Customized rules-based filters and tools to your business. According to the results of the 13th annual Card Fraud Report, U.S. merchants lost an estimated

$3.4 billion to fraud in 2013. The Advanced Fraud Detection Suite was specifically built to provide merchants with tools to better combat Card fraud. The benefits of advance fraud detection suite are reducing Costs: Minimize and prevent authorization and chargeback fees as well as possible transaction loss resulting from fraudulent transactions. Protect Profits: Maximize legitimate transactions, rather than refusing business due to a fear of potential fraud. Maximize Flexibility: Customize filter settings according to your unique business needs. Improve Intelligence: Restrict transaction activity from specific Internet Protocol (IP) addresses using powerful IP tools. Easy to Use: A setup wizard guides you through the configuration process. Examples of advance authorization detection technique involve biometrics.

Kwambukha,(2013) describes biometrics as an advanced authentication tokens and biometrics proliferate, the attention of attackers and malicious insiders will shift from the theft of credentials to the subversion of the back-end authentication systems. Purely software-based authentication systems may require hardening to bolster security and satisfy compliance obligations. Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication is used in computer science as a form of identification and control. It is also used to identify individuals in groups that are under surveillance.

Doody, (2008). Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

Situma, (2012) identified more traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information. Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication.

2.4.3 PCIDSS (Payment Card Industry Data Security Standard)

Compliance Detection Techniques.

Situma, (2012) states that this is a technique that involves encryption of data which ensure unauthorized access to information is not permitted; it involves the following methods decision tree. Douglas (2012) decision tree is also referred to as the use of a similarity tree or the use of logic as a technique. A similarity tree is defined as a node or labeled with attribute names.

The edges are labeled with values of attributes that satisfy some condition and 'leaves' that contain an intensity factor which is defined as the ratio of the number of transactions that satisfy these condition(s) over the total number of legitimate transaction in the behavior (Kokkinaki, 2015). The advantage of the method that is suggested is: that it is easy to implement, to understand and to display, however a disadvantage of this system is the requirements to check each transaction one by one. Nevertheless, similarity trees have given proven results (Fan et al. (2001) also worked on decision trees and especially on an inductive decision tree in order to establish an intrusion detection system, for another type of fraud.

2.4.5 Card Fraud Management Systems

Doody, (2008) states that another critical pillar in any security system is card management system it's the process of managing systems information that identity; classify credit card transactions into suspicious and non-suspicious classes. Card fraud management systems involve Card payment approval process.

Douglas, (2012) describes it as Payment fraud that involves gaining financial or material advantage through using a payment instrument (or information from a payment instrument) to complete a transaction that is not authorized by the legitimate account holder. In this definition, the lack of an account holder's authorization is the crucial in distinguishing characteristic of payment fraud.

Anderson (2015) stated that to prevent fraud, several steps must occur before a transaction is approved by a card issuer. The card is authenticated (to screen for counterfeits), the cardholder is identified (to prevent unauthorized use), and risk parameters set by the card issuer or merchant are checked for compliance (such as sufficient funds in an account). If the payment satisfies these steps, the payment is approved.

Bulus (2013) states that advances in the payment approval system have helped combat card payment fraud. Online approval of card payments, where transaction information is sent from the point of sale to the card issuer for immediate approval or rejection, was developed by the early 1980s and today is used in nearly every U.S. transaction (Stearns). In the 1990s, "neural network" computer systems, which use complex statistical modeling techniques, were applied to improve transaction analysis and help detect fraudulent transactions.

Anderson (2015) stated that internet merchants are now controlling payment fraud by using their own analysis of transactions before deciding to accept an online order (Cyber Source). The recent introduction of contactless cards in the United

States that transmit card information on radio waves (instead of through a swipe of a magnetic stripe) adds some security features that are superior to those on magnetic stripe cards. Card issuers and merchants face numerous challenges in making a correct approval decision.

Anderson (2015) futher emphasized that payment cards that issuers produce are not sufficiently difficult to counterfeit. To accommodate merchants and consumers, card issuers continue to allow payments via mail order, the telephone, and now the Internet, with only the information from a payment card. Some merchants do not properly check payment cards for counterfeits or review signatures of cardholders. Some consumers write their PINs on their payment cards or do not sufficiently protect their personal computers.

According to Pavel and Binkley (2007) the common underlying cause of these vulnerabilities is an information-intensive payment approval process and this reliance on information is growing. For example, online payment approval has allowed automated checks against wider sets of information, such as a cardholder's zip code or transaction history. More information will generally lead to a more accurate approval decision, which gives card issuers (and merchants) an incentive to continuously expand the data on which they rely.

Pavel and Binkley (2007) states that criminals also have strong incentives to gather and use this same information to commit fraud. The incentives of these two groups results in an escalating cycle that leads to more resources on each side to either protect or to compromise data. Relatively simple ways for criminals to get such information is to steal a wallet, intercept mail that contains account statements, or spy the information while it is used in a transaction. The recent transition to electronic payments processing has opened new avenues for gathering payment card data.

Pavel and Binkley (2007) states a disguised card reader can be fit over a legitimate slot on ATMs or other payment terminals to electronically capture card information (skimming). Video cameras placed in hard-to-detect locations can capture PIN numbers. Criminals also exploit the Internet, such as by sending out millions of email messages that trick a small number of recipients into revealing sensitive account or card information (phishing). On a larger scale, hackers can penetrate computer systems where the information is stored and transmitted.

Neha Sethi (2014) states that specialized electronic payment fraud industry appears to increasing. Security experts argue that since 2004 criminals who were carrying out card fraud and attacks on electronic banking got organized, thanks to a small number of criminal organizations and a number of chat-rooms and other electronic fora, where criminals can trade stolen card and bank account data,

hacking tools and other services. Elements of this industry specialize in activities such as writing malware, hacking databases, organizing underground electronic marketplaces, and money laundering.

2.5 Research Gap

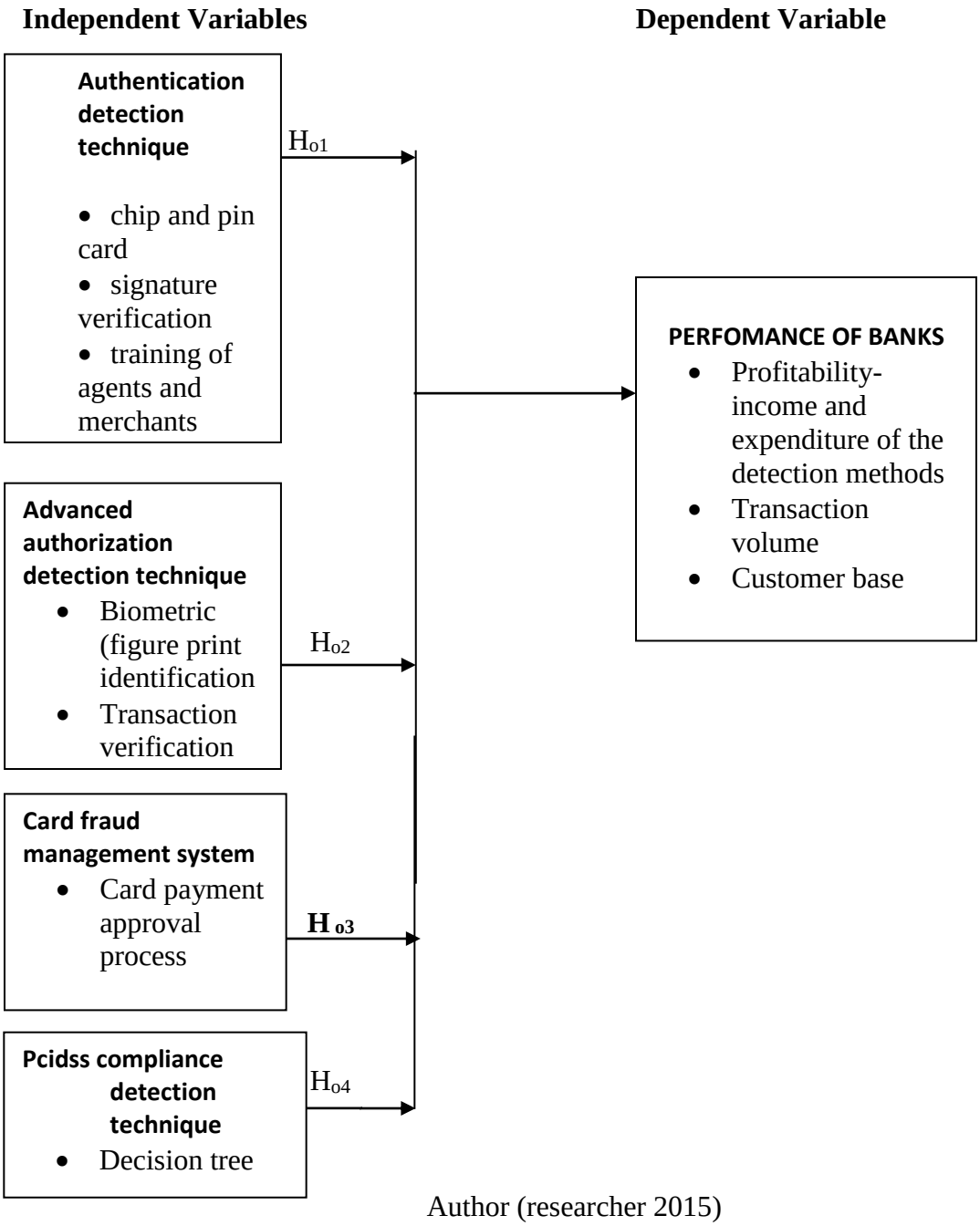
Sitienei (2012) observed that there are several factors influencing credit card fraud in the banking sector; however in his study he did not clearly indicate how card fraud detection techniques affect the performance of commercial banks, with many shareholders complaining of reduce profit hence reduced dividends a thorough analysis of the impact of card fraud detection techniques on bank performance should be analyzed. The existing knowledge gap on performance should ensure that such complaints from management and shareholders are addressed.

2.7 CONCEPTUAL FRAMEWORK

The conceptual framework illustrates a summary of the dependent and independent variables. It attempts to relate the independent variable with the dependent variables. In conclusion it's a breakdown and summaries the research. This literature review has identified four card detection techniques that affect the bank performance. Card fraud is a global issue that has affected commercial banks in the country mainly due to advances in information communication technology and the level of security in place. Card fraud management is a mutual responsibility amongst the commercial banks in Kenya. By implementing strong authentication technologies,

advanced authorization detection technique, card fraud management system and PCIDSS compliance detection technique in the country can ensure that fraud migrates to less secure areas.

Figure2.1 Conceptual Framework



Author (researcher 2015)

CHAPTER THREE:

RESEARCH METHODOLOGY

3.1 Introduction

This chapter provided details about the methodology adopted to assist in achieving the research objectives. According to Newing (2011), a research methodology dictates the research design structure, choosing of specific methods and developing a sampling strategy. It often also involved describing what analyses was carried out. This chapter covered research philosophy, research design, type of research employed, and population, sampling technique, sample size, instruments, pilot test and data analysis.

3.2 Research Design

The study adopted the descriptive research design because it enabled the researcher to summarize and organize data in an effective and meaningful way. It provided a tool for describing collections of statistical observations and reducing information to an understandable form. Kothari (2004) defines research design as a conceptual structure within which research is conducted. In addition, according to Cooper &Schindler (2006) descriptive research design is suitable where the study seeks to describe and portray characteristics of an event, situation, and a group of people, community or population which is the case adopted

3.3 Population

The target population consisted of 42 commercial banks that are members of the Kenya Credit and Debit Card Association (KCDCA) and have issued global payment cards that are either Visa or MasterCard. A census study was conducted on the target population. The bank representatives who will represent the bank will be card managers and risk managers.

	Target population of the 42 commercial banks
	Grand total
Card Managers	42
Risk Managers	42
Total	84
Source: Kenya Bankers association (KBA) 2013	

3.5 Data Collection

The study collected both primary and secondary data. The collection the primary data was facilitated by a semi structured questionnaire which was used. According to Mugenda and Mugenda (2003) questionnaires are suitable to obtain important information about the population. Orodho (2004) said this method reaches large number of subject who is able to read and write. Independently. Primary data is collected by the use of a semi –structured questionnaire. Questions on effect card fraud detection technique on commercial banks in Nairobi, Kenya were used in order to obtain specific information by providing a list of possible alternatives from which the respondents selected the answers that

best describes their opinion. Secondary data was obtained from review of reports from the Banking Fraud and Investigations Department (BFID 2012). Review of periodic reports filed by the listed banks was another source of secondary data. The questionnaire was distributed to the card fraud managers and risk managers in all the commercial banks. The researcher used the drop and pick method as all the banks in scope have their headquarters in Nairobi.

3.6 Data Analysis

Data analysis was performed on the completed questionnaire to answer the research question; what were the operational response strategies being employed by commercial banks in Kenya to combat fraud and how effective are they. Numbers of strategies used by commercial banks in Kenya were determined using descriptive statistics that is frequency and percent distributions. The prevalent strategies in use by most commercial banks were determined by mode and mean.

Faraway (2002) states that multiple linear regressions are used in situations where the number of independent variables is more than one. Regression analysis is also valuable for quantifying the effect of various simultaneous influences upon a single dependent variable. Further, because of omitted variables bias with simple regression, multiple regressions is often essential even when the researcher is only interested in the effects of one of the independent variables. Correlation analysis on the five point Like data obtained was used to indicate the extent in which the strategies used were associated with the payment card fraud rates in the commercial banks. Correlation analysis served to indicate the effect of applying individual strategies to address payment card fraud Equation (i) shows the linear

regression model of the independent variables against the dependent variable. Faraway (2002) states that Multivariable regression is used when there is more than one independent variable and which are not related to each other.

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X4 + E}$$

Where:

1. Y = the value of the dependent variable of performance of bank
2. $\{ \beta_i; i=1,2,3,4,5,6\}$ = The coefficients for the various independent variables
3. X_i for;
   X_1 =Strong Authentication detection
   X_2 = advanced authorization detection
   X_3 = Card Fraud Management Systems
   X_4 = PCIDSS Compliance detection

   E= Error term

To establish the strength of the association among the variables under study the Pearson correlation coefficient and multiple regressions will be utilized. The integrity and effectiveness of the model will be assessed by considering the coefficient of determination and analysis of variance. The descriptive and quantitative measure will be calculated using the Statistical Package for Social Sciences (SPSS) 17.

3.7 Data Presentation

Data was presented using graphical, pictorial representation which was also used as a way to show the survey of card fraud detection techniques and its effect on

performance of commercial banks in Kenya.

3.8 Reliability and Validity of the Instruments

Validity and reliability are two important characteristics of behavioural measure and are referred to as psychometric properties. They are not an all or none issue but a matter of degree. Alpha is an important concept in the evaluation of assessments and questionnaires. Nevertheless alpha has frequently been reported in an uncritical way and without adequate understanding and interpretation (Tavakol & Dennick, 2011)

3.8.1 Data Validity

Validity can be defined as the degree to which results obtained from an analysis of data actually represents the phenomena under study (Mugenda & Mugenda, 2003).Validity of a data Collection tool ensures that the items in the instrument are representative of the subject area while the content validity ensures that the tool actually measures what it is supposed to measure (Fraenkel &Wallen, 2000).Content validity will be measured by using experts in the field of study to validate the instrument.

3.8.2 Data Reliability

A reliable instrument consistently yields the same results when used repeatedly to collect data from the same sample drawn from a population (Orodho, 2005). Reliability is therefore the degree to which research instruments yields consistent

results when administered a number of times (Shaw& Wright, 1969). An instrument is reliable when it measures a variable accurately and consistently is used repeatedly under similar conditions.

Reliability of a questionnaire was measured using chronbach alpha for reliability and consistency of responses to the researcher's questions (Mitchell, 1996). Reliability will be ensured by pre-testing the questionnaire with a selected sample that will not to be included in the main study.

3.9 Ethical Consideration

The researcher acquired authority to conduct the studies. The researcher sought consent from the respondents and assured them that the research was solely for academic purposes and any confidential information obtained would not be revealed to any unauthorized third party. The researcher respected the institutional opinions and endeavored to embrace confidentiality**.**

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION

4.1 Introduction

This chapter presented the research findings in a study on card fraud detection techniques effect on the performance of commercial banks in Nairobi, county, Kenya. The analysis was focused on answering the research questions. The data was gathered exclusively from questionnaire as the research instrument. The response rate was fairly good because out of 80 questionnaires distributed, 71 were returned answered giving a response rate of 88.75%.

4.2 Social Demographic Characteristics of the Respondents.

This was a general analysis on the demographic data obtained from the respondents which included: - Job category, work duration in the bank, gender, age, nature of business, education level and number of years bank has offered card services.

4.2.1 Job Category

According to Douglas (2005) a job category is a broad based group of employees with comparable job responsibilities located at comparable levels of responsibility within an organization, if a researcher focuses on one job category they tend to be response bias and this affects the reliability, the researcher also established that response bias can be induced as result of focusing on one particular group and as such the study focused on two groups that is card managers and risk managers.

Table 4.1 Job Category of the Respondents

JOB CATEGORY	FREQUENCY	PERCENTAGE
Card managers	38	53.5%
Risk Manager	33	46.5%
TOTAL	**71**	**100**%

Source (researcher 2015)

Table 4.1 illustrates the job category of the respondents and a summary of the respondent who took part in filling the questionnaires administered. From the findings, 53.5% of the respondents who were the majority indicated that they were card managers while 46.5% of the respondents indicated that they were risk managers.

4.2.2 Work Duration

According to Mutua (2010) work duration is the amount of time a person spends and the effort used in trying to achieve a certain objectives. In his study he established that work duration affect the responses of the respondent, he established that employees who have worked for a longer duration tend to give more precise answers.

Table 4.2 Work Duration

Frequency	Population	Percentage
below 5 years	27	38.0
6-10 years	5	7.0
16-20 years	7	9.9
over 20 years	32	45.1

Total	71	100.0

Source (researcher 2015)

Table 4.2 indicates how long the respondents have worked. As per the study the respondents were asked how long they have worked with the bank. From the findings, 38% of the respondents indicated that they have worked below 5 year, 7% indicated that they have worked for 6-10 years, 9.9% indicated that they have worked for over 16-20 years, 45.1% indicated that they have worked for above 20 years. In the above study the majority of the respondent had worked for more than 20 years. The interesting feature of this data is that employees who have worked for long shoulder the responsibility of card fraud detection and prevention as per Mutua (2010) findings.

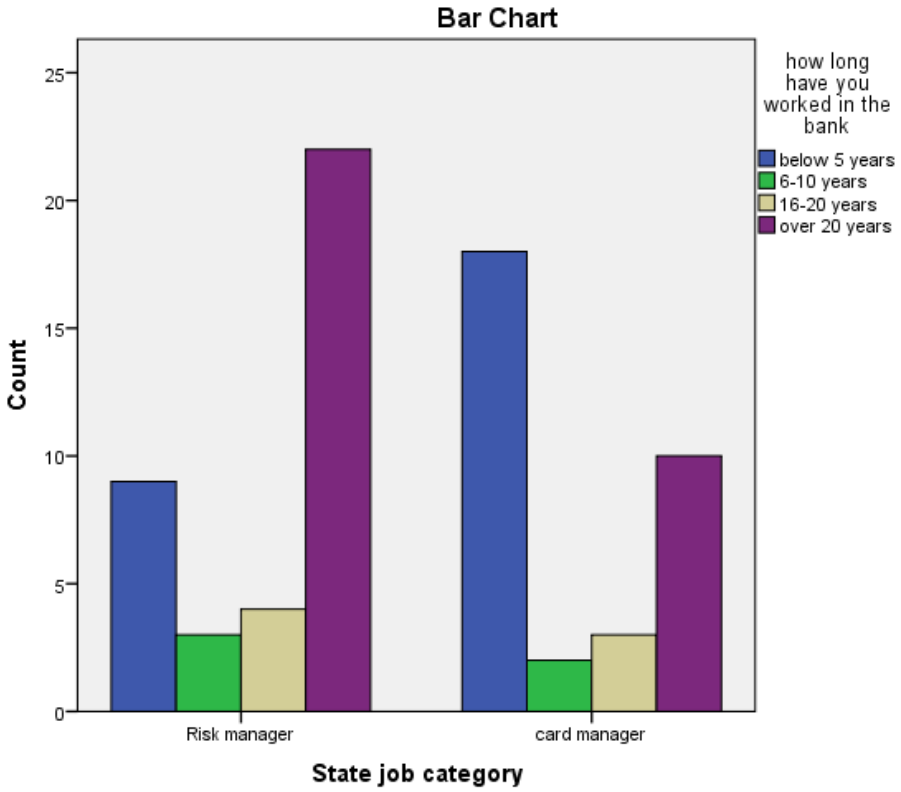
4.2.3 Distribution of the Respondents Experience and the Job Category.

According to Douglas (2005) social sciences research showed that personnel distribution of the respondents have very significant role to play in expressing and giving responses about the problem. Keeping this in mind, the study set to establish the distribution of the respondents experience and their job category.

Distribution of the respondent in terms of experience and job category is an important variable. It is evident from the table that most of the respondent who were risk manager had over 20 years of experience, while most of the card managers were below 5 years. In conclusion risk managers are selected

based on experience in the bank. According to Mutua (2010) experience is an important element in the ability to detect, prevent and avoid risk.

Figure 4.1: Distribution of the Respondents Experience and the Job Category



Source: field data (research 2015)

4.2.4 Distribution of the Respondents in Terms of Gender and Educational level.

Figure 4.1 illustrates the job category and education background of the participant who took part in the study. Education is one of the most important characteristic that might affect the person's attitude and his way of looking at issues and understanding any social and economic phenomenon. The response of an individual is likely to be determined by his educational status and therefore it becomes imperative to know the educational background of the respondent. Hence the variable education level was investigated and data pertaining to the education level is presented in the graph below

Table 4.3: Distribution of the Respondent In Terms of Gender, Education Level

Gender	college	University	Others	Total	Percentage
Male	2	39	3	44	62%
Female	3	24	0	27	38%
Total	5	63	3	71	100%

Source (researcher 2015)

The table 4.3 shows the distribution of the respondent in terms of gender, education level. From the findings 62% of the respondents who were the majority were men while 38% of the respondents were female. The study sought to establish the level of education of the respondents. From the findings, 89 % of the respondents who were the majority indicated that they were University graduates, 7% were college graduates and 4% were others. It can be concluded from the table above, that most of the respondents were progressive in their education and that higher education level is so important today in a knowledge

based society. It can be concluded from the table above, that most of the respondents were progressive in their education and that higher education level is so important today and is an indication of a knowledge based society. This result is in line with Anderson (2015) findings which indicate that detection techniques are determinant of bank performance which is determined by how bank staffs use the detection methods interchangeably.

4.3.1 Measure of the effects between Strong Authentication Detection Techniques with Bank Performance

According to Anderson (2015) advance authorization is a key variable in determining bank performance in that it affects customer base and profitability.

Table 4.4: Advance Detection Technique Affect The Bank Performance

	Frequency	Percent	Valid Percent	Cumulative Percent
Moderate extent	3	2.0	4.2	4.2
great extent	17	11.3	23.9	28.2
very great extent	51	34.0	71.8	100.0
Total	71	47.3	100.0	

Source (researcher 2015)

Table 4.4 demonstrates the respondents view on how advance detection technique affects the bank performance. According to Anderson (2015) advance authorization is a key variable in determining bank performance; It is evident from

table 4.4 that advance detection technique affect the bank performance, as per the findings 71.8% of the respondents who were the majority indicated that advance authorization detection technique affect bank performance with a very great extent, with 23.9 of the respondents indicating with great extent and 4.2% indicating with moderate effect and none of them indicating to a low extent and no extent. This result is in line with Anderson (2015) findings which indicate that advance authorization is a determinant of bank performance and is a major component in determining the performance.

4.3.2 Frequency of Fraud Training Conducted

Fraud training is amongst the strategies in fraud management that have been developed and are used by commercial banks to manage the menace of fraud. The respondents were required to indicate the frequency of fraud training conducted by the banks.

Table 4.5: Frequency of Fraud Training Conducted

	Cases					
	To a very great extent		Great Extent		Total	
	frequency	Percentage	Frequency	Percentage	frequency	Percent
How has						

PART F

REGULATION ON PERFOMANCE

29. To what extent do the following regulations govern the card industry? Use the scale of 1-5 where: 5 very great extents, 4 great extents, 3 moderate extents, 2 little extent, 1 no extent

	5	4	3	2	1
Prudential regulation and supervision					
Self-regulation					
In adequate regulatory frame work in the card industry					

APPENDIX IV

	NAMES OF BANKS
1	HFCK
2	GUARDIAN BANK
3	HABIB BANK
4	ORIENTAL COMMERCIAL BANK
5	TRANSNATIONAL BANK
6	PRIME BANK
7	PARAMOUNT BANK
8	FIDELITY BANK
9	UNITED BANK OF AFRICA
10	CHASE BANK
11	GTB
12	EQUITY BANK
13	BARCLAYS
14	DEVELOPMENT BANK
15	EQUITORIAL COMMERCIAL BANK
16	FAMILY BANK
17	HABIB AG ZURICH
18	CITIBANK
19	DTB
20	CREDIT BANK
21	BANK OF INDIA
22	BANK OF BARODA
23	NATIONAL BANK
24	MIDDLE EAST BANK OF KENYA
25	CFC STANBIC
26	STANCHART
27	JAMII BORA BANK
28	GIRO BANK
29	GUARANTEE TRUST BANK
30	CONSOLIDATED BANK
31	ABC
32	COOPORATIVE BANK

33	BANK OF AFRICA
34	NIC
35	KCB
36	ECOBANK
37	FIRST COMMUNITY BANK
38	POST BANK
39	GULF AFRICA
40	VICTORIA BANK
	Total

Source: Central Bank of Kenya Annual Report, 2015 (Central Bank of Kenya, 2015)