EMV CHIP CARDS AND OPERATIONAL RESPONSE TO PAYMENT CARD FRAUD BY COMMERCIAL BANKS IN KENYA

NAME: ALFRED MWENDA KITHINJI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION (MBA) SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

NOVEMBER 2015

DECLARATION

I declare that this is my original work and has not been submitted for examination in any other university or college.

Signature: …… Date: …….

Alfred Mwenda Kithinji

D61/64485/2013

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

Signature: …….. Date: ……..

Dr. Litondo Kate O.

Department of Management Science

School of Business

University of Nairobi

ACKNOWLEDGEMENTS

I thank the Almighty God for His blessings during this entire period of writing this paper and the entire study period.

I am grateful to my colleagues for their support during writing this paper. I also acknowledge the support of the respondents who took time to respond to my questionnaire.

I am grateful to Dr. Litondo Kate O, my project supervisor and Mr Lelei, the moderator for their guidance, patience and support throughout this project.

DEDICATION

This paper is dedicated to my lovely my wife Jane, and my parents Mr. and Mrs. Kithinji for their continued support and encouragement

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATM	AUTOMATED TELLER MACHINE
CBK	CENTRAL BANK OF KENYA
EMV	EUROMASTERCARDVISA
KBA	KENYA BANKERS ASSOCIATION
PIN	PERSONAL IDENTIFICATION NUMBER
POS	POINT OF SALE
BFID	BANKING FRAUD INVESTIGATIONS DEPARTMENT
PCI DSS	PAYMENT CARD INDUSTRY DATA SECURITY STANDARD
EFT	ELECTRONIC FUND TRANSFER
KYC	KNOW YOUR CUSTOMER
VPP	VISA PERSONAL PAYMENTS

ABSTRACT

The purpose of this study was to look at EMV technology adoption as an operational response strategy to payment card fraud by commercial banks in Kenya. The objectives were three fold, namely: to determine the extent of adoption EMV technology by Kenyan banks; to determine the challenges of using EMV cards in Kenya; and to establish the relationship between EMV card adoption and payment card fraud.

The study identifies the various types of payment card fraud and the impact payment card fraud has on financial institutions and their customers. The literature review identifies the operational response strategies to payment card fraud by commercial banks and the challenges experienced in adoption of EMV chip cards in Kenya.

The study employed a census study of all the commercial banks in Kenya. Data analysis was conducted using descriptive statistics and correlation analysis

The study establishes that commercial banks are aware of the challenges payment fraud caused and requirements necessary to minimize payment card fraud. Adoption of EMV is one of the methods fronted to reduce fraud; however this too has its challenges.

CHAPTER ONE: INTRODUCTION

1.1Background

The idea of using card payments originated in 1915. A small number of U.S. hotels and department stores began to issue what were then referred to as shoppers' plate. It was not until 1947 that the Flatbush National Bank issued cards to its local customers. This was followed in 1950 by the Diners Club, which was the first travel & entertainment or charge card, and eight years later the American Express card was born (O'Mahony Donal, 1961).

Nilson's report on the on market share of purchase transactions worldwide in 2014 highlights how Visa International and MasterCard dominate this worldwide business (The Nilson Report, 2014). The Kenyan payment card industry comprises of debit cards, credit cards and prepaid cards. Their uses range from paying for goods and services in stores, withdrawing cash from ATMs to most recently, paying for bus fare on public transport vehicles. Kenya has been developing into a hub for electronic payments as more Kenyans prefer the use of non-cash payment systems. With such an increase, the need for protection against fraud has become more compelling.

In 2014, Kenya's commercial banks lost $9.4 million in just six months (Olingo, 2014). This was mostly due to exploitation of gaps in non-cash payment systems in the country Data from the Banking Fraud Investigations Department (BFID) shows that there were 525 cases of fraud that led to a loss of $8.5 million by various financial institutions in the first quarter of 2014. The rising demands for financial transactions have favored this malpractice.

The Kenya Bankers' association (KBA) led the EMV migration of the Kenyan payment card industry using a three phase approach. The migration was to start with the replacement of ATMs in September 2013, followed by the migration of points of sale (PoS) terminals in December the same year and then closing with the certification of Card Management System (CMS) and replacing of magnetic stripe cards by March 2014 (KBA, 2015) . A liability shift was to take effect at the end of May 2014 where the banks would be liable for money lost in a fraudulent transaction carried out using a non-compliant card. (Mwaniki, 2014).

1.1.1. EMV/ Chip and Pin

EMV was named by its original developers; Europay, MasterCard and VISA (Engenico Group, 2012). It is a global standard for credit and debit payment cards based on chip card technology. EMV transactions are often referred to as "Chip and PIN" because PIN entry is required to verify the customer is the genuine cardholder. (Creditcall Ltd, 2015). In the wake of an alarmingly large-scale data breaches and increasing rates of counterfeit card fraud, most card issuers worldwide are migrating to this chip technology to protect their customers and reduce the costs of fraud.

There is a fundamental difference between a magnetic stripe card transaction, and an EMV chip transaction. For magnetic stripe, the card is simply a data store that is read by the terminal and then the card is no longer used. The terminal performs all the processing and applies the rules for payment (EMVCo, 2011). The stored unchanged data therefore makes magnetic strip cards more vulnerable to fraud as whomever accesses that data is also able to access the sensitive cardholder information necessary

for magnetic stripe transactions. EMV/chip card creates a unique transaction code that cannot be reused for every transaction, thus a cardholder's confidential data is more secure on a chip-enabled payment card (Gemalto, 2015).

In addition, chip card transactions contain dozens of pieces of information to be exchanged between the card, the terminal and the acquiring institution of the transaction. This is made possible by the terminal performing processing of card data and cryptographic authentication before a transaction successfully completes (Gemalto, 2015). The use of EMV technology does not prevent data breaches from occurring, but it makes it much harder for fraudsters who depend on data theft to succeed. The implementation of EMV/chip technology has been met with various challenges including; high cost involved in upgrading the payment infrastructure like the ATM network, Point of sales network and Bank EFT switch. There are also high costs of procuring of the chip embedded cards, personalization of the payment card and carrying out user education on the need to change. The security benefits have not been clearly proven; thus banks are not eager to spend in its implementation. Furthermore, the retention of the magnetic stripe on the back of the card negates the benefits accrued form adopting the technology (Vijayan, 2014).

1.1.2. Response Strategies to Fraud

Kenyan financial institutions have taken precautions to protect the banks against fraudulent practices. These precautions have been put in place not only to prevent fraudulent threats from outside the banks, but also from within by members of their staff. The institutions have responded to fraud by implementing different strategies that limits the possibility of fraudulent activities (Technology Banker, 2012). Some of the responses include; anti-money laundering workshops to train its staff on detecting

cases of bank related fraud and on desisting from committing fraud themselves, instituting multi-level access points where staff members have different access rights in the system, password management and a rigid recruitment process, allowing customers to set their own pin rather than issuing them one, passing of the Anti-Money Laundering Act to fight against bank crime, adopting of payment card industry data security standards (PCI DSS) and migrating to the EMV/chip technology. This has successfully steered the Kenya banking industry in upgrading its Automated Teller Machine network, point of sale network, EFT systems and payment cards following an industry wide initiative that was spearheaded by the Kenya Bankers Association and central bank of Kenya. This will be the focus of this research.

Payment Card Fraud can be defined as any illicit use, counterfeiting or alteration of a payment card unknown to the cardholder that entails the repudiation by the cardholder of a transaction that has been debited, as well as tampering with an automatic teller machine or illicit use of Point of Sale (POS) terminals in order to be able to use a payment card fraudulently. Payment card fraud occurs in two distinct transaction environments that are; card-present and card-absent, each of which offer unique card acceptance and fraud issues (Visa International, 2010). According to the statistical report on payment card fraud, the various types of Payment card fraud include; Card stolen fraud; card lost fraud; counterfeit fraud; account takeover fraud.

1.1.3. The Banking Industry in Kenya

Kenya's Banks are regulated by the Central Bank of Kenya Act, Bankers Act, and the Companies Act among other guideline issued under the Central Bank of Kenya (CBK). The Kenya banking industry comprises of 43 commercial banks, 12 micro

finance institutions and 86 forex bureaus (Central Bank of Kenya, 2015). The focus of this study is on the forty three commercial banks (most of which are small to medium sized and are locally owned). The commercial banks offer corporate and retail banking services but a small number, mainly comprising the larger banks, offer other services including investment banking (Central Bank of Kenya, 2014). All commercial banks in Kenya are under the Kenya Bankers Association (KBA) which works as a lobby for Kenyan banking industry. The adoption of the EMV cards was a KBA initiative targeting its members. The focus of this study will be commercial banks in Kenya.

KBA (Kenya Bankers' Association) has in the recent past been lobbying and engaging with various stakeholders in the Kenyan Payment card industry on the need for long-term risk mitigation with regard to fraud. These stakeholders include Visa International, MasterCard and The Central Bank of Kenya. (IT News Africa, 2014).

In early 2013, a process that would see all banks to be EMV compliant by 30th March 2014 was established by The Central Bank of Kenya. It was a bold step at the time considering very few countries in Africa were making the shift to EMV compliance, placing the country at par with the rest of the world in enhancing fraud mitigation systems. In a press statement by Paynet Kenya in July 2014, Group CEO Bernard Matthewman announced that three Kenyan banks were live on their EMV Chip platform and were already issuing their customers with new generation cards. (IT News Africa, 2014). The press statement however did not reveal the identities of the 3 banks, but at the time, Kenya Commercial Bank which is Kenya's largest bank by capitalization and footprint, led the migration effort with an announcement in

newspapers that it was moving its debit cards to the new EMV system, to improve their customers experience and provide more security. (IT News Africa, 2014).

Equity Bank, one of the largest bank by customer base with 8.4 million accounts, had already begun moving its customers in December 2013 with the issuance of MasterCard-linked EMV debit and credit cards. Other banks like Family Bank, Paramount Bank, Ecobank and Prime Bank made the list of banks that had signed deals with Visa and MasterCard to supply their customers with EMV cards (Business Daily, 2014). By February 2014, data from the Central Bank of Kenya showed there were 11.5 Million cards issued in the country. Kenya Bankers Association estimates that slightly more than 50% of these cards have been replaced with EMV/Chip cards (IT News Africa, 2014).

1.2 Statement of the Problem

A study on the strategies for competitive advantage in the credit card business outlines just how much the use of payment cards has been on the increase in Kenya, with regular shoppers opting for card over cash due to the convenience, safety and reliability offered by cards (Mbogholi, 2009). It is also worth noting that a considerable growth in card usage in Kenya and value of cards transactions in the last two years are a contributing factor to the high loss of funds through payment card fraud. For instance, a research on Kenya's payment card industry recorded the number of payment cards in circulation to be 9.7 million, with a transaction value of KES1.5 trillion (US$18.5 billion) in 2013 (Research and Markets, 2014). This number significantly increased in 2014 as The Central Bank of Kenya data indicated that as of the end of August 2014, the number of debit cards stood at 11.8 million, up from 10.9 million at the end of the first quarter and 11.5 million in the first half of the year (Mail

& Guardian, 2014). If the trend continues, the numbers are expected to go up in 2015 which in turn leads to more loss of funds as a result of payment card fraud.

Studies on payment card fraud response strategies are lacking with most studies either focusing on bank fraud or response strategies in general. Munyua (2013) research on the operations response strategies to payment card fraud by commercial banks in Kenya concluded that commercial banks are utilizing a number of response strategies to deal with card fraud but are in need of legislative and regulatory support. Wanyama (2012) studied the effectiveness of fraud response strategies adopted by Co-operative Bank of Kenya limited. Their findings concluded that know your customer (KYC), use of advance technology, regular audits, real-time monitoring, strong internal controls and data security are some of the strategies being employed by commercial banks to combat fraud. Cheptumo (2010) Study on the response strategies to fraud and related challenges by Barclays Bank of Kenya findings illustrated how weak internal controls, electronic storage of customer data and technological advancement are some of the reasons why fraud happens. Study by Wanjiru (2011) on strategic responses of Equity Bank to fraud related risks, found that fraud impacts negatively on banks profitability as income lost through fraud would have been reinvested towards growth, technology can be used to either favor or combat fraud and the Group Fraud Policy that's applicable to all Equity Banks in the world is very effective.

All these studies do not specifically look at the adoption of EMV card as a way of addressing payment card fraud in Kenyan banks. Therefore the aim of this study is to determine whether adoption of EMV chip card has led to a decline in payment card fraud within the Kenyan Commercial Banks. The study aims to answer the following

questions: a) Does adoption of EMV cards have any effect on payment card fraud? ; And b) what challenges do commercial banks encounter in the adoption of EMV cards

1.3 Objectives of the study

The main objective of the study was to determine whether adoption of EMV chip card has led to a decline in payment card fraud within the Kenyan Commercial Banks.

The specific objectives were to:

a) Establish the extent to which commercial banks have implemented the EMV response strategies to fraud.

b) Determine the challenges of using EMV cards in the Kenya.

c) Show the relationship between EMV card adoption and payment card fraud.

1.4. Value of the study

This study will be valuable to operations and IT managers in commercial banks in assessing the impact of adopting EMV/ chip technology as a strategy for reducing card fraud.

This study will be beneficial to the Central Bank of Kenya in establishing governance policies as they relate to fraud through cards. This study is valuable to the legal sector as it informs on an area that has been unknown and misunderstood, but greatly exploited by criminals. 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.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This literature review will consider bank fraud in general, payment card fraud, the operational response strategies that are currently in place to manage payment card fraud and adoption of EMV technology as an effective operational response strategy to payment card fraud. It will also explore the various challenges towards effective execution of EMV as an operational response strategy.

2.2 Theories

Some of the theories that can be applied in this study include; Technology acceptance theory. This theory posits that perceived usefulness and eases of use; determine an individual's intention to use a system with intention to use serving as a mediator of actual system use. Perceived usefulness is also seen as being directly impacted by perceived ease of use (Venkatesh, Morris, Davis, & Davis, 2003). The adoption of EMV technology can be seen to be affected by the impact it has in reducing payment card fraud as well ease with it its implementation will occur.

Another theory which can be applied is the Delone and McLean IS success model. DeLone and McLean reviewed the existing definitions of IS success and their corresponding measures, and classified them into six major categories. They created a multidimensional measuring model with interdependencies between the different success categories (DeLone & McLean, 1992). This theory can be applied to study the impact of adoption of EMV technology in the Kenyan banking sector. The success of EMV technology in curbing payment card fraud can be studying by looking at definitions and measures of IS success according to Delone and McLean model.

In my research I will apply the task-technology fit theory. Task-technology fit (TTF) theory holds that IT is more likely to have a positive impact on individual performance and be used if the capabilities of the IT match the tasks that the user must perform (Goodhue. & Thompson, 1995). Goodhue and Thompson (1995) found the TTF measure, in conjunction with utilization, to be a significant predictor of user reports of improved job performance and effectiveness that was attributable to their use of the system under investigation. The Goodhue and Thompson (1995) model operates at the individual level of analysis but (Zigurs & Buckland, 1998) presented an analogous model operating at the group level. Since the initial work, TTF has been applied in the context of a diverse range of information systems including electronic commerce systems. I will try to use the theory as a significant predictor of decline of transaction fraud due to the use of EMV technology.

2.3 Bank Fraud

Bank fraud has been defined as a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank (Chakrabarty, 2013). This definition suggests that bank fraud in general is in most cases perceived in the context of electronic banking. The most common types of bank fraud with regard to electronic banking are; Cheque fraud, Electronic fraud, Identity theft fraud and Credit/Debit card fraud.

Cheque fraud occurs when a cheque is used to gain financial advantage by: altering the cheque's payee or amount without required authority, theft of legitimate cheques and then altering them, duplication or counterfeiting of cheques, using false invoices to get legitimate cheques, depositing a cheque into a third party account without authority or depositing a cheque for payment knowing that insufficient funds are in the account to cover the deposited cheque (ANZ Banking Group Ltd, 2015).

Electronic fraud occurs when the banks' customers are targeted with Electronic Funds Transfer Crime; Identity-Related Crime; On-line Share-market Manipulation. (Smith, 2002) It therefore suggests that any form of dishonesty that entails the use of the Internet as the target or means of obtaining some financial reward can be regarded as E-fraud.

Identity Theft Fraud happens when fraudsters access enough information about someone's identity to commit identity fraud. Identity theft fraud can take place whether the victim is alive or deceased (Action Fraud, 2015). Such information is obtained from Theft, including theft of mail from your mailbox at home, going through the victim's garbage bins, Telephone, Fax and Mail scams or even over the Internet through pop up advertisements that require you to give your personal details. This type of fraudster uses your Date of birth, Utilities bills like phone, electricity and water bills and your Address details to assume your identity.

2.4 Payment Card Fraud

Payment card fraud occurs in two distinct transaction environments that are; card-present and card-absent, each of which offer unique card acceptance and fraud issues

(Visa International, 2010). According to the Ministry of Finance (2012), the various types of Payment card fraud as outlined by the ministry of include;

Card stolen fraud; which is theft of a payment card or its unauthorized use by a party other than the cardholder. This may occur through trapping the card in an ATM or physical theft of the card. Payment Card fraud can occur also in cases in which the payment card is intercepted and stolen during the period from when it is sent by the issuer until when it is received by the legitimate cardholder at his or her postal address. This type of fraud is referred to as card not received fraud. Transactions on articles of high value such as jewelry, luxury items, are done immediately on the card often before the legitimate cardholder becomes aware of the theft and before the card has been ordered frozen

Card lost fraud; this is the illegal use of payment card found after being misplaced by the legitimate cardholders. Card lost fraud is difference to card stolen fraud by fact that the illicit action is derived from the accidental misplacement of the card, and not from its voluntary theft

Counterfeit card fraud; involves a material change to a payment card aimed at recording, transferring, cloning, altering or replacing the data contained in the card in order to permit illicit transactions either concurrently or subsequently. This type of fraud includes various activities such as physical carding, re-encoding, skimming and shoulder-surfing, that compromise the cardholder's card data. Payment Card data compromise can occur when individuals gain unauthorized access to digitized card information through interception on a remote network or on a physical workstation through use of key-logging software. Card data can also be fraudulently acquired through false electronic mail messages addressed to the legitimate cardholder with

aim of causing him or her to directly reveal his/her card details, a process known as phishing. Card information can also be acquired from discarded purchase receipts, accounting documentation or receipts from banking tellers or counters. Card numbers may be reproduced illicitly through sophisticated computer programs that allow the reproduction of the algorithms used to assign PIN codes. The PIN codes can also be acquired through use of hidden miniature cameras- a technique known as shoulder-surfing.

Another more recent type of Payment card fraud is account takeover fraud, which occurs when a card is used with a false identity in which a cardholder's personal information is fraudulently used to access an account in the cardholder's name. It is a type of fraud that relies on stolen card data to purchase goods from the internet, mail order, or telephone merchants or to counterfeit a payment card and use it in an ATM cash withdrawal or in a face-to-face transaction at a point-of-sale (POS). Card Not Present (CNP) transactions are the most vulnerable to stolen data because payment cards can-not be inspected (Sullivan, 2010).

2.5 Operational Strategies to Payment Card Fraud

Strategy refers to a plan of action designed to achieve a particular goal. Strategy is the match between an organization resources and skills and the environmental opportunities it wishes to accomplish. It is important to provide guidance and direction for the activities of the organization. It is the process by which managers set an organization's long term course, develop plans in the light of internal and external circumstances, and undertake appropriate action to reach those goals (Scholes, Whittington, & Johnson, 2002). In relation to this research, the "Action" referred to here are the strategies employed in managing Payment Card Fraud by commercial

banks in Kenya. Such operational response strategies that are in place include; Organizing and attending anti-money laundering workshops by Banking institutions to train its staff on detecting cases of bank related fraud and putting up internal control measures that encourage staff on desisting from committing fraud themselves. This strategy considers both internal and external fraud cases.

Implementing card management systems that speeds up transaction times in order to curb fraud. In 2013, VISA international announced the launch of Visa Personal Payments (VPP) in collaboration with Equity Bank. The VPP is multi-currency; multi-company, multi-country system has a capacity of 35 million accounts and a processing speed of 300,000 transactions per minute. This system is supported by Way4, an online Card Management System that has multi-institution and multi-currency transaction processing capability and has the ability to handle over 60 million cards with speed performance of 180,000 transactions per minute (Equity Bank, 2013). The system's security precaution is demonstrated when you visit the unique link which will be provided to you via text message as you are doing your transaction. The browser you are using should display the secure padlock symbol that indicates you are on a secure webpage. If your browser shows a security warning, or the padlock is not visible, you should not enter your card details. Considering the number of transactions that the VPP handles, the more other banks use, and the more fraudulent transactions will decrease (Equity Bank, 2013).

Instituting multi-level access points where staff members have different access rights in the system, password management and a rigid recruitment process. In cases where the required number of access authorizers do not approve a transaction, the subject transaction will be held pending for a certain period of time – as per the banks'

guidelines on such circumstances. This period will allow sufficient time for the transaction to be authorized and any transaction still requiring additional authorizations after this specified period will be automatically deleted. They different access rights can be: None - no information will be displayed to the User, View only- can create payees, billers and payers but not execute payments, Create No View - can setup payments for processing and is not counted as an authorizer and cannot authorize payments created by other users. Balances, pending payments and transaction history are not viewable, Create View - can setup payments for processing but is not counted as an authorizer and cannot authorize payments created by other users, Execute View - Full access for account within limits and payment actions allowed, Execute No View - Full access for account within limits and payment actions allowed. Balances, pending payments and transaction history are not viewable. Multi-level authorization access makes it harder for fraudsters as it improves the likelihood of detecting a suspect transaction at one of the levels before the transaction completes (Technology Banker, 2012).

Use of financial services software to improve corporate governance and aid in risk management. Of particular notice are the Oracle Mantas Anti Money Laundering Fraud products. It provides an enterprise platform enabling efficient detection, investigation, and reporting of suspected money laundering and terrorist financing activity. It also provides regulators with a comprehensive view of financial activity, reduces compliance costs through streamlined investigations, saves time and lowers the staff costs (Technology Banker, 2012).

Sending the card and pin separately instead of together. This is strictly for security purposes, when you receive a new debit card, the PIN number is sent in a separate

envelope so that in case it is lost in the mail the card and PIN number are not together. It is very effective in protecting the cardholder from card lost fraud and card stolen fraud (Technology Banker, 2012).

The Anti-Money Laundering Act to fight against bank crime. All financial institutions are required to submit suspicious transactions and Cash Threshold Reports to the Financial Reporting Centre which are used to facilitate the consolidation of financial intelligence for analysis (Technology Banker, 2012).

2.6 EMV as an Operational Response Strategy to Payment Card Fraud

EMV chip technology has become the global standard for credit card and debit payment cards. The technology sets standards for operation of chip cards, point-of-sale terminals and ATMs. It was established in 1994 by Europay International, which was later acquired by MasterCard in 2002. Today, the EMV standard is managed by EMVCo which is a joint venture consisting of MasterCard, VISA, American Express, JCB, Discover, MasterCard, and UnionPay as equity partners (Engenico Group, 2012)

Payment Card Fraud in non-EMV countries is above the global average and is still on the rise. The Aite Group reported that the fraud rate recently doubled in the US from 5 to 10 basis points. Furthermore, the lessons learned from the many migration activities worldwide clearly indicate that fraud is shifting towards those regions that have not yet implemented EMV chip technology (from Malaysia to Thailand, and from the UK to mainland Europe, etc.). As the rest of the world has either already migrated to EMV or has firm plans to do so, if countries do not follow suit, they could

become the primary target of fraudsters and fraud rates will continue to rise (Gemalto, 2015).

2.6.1. Challenges in Adoption of EMV Technology

The EMV standard has received considerable attention from stakeholders in the global payment card industry. According to KBA's CEO Habil Olaka, Kenya is now one of the few countries in Africa to adopt the EMV standard at an industry level, placing the country at par with other leading countries in enhancing fraud mitigation systems (CAPITAL FM, 2014). As effective as EMV is in dealing with fraud, the following challenges associated with its adoption also need to be taken into account;

Lack of clear guideline on EMV technology to use. The Kenya bankers association did not give clear guidelines on the required implementation with some institutions implementing chip without the Pin authentication for POS transactions. This negates the benefits of adoption of the technology. Also cards being issued still have the magnetic strip on the back of the card which weakens any benefits of having the EMV technology in the first place (Vijayan , 2014).

Tight migration timelines to new platforms. According to KBA CEO Habil Olaka, upgrading of ATM infrastructure was to be done by August 2013, POS infrastructure was to be complete by December 2013 and issuing of Cards was to be done by March 2014. All banks are yet to complete issuance of EMV cards with some yet to begin the process. Mr Olaka attributed this to the large quantity of cards that need to be issued and delays by customers in picking up their cards (KBA, 2015).

Slow adoption of the EMV standards. Some banks are slow to issue EMV chip cards in the market. This may cause products such as mobile payment to hurt the

competitive position of ATM and POS transactions for commercial banks (THALES, 2015). The more popular mobile payments become the more revenue loss by commercial banks with regard to ATM and POS transaction activity.

Unsecure Card issuing processes. Customer and account information can be stolen if card issuing processes are not secure (Thales, 2015). In cases where the bank outsources card processing to other institutions, it is up to the bank and the institution to come up with a secure system that will protect the cardholders from any form of fraudulent activity.

Inadequate conformance to compliance obligations can result in fines and reputational risk, damaging your position in an increasingly competitive market (Thales, 2015). This is mostly illustrated by the liability shift in the EMV migration process. This liability shift means that banks are liable for money lost in a fraudulent transaction carried out using non-compliant cards after the agreed deadline set by banks has passed.

The high cost of EMV migration. According to Okoth (2014), the costs of EMV migration has been quite an undertaking as EMV certification costs between $6,000 and $10,000 (KSh525,000 and KSh875,000) per institution. System upgrades cost much more and vary depending on the vendor. A number of banks have had to outsource their cards systems to third party processors due to the cost implications, while others had to procure completely new card management systems. The same has been collaborated by an article on the standard newspaper on 20th May 2014 (Standard Newspaper, 2014).

Inflexible processes and overreliance on legacy systems - outdated computer systems that are used instead of available upgraded versions, could create operational silos that

drive up costs and business risk. Part of the delay in EMV migration is reportedly aided by the fact that the old magnetic strip cards continue to be accepted by the new EMV-compliant ATM machines.

2.7 Summary

This literature review has identified the operational response strategies to fraud in commercial banks, EMV chip cards as a response strategy and the challenges faced in implementing EMV chip cards. Although this study focusses on Payment card fraud, other types of fraud are also mentioned while pointing out that most types of bank fraud are associated with electronic banking. As effective as some of the operational response strategies are, the use of EMV technology as the most effective response strategy is emphasized, with a more detailed account of how EMV conforms to global standards and how these standards are to be employed by Kenyan commercial banks to combat fraud. In addition, there is an overview the challenges Kenya's commercial banks have encountered when using EMV technology.

2.8 Conceptual Framework

The conceptual framework below demonstrates the effect of adapting EMV cards to Payment card fraud. We will be looking at institutions which have adopted EMV technology and those that are yet to adopt. It also illustrates some of the intervening factors that also influence payment fraud. We will study the reduction of payment fraud by looking at the reduction or increase in the different types of payment card fraud.

Independent Variable **Dependent Variable**

I

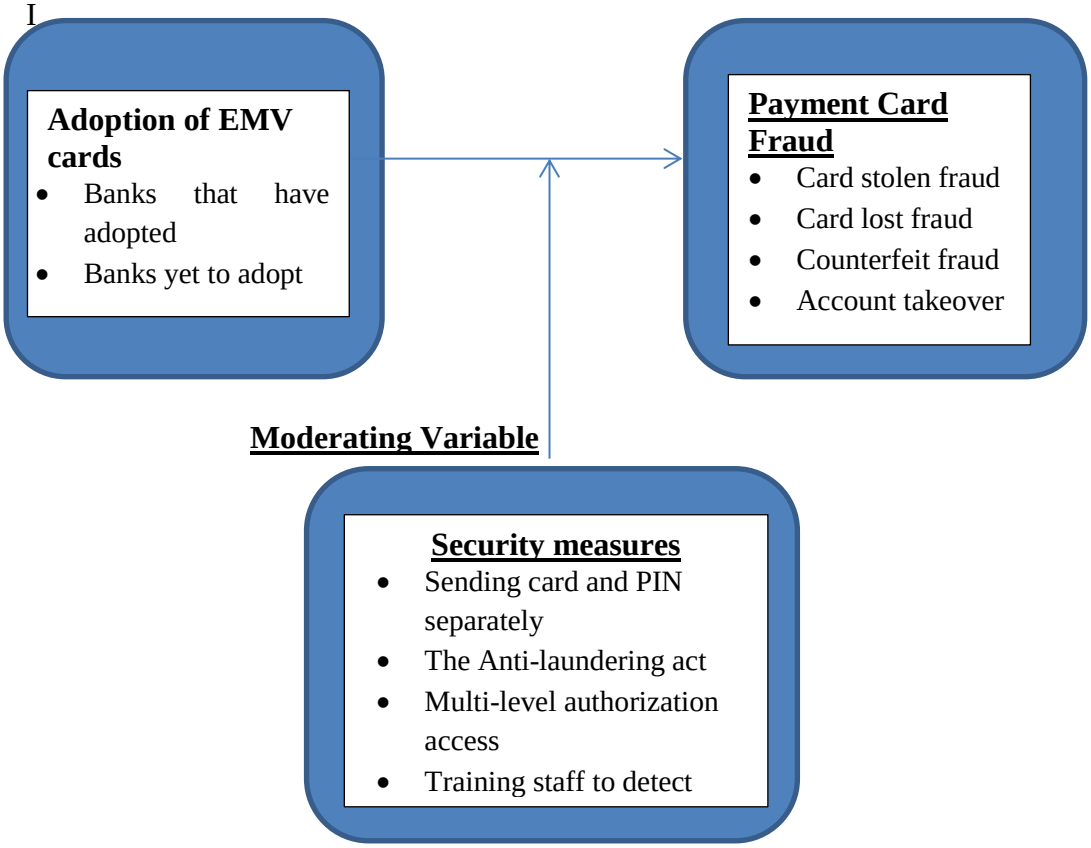

Figure 1: Conceptual Framework

CHAPTER THREE: RESEARCH METHODOLOGY

3.1.Research Design

The descriptive research study was used to provide a focused and detailed insight to EMV technology being employed by commercial banks in Kenya as a response strategy. The data collected was used for both qualitative and quantitative analysis to measure the effectiveness of using EMV technology.

3.2.Target Population

The target population consisted of all commercial banks in Kenya that have issued payment cards that are either EMV or magnetic stripe. A census study was conducted on the target population. The study focused on operations managers and information technology managers with expert knowledge on cards and card fraud.

3.3.Data Collection

This study used primary data. The data Primary data was obtained from operations managers and information technology managers. The data captured EMV adoption as a management operational response strategy to payment card fraud and its level of effectiveness.

A questionnaire in structured form was administered to collect primary data. It was administered through electronic mail to operations managers and information technology managers. The questionnaire was composed of three sections namely: Section A which covered demographic information of the respondents, Section B which focused on challenges and section C focusing on payment card fraud.

3.4.Data Analysis

The collected data from the field was analyzed to answer the research question; has adoption of EMV chip card led to a decline in payment card fraud within the Kenyan Commercial Banks.

Objective a) the extent to which commercial banks have implemented the EMV response strategies to fraud will be established using descriptive statistics.

Objective b) the challenges of using EMV in the country will also be determined using the following descriptive statistics.

Objective c) The relationship between EMV adoption and payment card fraud will be established using the following regression model using the formula;

$$\mathbf{Y = a_0 + a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 + e}$$

Whereby;

Y = Payment card fraud

X_1 = Adoption of EMV cards

X_2, X_3, X_4 = Security measures

a_0 = Constant

a_1 a_2 a_4= regression coefficient

e = error term

The responses from the questionnaire were coded to facilitate statistical analysis by use of descriptive statistics. A five point Likert scale was used to measure the psychological attitudes, preferences and subjective reactions on managers to decision

variables. The responses were coded with figures of 1 to 5 representing various levels and directions of decisions and preferences.

In analyzing data, sample means and standard deviations of the responses will be calculated. Descriptive statistics, mainly percentages will be used. Bar graphs, tables and pie charts will be used to present the findings of the study. This is because of their ability to bring relative form to the otherwise abstract nature of the influences under investigation in research.

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1. Introduction

This chapter outlines the results of the data analysis. The data from the completed questionnaires was summarized and tabulated in the form of percentages and frequencies. The data was gathered primarily from the questionnaire that was designed in line with the objectives of the study and also from secondary sources.

4.2. General Information

This section presents factors relating to payment card fraud from information gathered from respondent banks. It highlights: the type of cards issued, the average number of cards issued, the preferred transaction channels, the perceived card fraud trend by transaction environment and the prevalence of the various fraud types is presented, the challenges faced by the respondent banks and the perceived level of support from legislature, regulator and card schemes towards addressing the fraud challenge.

Figure 2 below shows the percentage of the type of cards issued by the respondent

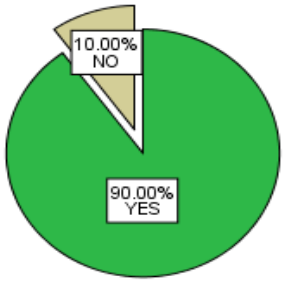

Figure 2 percentage of type of card issued

90 percent of the respondents have issued EMV chip cards to the market. While 10% of the respondents are yet to issue the chip cards.

Figure 3 below shows the distribution of number of cards issued by the respondents

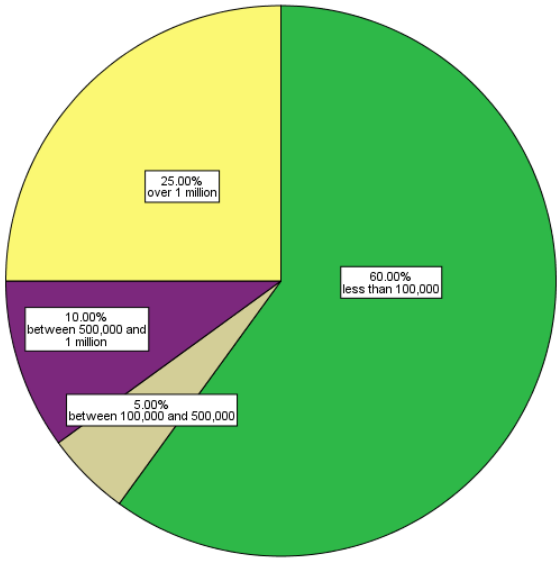

Figure 3: Distribution of card issued.

Of the respondents 60% issued less than 100,000 cards. 5% issued between 100,000 and 500,000 cards, 10% issued between 500,000 and 1 million cards while 25% issued over 1 million cards.

Figure 4 below shows card usage at POS merchants

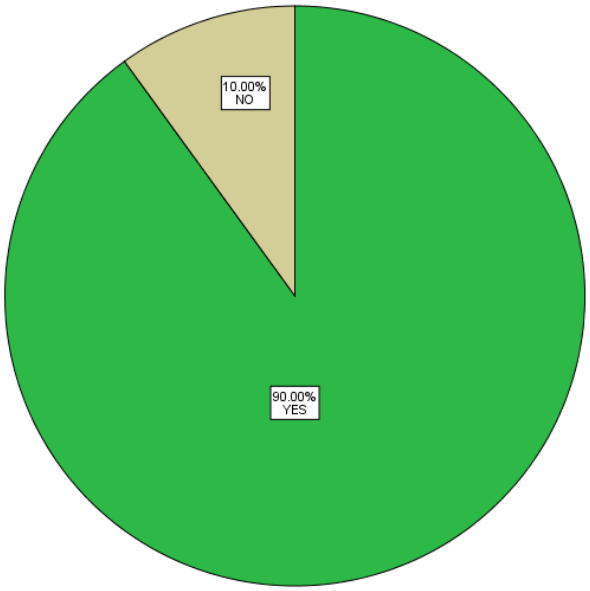

Figure 4: Card usage at POS merchants.

90% of the respondents' customers use their card at POS merchant locations while 10% do not. This can be attributed to the increased preference of making payment using cards as opposed to carrying cash. The government has been in the forefront in advancing a cash lite society

Figure 5 below shows card usage at ATM points

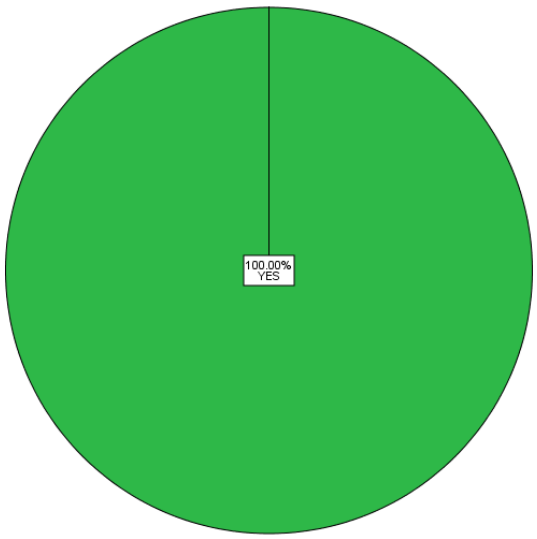

Figure 5: Usage of cards at ATM

All the respondents' customers use their cards at ATM points. This is probably because customers are issued payment cards to access funds in their accounts. The payment cards make it easier to get cash any time of the day. The result could also be because of the large number of card issued are debit cards whose main purpose is account access.

Figure 6 below shows card usage at online merchants

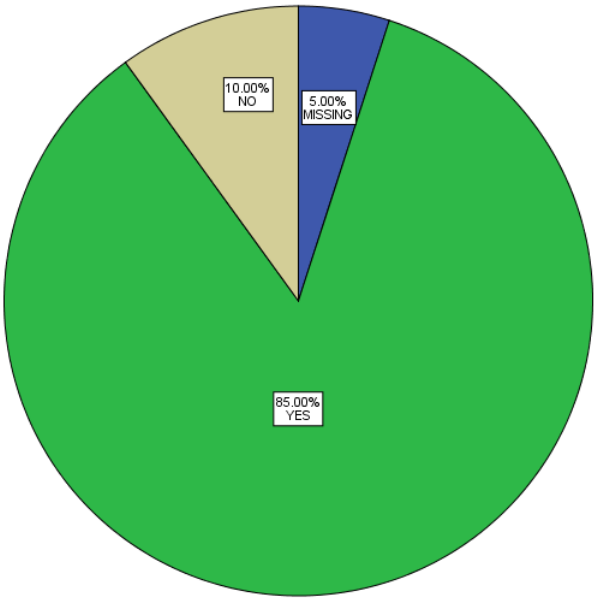

Figure 6: Usage at for online payments

85% of the respondents' customers use their cards to pay for goods and services online. 10% do not use their cards to make online payments. 5% of the respondents refrained from responding to the question. The high usage of payment card for online payment can be attributed to the progressive increase in ecommerce in the Kenya market. The advancement of ecommerce sites like www.Jumia.com giving opportunity for purchasing of goods and service at any time and from any location as long has the buyer has access to the internet.

Table 1 below show the other strategies employed by the respondents to combat fraud.

	Card and pin issued separately	Anti Money Laundering Act by Bank	Multi-level authorization access by bank	Regular Employee Training On Fraud
Mean	1.50	1.00	1.00	1.00
Median	2.00	1.00	1.00	1.00
Std. Deviation	.761	.000	.000	.000

Table 1: Other Methods of Card fraud prevention

From the responses it is clear issuance of the Pin by different people is the most used fraud prevention strategy. The most utilized fraud prevention strategy is issuance of card and pin separately. This is probably because it is the easiest to implement. Implementation of anti-money laundering act, multilevel authorization access and regular employee training are in use in combating card payment fraud.

4.3. EMV as an Operational Strategy

Table 2 shows the challenges in adopting EMV chip cards

Challenges In Adopting EMV Chip Cards			
	Mean	**Median**	**Std. Deviation**
Lack of guidelines has slowed down the adoption of EMV	2.85	3.0	1.226
Enough time was given for EMV cards roll out	2.95	3	1.099
Slow EMV adoption affects the bank's reputation	3.40	3	1.392
EMV increases card data security	2.60	2	2.062
Banks relay on legacy or inflexible systems	2.70	3	1.174
Delayed adoption of EMV has increased mobile payments	2.65	2	1.599

Liability shift will spur bank to support quick EMV adoption	3.55	3.50	1.317
CBK has supported combating fraud	3.20	4	1.152
The justice system is well equipped to deal with fraud	2.00	2	.973
KBA's card security programs deal with fraud effectively	2.45	3	.945
Major card schemes support tackling card payment fraud in Kenya	2.70	2.5	1.081
My organization has suffered reputational damages	2.70	3	.865
Other challenges	1.00	1	.858

Table 2 Challenges in adoption of EMV

The respondents experienced various challenges during the roll out of the EMV chip cards. The respondents agree the central bank is providing sufficient support in combating payment card fraud. Most respondents disagree with the notion that the justice system in Kenya is well equipped in handling card fraud. The respondents also agree liability shift will speed up adoption of EMV technology. This is probably due to that fact that banks will bear the cost of fraudulent transactions carried out with magnet strip cards. They agree that the lack of clear guidelines on EMV technology to use, has slowed the adoption of the technology. The KBA did not give proper guideline on the EMV technology to be adopted. This made it difficult for the banks to quickly move to |EMV technology.

The CBK has been in the forefront in supporting the fight against payment fraud. However, the justice system is still lagging behind the other players i.e. the KBA, CBK and the major card schemes

Table 3 show challenges in managing card payment fraud

Challenges In Managing Card Payment Fraud			
	Mean	**Median**	**Std. Deviation**
When to block and reissue	3.10	3.00	1.683
Communicating to customer about fraud event	2.70	3.00	.923
Lack of automation and tools	3.55	3.50	1.146
Inadequate personnel	2.15	2.00	.875
Lack of clear policies, procedures and guidelines	2.00	2.00	1.076

Table 3: Challenges in Managing Card Payment Fraud

The respondents agree greatest challenge to managing payment card fraud has been the lack of automation and tools. The lack of automation and tools due to the high cost involved in procuring, installation and running these systems. Other challenges include identifying when to block compromised cards and when to communicate to the customer about fraud on their card. Inadequate personnel and lack of clear policies were not seen as big challenges by the respondents.

Table 4 below shows organization exposure to payment card fraud

Organization Exposure To Payment Card Fraud			
	Mean	**Median**	**Std. Deviation**
Attempted card fraud in last six months	3.25	3.00	1.020
Actual card fraud in the last six months	3.40	3.00	1.188
Card fraud incidences have decreased in last six months compared to the previous six months	3.55	3.00	.826
Lost card fraud experienced this year	2.75	3.00	.786
Stolen card fraud experienced this year	2.80	3.00	.834
Experienced counterfeit fraud at POS this year	2.05	2.00	.826

Experienced counterfeit fraud at ATM this year	2.50	2.00	1.277
Account take over fraud experienced this year	2.55	2.00	.826
Experienced data breaches on our card systems	1.85	2.00	.489
Experienced data breaches on our merchant systems	1.85	2.00	.489
Card present fraud has been on the increase in our organization	1.85	2.00	.671

Table 4: Organization exposure to payment card fraud

The respondents were none committal on the frauds experienced during the last six months. The respondents showed they had not experienced different types of payment card fraud in the last one year. The low response rate on the above exposure can be attributed to the respondents protecting their organization from reputation loss. Commercial banks closed guard fraudulent cases, to protect the institutions from bad publicity.

Table 5 below shows statistics on different frauds experienced in the last six months.

Statistics

	Reported payment card fraud in last 6 months	**Reported cards stolen fraud in last 6 months**	**Reported cards lost fraud in last 6 months**	**Reported counterfeit fraud in last 6 months**	**Reported account take over fraud in last 6 months**
Mean	1.90	1.95	1.80	1.70	1.65
Median	2.00	1.00	1.00	1.00	1.00
Std. Deviation	1.071	1.356	1.322	1.174	1.387

Table 5: Fraud statistics in the last 6 months

The respondents indicated that in the last six months banks less than 10 cases for each type of fraud. Overall respondents reported total card fraud of between 100 and 1000 cases

Table 6 shows the model summary

Model Summary

Mode	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.287[a]	.083	-.025	1.085

a. Predictors: (Constant), Card and pin issued separately, EMV Cards Issued

Table 6: The model summary

From the analysis there is a low degree of correlation between card payment fraud and EMV card adoption. The total variation of the dependent variable that can be explained by the independent variable is only 8.3%

Table 7 showing how well the regression equation fits the data

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.800	2	.900	.765	.481[b]
	Residual	20.000	17	1.176		
	Total	21.800	19			

a. Dependent Variable: reported payment card fraud in last 6 months

b. Predictors: (Constant), Card and pin issued separately, EMV Cards Issued

Table 7: Regression equation fit

Here, $p = 0.481$, which is more than 0.05 and indicates that, overall, the regression model does not statistically significantly predicts the outcome variable.

Table 8 shows relationship between EMV adoption and card payment fraud.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.000	.969		3.096	.007
	EMV Cards Issued	-1.000	.830	-.287	-1.205	.245
	Card and pin issued separately	2.671E-018	.336	.000	.000	1.000

a. Dependent Variable: reported payment card fraud in last 6 months

Table 8: Coefficients table

The regression equation is $\mathbf{Y = 3 - 1_{X1} + 0.000000000000000026710x_{2+}e}$

4.4. Discussions of the Finding

The objective of the study was to find out the relationship between adoption of EMV card technology and the reduction of payment card fraud. The study found that majority of the banks had adopted EMV technology as a way of mitigating payment card fraud with 90% of the respondents having adopted the technology.

All the banks in the study showed their customers use of their card at ATM terminals with 90% using their cards at POS merchant sites. 85% of the respondents indicated their customers made payment online using their debit cards. The different channels show the susceptibility of bank customers to fraud through the various channels.

Apart from the use of EMV chip cards commercial banks on Kenya have also adopted other methods to mitigate against payment card fraud. The most utilized method is the issue of payment cards and pin by different personnel at 33.33% with the rest of the methods i.e. use of multi-level authorization system, anti-laundering act and regular training of employees being applied equally across all respondents.

Most of the respondents believe liability shift will speed up adoption of EMV technology as the banks try to mitigate against losses from the shift. This is also seen as a challenge by the banks. Some of the other challenges bank have experienced in adoption of EMV cards include slow adoption affecting reputation of the bank with 16.73%, insufficient time to adopt EMV technology at 14.25%, lack of clear guidelines at 13.77% and banks use of legacy systems at 13.04%.

The respondents in the study felt that support offered by the criminal justice system in addressing payment card fraud is inadequate. The criminal justice system was faulted for lengthy processes and light sentences. Respondents indicated that banks bear the burden of proof in times while there is limited knowledge in regard to payment card fraud among prosecutors and the police. The central bank of Kenya has been praised for putting in place guidelines that relate specifically to payment cards and payment card fraud but still is required to do more. Major card schemes such as Visa, MasterCard and Union Pay continually engage the commercial banks on card risk management practices whilst providing regulations to assist banks in resolving fraud related disputes.

The study established some of the challenges facing commercial banks in addressing payment card fraud as lack of automation and use of legacy systems. Card fraud management systems require substantial investment compared to the perceived return. The study further established that most banks have suffered reputational damage as a result of payment card fraud incidences and are reluctant to communicate to their customers about card fraud incidents.

This study shows that there is low correlation between payment card fraud and adoption of EMV chip cards. The regression model adopted does not statistically significantly predict outcome variable.

CHAPTER FIVE SUMMARY CONCLUSIONS AND RECOMMENDATIONS

5.1. Introduction

The Kenyan payment card space has been growing exponentially over the last couple of years. This has brought about increase on payment card fraud. KBA and CBK took an initiative to protect the payment card industry by pushing for the migration of all payment card platforms to EVM technology. The banks were to issue new EMV chip cards and upgrade their infrastructure to process EMV chip cards. Most of the commercial banks have implemented the initiative but some are still lagging behind especially in issuance of chip cards.

My study focused on finding out is there was a decline on payment card fraud after the introduction of EMV chip card in the Kenyan payment card industry. The specific objective of my study were to: a)Establish the extent to which commercial banks have implemented the EMV response strategies to fraud; b) Determine the challenges of using EMV cards in the Kenya; c) Establish the relationship between EMV card adoption and payment card fraud.

5.2. Summary of the Finding

From the study carried out I was able to test my objectives and the results were as below.

On the first objective of the study, majority of the commercial banks have adopted the technology with 90% of the respondents already issuing EMV chip cards.10% of the respondents were yet to issue EMV chip cards to their customers.

On the second object of the study, I found several challenges that have slowed down adoption of EMV technology which include unrealistic timeline to make the change from magnetic strip to chip cards, use of legacy systems, and lack of clear guideline on the EMV technology to be adopted.

The criminal justice system in the country has also been faulted for not offering sufficient support to combat payment fraud. CBK is seen to offer most support in combating card payment fraud in the country. The major card schemes and KBA's card security system are also seen to offer some support in combating card payment fraud.

The third objective of the study is to establish a relationship between EMV chip card adoption and card payment fraud. This was not proved by the study. This could have been due to the limited responses. Only 23 responses were provided from a population of 43 banks.

5.3. Conclusion

The number and value of payment card transactions have increased exponentially; as have the channels to conduct transactions. There is a push for card payment in the transport sector, as well as an increase in online stores which reach a wider market; the most likely mode of payment will be payment cards. Payment card fraud is a challenge that presents challenge to such endeavors. It is becoming more challenging as information communication technology advances and its impact is being felt by commercial banks and their customers. Proceeds from payment card fraud are being used to fund criminal activities, increased losses to commercial banks and increased customer inconvenience.

This study has established that commercial banks are aware of the challenges payment fraud caused and requirements necessary to minimize payment card fraud. Adoption of EMV is one of the methods fronted to reduce fraud; however this too has its challenges as highlighted in the study.

5.4. Recommendations

There is need for more involvement in the process of EMV adoption by the central bank. So far the need to move to the EMV platform has been spearheaded by KBA with little assistance from the central bank. This has given commercial banks room to not fully comply with the EMV adoption requirement as per the set timelines. There is need for the central bank to take control to ensure all commercial banks are compliant.

The government should offer tax incentives to reduce the cost involved in adoption of EMV technology. The high cost of infrastructure is a major cause of slow adoption. The government can assist by offering tax break to enable the country adopt faster. By offering tax break the government will also make it cheaper for bank customers to acquire chip cards at a lower cost.

5.5. Limitations of the study

The study focused only on commercial banks in Kenya leaving out other financial institutions issuing payments cards. Another limitation is the sample of the study because out of the forty three (43) commercial banks only 23 responded. The study would have given a better insight of the impact of EMV adoption on payment card fraud if all the commercial banks responded. The payment card industry in the Kenya is still developing, a mature industry would present other response strategies to

payment fraud that can be adopted by not only commercial banks but other financial institutions. The limited response on the fraud occurrence made it difficult to calculate the correction between payment card fraud, the EMV adoption and other moderating variables.

5.6. Suggestions for further research

As all commercial banks in Kenya roll out EMV chip cards, it presents an opportunity to learn the impact of its adoption and study if the return on investment is worth the cost of adoption.

REFERENCES

Action Fraud. (2015). Retrieved from http://www.actionfraud.police.uk/fraud_protection/identity_fraud

ANZ Banking Group Ltd. (2015). *Personal> Ways to bank> Types of banking fraud*. Retrieved February 27, 2015, from Austrailian and New Zealand Banking group Web site: http://www.anz.com/personal/ways-bank/security/online-security/threats-banking-safety/fraud-types/

BUSINESS DAILY. (2014, March 19). John Gachiri. *Banks falling behind schedule for secure ATM cards switch*. Retrieved from http://www.businessdailyafrica.com/Banks-race-to-beat-deadline-for-ATM-cards-migration/-/539552/2249406/-/107infl/-/index.html

CAPITAL FM. (2014, April 28). Kennedy Kangethe. *70pc of bank cards in Kenya are EMV compliant*. Retrieved from http://www.capitalfm.co.ke/business/2014/04/70pc-of-bank-cards-in-kenya-are-emv-compliant/

Central Bank of Kenya. (2015). Retrieved from www.centralbank.go.ke: https://www.centralbank.go.ke/index.php/bank-supervision/forex-bureaus/14-bank-supervision/82-licensed-forex-bureau; https://www.centralbank.go.ke/index.php/bank-supervision/microfinance-institutions/14-bank-supervision/83-list-of-licensed-deposit-taking;

Central Bank of Kenya. (2015). Commercial Banks & Mortgage Finance Institutions. *Commercial Banks & Mortgage Finance Companies - (PDF format, 217KB)*. Retrieved April 7, 2015, from https://www.centralbank.go.ke/images/docs/Bank%20Supervision%20Reports/Commercial%20Banks%20Directrory%20-%2013%20December%202011.pdf

Chakrabarty, D. K. (2013, July 26). *Frauds in the Banking Sector: Causes, Concerns and Cures.* Retrieved from Reserve Bank of India Web site; Speeches tab: http://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826

Charles, M. (2014, April 28). BUSINESS DAILY. *Banks say customers delaying switch to new cards ahead of second deadline*. Retrieved from http://www.businessdailyafrica.com/Banks-say-customers-delaying-switch-to-new-ATM-cards-/-/539552/2296566/-/o3ea9y/-/index.html

Cheptumo, N. (2010). *Response Strategie to Fraud Related Challenges by Barclays Bank of Kenya.* Nairobi: Unpublished MBA Project of the University of Nairobi.

Creditcall Ltd. (2015). *What is EMV Chip Card Technology?* Retrieved May 20, 2015, from Level2Kernel: https://www.level2kernel.com/emv-guide.html

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research (3:1)*, 60-95.

EMVCo. (2011, May). A Guide to EMV. 17. Retrieved from http://paysmart.com.br/wp-content/uploads/2013/03/EMVCo-A-Guide-to-EMV.pdf

Engenico Group. (2012). *Europay, MasterCard & Visa - EMV - Frequently Asked Questions.* Retrieved from http://ingenico.us/wp-content/uploads/2012/07/Ingenico-EMV-FAQ-07052012.pdf

Equity Bank. (2013, May 23). Retrieved from www.equitybankgroup.com: http://equitybankgroup.com/index.php/blog/2013/05/visa-and-equity-bank-launch-new-money-transfer-service-visa-personal-payments

Gemalto. (2015, May). *EMV brings powerful security for every transaction*. Retrieved May 10, 2015, from http://www.gemalto.com/emv/security

Gemalto. (2015). *Gemalto's EMV Case Study Booklet: share the experiences of financial institutions around the globe.* Retrieved March 10, 2015, from www.gemalto.com: http://www.gemalto.com/financial/inspired/17-financial-institutions-share-their-emv-experience

Goodhue., D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quatery*, 213-236.

IT NEWS AFRICA. (2014, July 16). *Paynet extends chip adoption in Kenya.* Retrieved from http://www.itnewsafrica.com/: http://www.itnewsafrica.com/2014/07/paynet-extends-chip-adoption-in-kenya/

KBA. (2015, May 12). Retrieved from http://www.kba.co.ke/media/latest-news/313-banking-industry-successful-in-addressing-card-skimming-with-adoption-of-emv-standards-on-chip-and-pin-technology-for-payment-cards

KBA. (2015, September 1). *KBA Statement on the Banking Industry's Migration to the EMV Standard.* Retrieved from www.kba.co.ke: http://www.kba.co.ke/home/92-latest-news/277-kba-statement-on-the-banking-industrys-migration-to-the-emv-standard

Mail & Guardian. (2014, October 30). *Payment cards grow to 12m in Kenya, but use stagnates.* Retrieved from Mail & Gaurdian Africa: http://mgafrica.com/article/2014-10-30-payment-cards-grow-to-12m-in-kenya-but-use-stagnates

Mbogholi, J. M. (2009). *Strategies for competitive advantage in the credit card business: a survey of member banks of the Kenya Credit and Debit card Association.* Nairobi: Unpublished MBA Project of the University of Nairobi.

Mbwayo, M. (2005). *Strategies applied by commercial banks in Kenya in Anti-Money.* Nairobi: Unpublished MBA Project of the University of Nairobi.

Ministry of Economy & Finance. (2012). *Statistical Reprt on Payment Card Fraud.* Rome: Ministry of Economy and Finance in Rome - DEPARTMENT OF THE TREASURY.

Mundi, I. (2014). *Kenya Demographics Profile 2014*. Retrieved January 30, 2015, from Index Mundi - Country Facts: http://www.indexmundi.com/kenya/demographics_profile.html

Mwaniki, C. (2014, April 9). BUSINESS DAILY. *Switch to new ATM cards pushed to May after banks fail to beat deadline*. Retrieved from http://www.businessdailyafrica.com/Switch-to-new-ATM-cards-pushed-to-May-/-/539552/2273112/-/7a9er5z/-/index.html

Mwende, J. (2014, May 24). *Overview of the banking indusry in Kenya.* Retrieved from The Nation Business Review: http://www.kenyanbusinessreview.com/557/banking-industry-in-kenya/.

Njagi. (2009). *effectiveness of know your customer policies adopted by commercial banks in Kenya in reducing money laundering and fraud incidences.* Nairobi: Unpublished MBA Project of the University of Nairobi.

Olingo, A. (2014, November 15). *Kenya's commercial banks lose $9.4m to fraud in just six months.* Retrieved from The East African: http://www.theeastafrican.co.ke/news/Kenyan-commercial-banks-lose--9-4m-to-fraud-in-just-six-months/-/2558/2523802/-/rd9jyuz/-/index.html

O'Mahony Donal, M. P. (1961). *Electronic Payment Systems for E-Commerce 2nd Edition.* Norwood, MA: Artech House Inc. Retrieved February 4, 2015

Research and Markets. (2014, November). *Kenya's Cards and Payments Industry: Emerging Opportunities, Trends, Size, Drivers, Strategies, Products and Competitive Landscape*. Retrieved February 2014, from www.researchandmarkets.com (Online): http://www.researchandmarkets.com/research/zbscq3/kenyas_cards_and

Scholes, K., Whittington, R., & Johnson, G. (2002). *Exploring Coperate Startegy.* New Delhi: Prentice-Hall.

Smith, A. G. (2002, November 13). Identifying and Responding to Electronic Fraud Risks . *30th Australasian Registrars' Conference Canberra; Australian Institute of Criminology*. Retrieved from http://www.aic.gov.au/media_library/conferences/other/graycar_adam/2002-11-registrars.pdf

STANDARD NEWSPAPER. (2014, May 20). Jackson Okoth. *Transition hitches as migration to chip ATM cards nears tail end*. Retrieved from http://www.standardmedia.co.ke/business/article/2000121705/transition-hitches-as-migration-to-chip-atm-cards-nears-tail-end

Sullivan, J. R. (2010). FEDERAL RESERVE BANK OF KANSAS CITY. *The Changing Nature of U.S. Card Payment Fraud: Industrryand Public Policy Options*, 101-133.

Technology Banker. (2012, January). *Fraud Solutions for Africa Banks – A Kenyan Perspective.* Retrieved from Technology Banker: http://www.technologybanker.com/security-risk-management/fraud-solutions-for-africa-banks-a-kenyan-perspective#.VM_5gnspo9w3.

THALES. (2015). *EMV and Payment Card Issuance; Risks Associated with EMV and Payment Card Issuance.* Retrieved from thales-esecurity.com: https://www.thales-esecurity.com/solutions/by-technology-focus/emv-and-payment-card-issuance

The Nilson Report. (2014). Purchase Transactions Worldwide; Market shares of 2014. Retrieved from http://www.nilsonreport.com/publication_chart_and_graphs_archive.php

Venkatesh, V., Morris, M. G., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. *IS Quaterly*, 425-478.

Vijayan , J. (2014, February). Retrieved from http://www.computerworld.com/article/2487581/endpoint-security/5-issues-that-could-hamper-emv-smartcard-adoption-in-the-u-s-.html?page=2

Vijayan, J. (2014, February 11). Retrieved from http://www.computerworld.com/article/2487581/endpoint-security/5-issues-that-could-hamper-emv-smartcard-adoption-in-the-u-s-.html

Visa International. (2010). *Global Visa Acquirer Fraud Control Manual.* New York: Visa International.

Wanaemba, M. A. (2010). *Strategies Applied by Commercial Banks in Kenya to Combat fraud.* Nairobi: Unpublished MBA Project of the University of Nairobi.

Wanjiru, L. (2011). *Strategic response of Equity Bank to fraud related risks.* Nairobi: Unpublished MBA Project of the University of Nairobi.

Wanyama, T. (2012). *Effectiveness of fraud response strategies adopted by Co-operative Bank of Kenya limited.* Nairobi: Unpublished MBA Project of the University of Nairobi.

Zigurs, I., & Buckland, B. K. (1998). A theory of task/technology fit and group support systems effectiveness. *MIS Quaterly*, 313-334.

APPENDICES

List of Commercial Banks in Kenya

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

Source: Central Bank of Kenya Website (Central Bank of Kenya, 2015)

Questionnaire

This questionnaire seeks to collect information on the effectiveness of EMV technology by commercial banks in Kenya as a response strategy to payment card fraud. Kindly note all information will be kept confidential and will be used for academic purposes only.

Please answer all sections below by ticking the appropriate box

Section A.

1. Which department are you in?

   □ Operations department

   □ IT department

2. Which category is your Bank

   □ Top Tier

   □ Middle Tier

   □ Small Tier

3. How many active cards do you have in circulation?

   □ Less than 100,000

   □ Between 100,000 and 500,000

   □ Between 500,000 and 1 Million

   □ Over 1 Million

4. Have you issued EMV cards?

□ Yes

□ No

5. Do your customers use their cards at POS merchant locations?

□ Yes

□ No

6. Do your customers use their cards at ATM Terminals?

□ Yes

□ No

7. Do your customers use their cards for online payments?

□ Yes

□ No

8. Are cards and PIN issued by the same personnel?

□ Yes

□ No

9. Has the bank implemented the Anti money laundering act in entirety?

□ Yes

□ No

10. Has the bank put in place multilevel authorization access system?

□ Yes

□ No

11. Does the bank carry out regular employ training on fraud detection?

□ Yes

□ No

12. What is your gender?

□ Female

□ Male

13. What is your age? …….

14. What is your education level?

□ Diploma

□ Undergraduate degree

□ Post graduate degree

Section B

Please indicate the extent to which you agree or disagree with the following statements regarding challenges.

Key: 1-Strongly Disagree, 2- Disagree, 3- Neutral, 4- Agree, 5- Strongly Agree

	1	2	3	4	5
1. The lack of clear guidelines on the EMV technology to use has slowed your adoption of the technology.					
2. The timeline given for implementation of EMV were sufficient to complete the rollout of the EMV technology					
3. Slow adoption progress in issuing EMV cards may hurt the reputation of the bank					
4. There is increased customer data security accompanying issuance of EMV cards.					
5. The bank relies on inflexible or legacy systems.					
6. Delayed adoption of EMV cards has led to a shift to use of mobile payment					
7. The coming into force of liability shift will spur banks to quickly adopt EMV technology.					
8. The Central Bank of Kenya has provided support in combating card					

payment fraud					
9. The criminal justice system is well equipped to deal with card payment fraud					
10. KBA card security awareness programs are effective in reducing card payment fraud					
11. The main card schemes in the country have provided adequate support in tackling card payment fraud in Kenya					
12. My organization has suffered reputation damage from card payment fraud incident reports					
13. Other challenges a. …….. b. …….. c. …….. d. …….. e. …….. f. ……					

How would you rank the following challenges in managing card compromise event? (Ranking scale is 1 to 5 with 1 as easy and 5 most difficult)

	1	2	3	4	5
1. When to block and reissue					
2. Communicating to the customer about a fraud event					
3. Lack of automation and tools					
4. Inadequate personnel					
5. Lack of clear policies, procedures and guidelines					

Section C

Please indicate the extent to which you agree or disagree with the following statements regarding your organization's exposure to card fraud.

Key: 1-Strongly Disagree, 2- Disagree, 3- Neutral, 4- Agree, 5- Strongly Agree

	1	2	3	4	5
1. We have experienced attempted card fraud in the last six month					
2. We have experienced actual card fraud in the last six months					
3. Card fraud incidences have decreased with in the last six months compared previous six months					

4. We have had lost card fraud this year					
5. We have had stolen card fraud this year					
6. We have had counterfeit card fraud at a POS this year					
7. We have had counterfeit card fraud at ATMs this year					
8. We have had account takeover fraud					
9. We have experienced a data breach on our card systems					
10. We have experienced a data breach on our merchant systems					
11. Card present fraud has been on the increase in our organization					

12. How many payment cards fraud have been reported in the last 6 months?

□ Less than 100

□ Between 100 and 1000

□ Over 1000

13. How many cards stolen fraud have been reported in the last 6 months?

□ Less than 10

□ Between 10 and 50

□ Over 50

14. How many cards lost fraud have been reported in the last 6 months?

□ Less than 10

□ Between 10 and 50

□ Over 50

15. How many counterfeit frauds have been reported in the last 6 months?

□ Less than 10

□ Between 10 and 50

□ Over 50

16. How many account takeover frauds have been reported in the last 6 months?

□ Less than 10

□ Between 10 and 50

□ Over 50

Thank you very much for your cooperation.