OPERATIONAL RESPONSE STRATEGIES TO PAYMENT CARD FRAUD BY COMMERCIAL BANKS IN KENYA

JEREMIAH MURIITHI MUNYUA

D61/8974/2006

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

OCTOBER 2013

DECLARATION

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

Signature: _____ Date: _____

Jeremiah Muriithi Munyua

D61/8974/2006

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

Signature: _____ Date: _____

Kariuki C. Ngugi, Lecturer

Department of Management Science

School of Business

University of Nairobi

DEDICATION

This operations management paper is dedicated to my lovely daughter Abigail, and my parents Mr. and Mrs. Jackson Munyua for their continued support and encouragement.

ACKNOWLEDGEMENT

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 invaluable support and the insights they have shed in writing this paper. I also acknowledge the support of the members of the KCDCA fraud forum.

I am grateful to Kariuki C. Ngugi, my project supervisor and Muthoni Margaret, the moderator for their guidance, patience and support throughout this project.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS

KBA	KENYA BANKERS ASSOCIATION
KCDCA	KENYA CREDIT AND DEBIT CARD ASSOCIATION
CBK	CENTRAL BANK OF KENYA
PCIDSS	PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS
ATM	AUTOMATED TELLER MACHINE
POS	POINT OF SALE TERMINAL
EMV	EUROMASTERVISA
PIN	PERSONAL INDENTIFICATION NUMBER
OCG	ORGANIZED CRIMINAL GROUP
KYC	KNOW YOUR CUSTOMER

ABSTRACT

The purpose of this study was to determine the operational response strategies to payment card fraud by commercial banks in Kenya. The objectives were two fold, namely: to determine the operational response strategies used by commercial banks to address the payment card fraud challenge; and to determine the effectiveness of the operational response strategies in addressing the payment card fraud challenge.

The study clearly 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 key operational response strategies to payment card fraud by commercial banks and the measures employed to determine their effectiveness

The study employed a census study of all the members of KCDCA. This was found suitable since member banks of KCDCA issue cards that are accepted worldwide and are key stakeholders in employing strategies to address the payment card fraud challenge. Data analysis was conducted using descriptive statistics and correlation analysis

The study concludes that a mix of operational strategies have been employed by commercial banks to; minimize payment card fraud, protect cardholder data, monitor and respond to compromise events as they occur. Enabling strong authentication; issuing chip and pin cards; sending transaction alerts; complying to PCIDSS; using fraud prevention and detection systems are some of the operational response strategies used by commercial banks in Kenya to address the payment card fraud challenge. The strategies are applied in varying degrees, explaining why only a few banks in Kenya issue chip cards or have real time fraud management solutions as at October, 2013.

CHAPTER 1: INTRODUCTION

1.1 Background of the Study

According to a report quoted by the Daily Nation (26th Dec. 2012), commercial banks in Kenya lose close to KES 3 billion a year due to payment card fraud. A local bank in December, 2012 had a number of its customers fall prey to increased ATM fraud during the December 2012 festive season, compelling the bank to issue replacement cards for most of its customers and saw it lose close to KES 300 million. Payment card fraud has mutated into a sophisticated crime carried out by tech-savvy criminals, using modern technology, they have assailed financial institutions with losses which at times go unreported. These important payment card fraud losses are 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. 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). KBA have also been carrying out awareness campaigns through the media in an effort to stem rising incidences of payment card fraud (KBA, 2013).

Payment card fraud occurs when someone gains financial or material advantage by using a card, or information obtained fraudulently from a card, to complete a transaction that is not authorized by the legitimate card holder. Types of payment card fraud include; identity theft on cards, stealing cards in transit/mail, physical theft, account takeover, counterfeit and skimming. A major reason why fraud occurs is because fraudsters are allowed to do so. There is a motive, an opportunity and a rationale by which the fraudster operates. Payment card fraud is perpetrated by pre-planned fraudsters, who intend from the beginning to commit fraud, intermediate fraudsters, who start off honest but turn to fraud when times get hard and slippery-slope fraudsters who simply carry out fraud (Doody, 2008).

Payment cards are accepted across many merchant outlets, hotels, restaurants, airlines and car hire firms, by doing so they reduce the need for consumers to carry cash in the

local currency or traveler's cheques. The major international card associations such as Visa, MasterCard, American Express, Diners Club and JCB all seek to have their payment cards accepted in the widest possible range of merchant outlets (Worthington, 1995). In Kenya, Visa and MasterCard, are the two major card associations, each have over 12 million acceptance locations throughout the world, who take payments by the credit and debit cards issued by various Banks, while American Express has over 102.4 million cards worldwide (American Express Company, 2013). There are various types of payment plastic cards or payment cards, they include; debit cards, credit cards, charge card, pre-paid cards and fleet cards (Wikipedia, 2013). The plastic payment card market in Kenya is growing at an increasing rate; in 2013 there has been a greater focus on the East African Market by MasterCard, Visa International, and China Union Pay to grow the popularity of card use and promote cashless transactions. The number of payment cards in the market currently stands close to 10 million (KBA, 2013). Data from the Central Bank of Kenya, indicates that the value of transactions effected through cards in the year ending 2012 increased by 7.95 percent (Sunday, 2013).

As at June 30th 2012, there were forty three commercial banks, thirty-five of the banks, most of which are small to medium sized, are locally owned. Six of the major banks are listed on the Nairobi Stock Exchange. 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, 2012). Banks in Kenya have come together under the Kenya Bankers Association (KBA), which serves as a lobby for the banks' interests and addresses issues affecting its members. The Kenya Credit and Debit Card Association (KCDCA) is the umbrella body which brings together organizations that deal with payment cards in Kenya. It comprises of twenty two member banks and processing centers. Its mission is to harmonize the card industry by striving to provide a conducive environment resulting to the realization of the stakeholder objectives. Comprising part of its executive board is the Fraud Committee charged with training of merchants and sharing of fraud information (KCDCA, 2012).

Operations strategy has been defined as the strategic reconciliation of market requirements with operations resources (Lewis, 2008). According to Porter (1980) an organization's interaction with its environmental factors that is; political, legal,

economic, social, technological, customer and competitive factors, is at the heart of strategy development. Pearce and Robinson (1991) define a strategic response as the set of decisions and actions that result in the formulation and implementation of plans designed to achieve a firm's objectives. According to Porter (1998) operational responses are part of a planning process that coordinates operational goals with those of the larger organization. They are the determinants of both market place success and of financial success. Commercial banks in Kenya have employed various strategies to address the fraud challenge; some of these include transaction monitoring, data security, training and awareness campaigns and sending transaction alerts.

1.2 Statement of the Problem

Use of payment cards has been increasing on at increasing rate in Kenya; regular shoppers are opting for card over cash due to the convenience, safety and reliability offered by cards (Mbogholi, 2009). More merchants in different sectors are also signing up to be receiving payments by card rather than cash since cards discourage theft by merchant employees, reduce the amount of cash on the premises, reduce the back office expense of processing cash and transporting it to the bank. The ongoing increase in card acceptance and usage has made cards increasingly attractive to fraud. In Kenya, the press on almost a monthly basis feature articles particularly on skimming at Automated Teller Machines which has become rampant affecting the entire banked population and costly to many financial institutions. Since card payments are often considered as a fast and cheap way of making payments, payment card fraud can harm the efficiency of the entire retail payment system by causing financial and reputation loss to commercial banks and greatly inconveniencing cardholders.

Studies on payment card fraud response strategies are lacking. Most studies have focused on general bank fraud in general. Some like Wanaemba (2010) and Wanyama (2012) conducted studies on strategies employed by banks in Kenya to combat bank fraud. Their studies concluded that know your customer (KYC), use of advance technology, regular audits, real-time monitoring, strong internal controls and data security as some of the strategies being employed by commercial banks to address the fraud challenges they face. Cheptumo (2010) studied response strategies to fraud related challenges in Barclays

Bank, Kenya. His findings indicate that weak internal controls, electronic storage of customer data and technological advancement are some of the reasons why fraud happens. Other studies conducted on the subject include: Mbwayo (2005) who did a study on strategies applied by commercial banks in anti-money Laundering compliance programs, Njagi (2009) who looked at effectiveness of know your customer policies adopted by commercial banks in Kenya in reducing money laundering and fraud incidences and Wanjiru (2011) who studied strategic responses of Equity Bank to fraud related risks.

Therefore the aim of this study is to fill the knowledge gap by determining the operational response strategies being employed by commercial banks in Kenya to combat payment card fraud and their effectiveness. It will also provide insights into payment card fraud that is; the types and impacts of payment card fraud.

1.3 Objectives of the study

This research will aim to achieve the following objectives:

i. To determine the operational response strategies adopted by commercial banks in Kenya to address payment card fraud
ii. To determine the effectiveness of operational response strategies adopted by commercial banks to payment card fraud

1.4 Importance of the study

This study is valuable to card fraud managers in the payment card industry as they explore the most effective operations strategy to adopt in responding to the payment card fraud challenge. They will be enlightened on the various strategies available, how to implement them and be able to ascertain the effectiveness of the strategies they are currently employing. 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 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, by highlighting a low risk high impact fraud type.

CHAPTER 2: LITERATURE REVIEW

This literature review will consider the various types of payment card fraud, the operational response strategies employed in effectively managing the challenge of plastic card fraud and how to measure the effectiveness of these strategies. The literature review will also explore the various barriers towards effective execution of these strategies.

2.1 Payment card fraud

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 is; card-present and card-absent, each of which offer unique card acceptance and fraud issues (Visa, 2010). The statistical report on payment card fraud of 2012 by the Ministry of Economy and Finance in Rome details the following types of payment card fraud;

Card stolen fraud 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 Automated Teller Machine (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.

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 and skimming.

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 their card details, a process known as phishing. Card information can 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;

Account takeover fraud is where 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. Two common ways to use stolen data for card payment fraud are 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). Internet, mail order, or telephone transactions, referred to as card-not-present (CNP) transactions, are vulnerable to stolen data because payment cards cannot be inspected (Sullivan, 2010).

2.2 Impact of Payment Card Fraud

On a global level, fraud migrates from more secure to less secure regions and channels. This shift is accelerated by an adept and organized criminal community (MasterCard, 2011). Fraud rates across various regions differ due to a number of factors, including the mix of payment cards in use, transaction authorization systems, the types of payments made using cards, evolving security standards, and the use of older card technology that has relatively weak security features (Sullivan, 2010). Card fraud has evolved with advancement in technology and communication. Organized international criminal bodies are utilizing the global communication network to obtain card details and defraud unsuspecting cardholders. The Europol's report for Credit Card Fraud of 2012, states that the criminal market of payment card fraud within the European Union (EU) is dominated by well-structured and globally active organized crime groups (OCGs). Criminal networks have managed to affect non-cash payments in the EU to the extent that protection measures are very expensive and need to be implemented on a global level. Consequently, the use of payment cards can be inconvenient and no longer fully secure for cardholders.

Payment card fraud is a low risk and highly profitable criminal activity which brings organized crime groups originating from the EU a yearly income of around €1.5 billion Euros. These criminal assets can be invested in further developing criminal techniques or can be used to finance other criminal activities or start legal businesses. The report further goes to state that the majority of illegal face-to-face card transactions affecting the European Union take place overseas, mainly in the United States (Siciliano, 2013). In 2012, media reports cited cases of over 10 million credit and debit cards compromised in a breach at Global Payments, a US based credit processor (Global Payments data breach exposes card payments vulnerability, 2012).

Locally, 2011, 2012 and 2013 has seen a concentration of PIN debit card compromise at Kenyan bank ATMs, many of which are unprotected, in remote areas or lack surveillance. The Kenyan press had several headlines of banks grappling with numerous complaints, with one bank having to replace cards for most of its cardholder base. Many financial institutions are reeling from increasing fraud cases, according to a report by Deloitte East Africa in 2010, Kenyan banks lost close $36 million in card present and card-not-present (CNP) fraud (Abiage, 2011). Due to the rampant fraud cases reported by banks in the country, the Kenya Bankers Association (KBA) issued a directive for all banks to migrate to chip-based technology for debit and credit cards by March 2014. With an average of over 10 million cards in the country, the capital investment employed in ordering for the plastics, system upgrades, training of bank personnel and media campaigns, banks are set to spend about KES 2.5 billion on the exercise (Situma, 2013). Chip cards offer a more secure way to process card present transactions, however with increased internet penetration, Kenyans are now making online purchases for home entertainment, social networking and groceries, with one fraud avenue closed, fraudsters are now likely to turn their efforts to card-not-present fraud.

The costs of fraud are passed on to society in the form of increased customer inconvenience, opportunity costs, unnecessarily high prices for goods and services, and criminal activities funded by fraudulent gains. The major card associations track and report fraud losses as a percentage of sales volume or loan amounts outstanding, currently the figure stands at about eight cents per hundred or eight basis points (Wilhelm, 2004).

The impact of customer satisfaction from having transactions declined and cards blocked and reissued is evident on complaints posted on social networks and the press. The negative publicity resulting from such has a potentially damaging effect on the affected banks reputation, as upset customers may switch to competitors. The broad brush methods of blocking and reissuing all compromised cards are wasteful, costly and disruptive (Fico.Com, 2012).

2.3 Operational Response Strategies to Payment Card Fraud

According to Masuda (1993) there is evidence that program initiatives and an industry-wide action with the exchange of fraud-related intelligence data amongst regional and national authorities seem to be the key to reduce credit card fraud. Williams (2007) presents 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.

According to Noka (2010) the strategies employed in payment card fraud management entail a multilayered approach to security and risk management. These strategies involve; 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, processed or transmitted throughout the payment system and monitoring and managing events as they occur to ensure that issues are effectively addressed and minimize the impact of fraud. Noka further emphasizes that the success of these strategies lies on a trust and partnership relationship with stakeholders such as law enforcement agencies, industry trade groups, association such as Kenya Bankers Association (KBA) and Kenya Credit and Debit Card Association, regulators such as CBK, and legislators. By promoting security awareness through education and training, the fraud challenge through payment cards can be addressed.

Minimizing fraud involves employment of advanced authorization systems, card risk management systems, EuroMasterVisa (EMV) Chip cards, strong authentication, data devaluation, and secure card-not-present authorizations. Advanced authorization tools

monitor authorizations in real-time enabling risk managers to immediately identify and respond to emerging fraud patterns and trends. Card risk management systems enable financial institutions to create, test and execute card authorization rules. These systems allow card issuers to decline or approve authorizations or create fraud cases from flagged suspicious transactions. EMV chip cards have an enhanced authentication mechanism that allows payment providers to move away from static information held on a cards magnetic strip. These cards significantly limit a fraudster's ability to counterfeit cards. Data devaluation is part of a dynamic password authentication (DPA) technique used to generate unique and random passwords for internet and mail order telephone order (MOTO) applications, so the risk of fraudsters stealing passwords is effectively eliminated (Visa International, 2013). Secure card-not-present transactions are effected using 3-D secure technology, which is an additional layer of security for online credit and debit card transactions (Wikipedia, 2013).

Protecting vulnerable card data whenever it is stored, processed or transmitted has been achieved through application of the various programs and standards. Payment Card Industry Data Security Standard (PCIDSS) is an important baseline of security adopted by merchants, payment processors, card issuers and acquirers. Its goal is accomplished by creating secure networks, strong access controls, data encryption, computers protected with firewalls and antivirus programs, and security policies designed to establish an effective internal control environment (PCI Security Standards Council, 2013). These standards help prevent hackers from breaching computer security and committing fraud. Personal Identification Number (PIN) security is a program designed to ensure the secure transmission of cardholder PINs from the point of entry (Visa Europe, 2013). Data field encryption protects card information from the swipe to the acquirer processor with no need for the merchant to process or transmit card data in the clear. It renders cardholder data useless to criminals in the event of a data breach (Visa, 2009). Data elimination is the processing of completely obliterating all card data from data storage devices such as hard drives and flash drives. It ensures that data does not fall to the wrong hands (Smart Storage Systems, 2012). To ensure data security, card manufacturers and personalizers are periodically certified to ensure compliance with standards enumerated by PCIDSS.

Monitoring and responding to events as they occur requires that institutions invest in systems that can send transaction alerts, track compromised account activity, monitor chargebacks and have in place a rapid compromise response and investigations team. These ensure that issues are effectively addressed and the impact of fraud is minimized (Noka, 2010).

2.4 Effectiveness of Operational Response Strategies to Payment Card Fraud

The effectiveness of the various strategies is determined by computing the point of detection, false positive ratio and fraud basis points. Point of detection measures how many missed fraudulent transactions occur prior to the system generating its first alert on an account. False positive ratio is the number of transactions a system flags as suspicious, compared to the number of transactions that are actually fraudulent. Fraud basis point is a ratio used in the fraud industry to asses overall anti-fraud performance, it shows the ratio of fraud losses to sales turnover as a percentage, one basis point is one hundredth of one percent. Another performance measure is the savings through fraud prevention, the open to buy at the time of fraud identification, or alternatively the fraudulent transactions declined as a result of blocking (ACI Worldwide, 2010).

While the above response strategies are being developed and implemented, barriers remain, such as conflicts of interest, inadequate incentives, poor governance, potential redundancy, slow adoption of new security standards and a relatively high rate of card fraud losses. Efforts to improve card payment security by one member of the network may benefit other members, just as one member's security breach may harm others. But because one member of the network has no incentive to take account of the external benefits or costs of others, security for the network is less than optimal. Conflicts of interest can arise over the appropriate level of effort to enhance security. Some members will prefer relatively little effort, leaving the security of the entire network subject to its weakest links. Conflicts of interest can also complicate the development of security standards. Technically, standards would be more effective if members of the network determined them cooperatively (Anderson, 2008, Braun, 2008).

Research has shown that a governance structure that includes all the various interests in the network is key on standard setting. The International Organization for Standardization (ISO) uses a model of cooperation to coordinate international security standards for payments. The PCIDSS and EMV standards are not developed in these standard-setting organizations. Instead, they use a centralized model controlled by the card issuers and networks. The centralized model may allow security standards to be developed rapidly, but perhaps at the expense of adoption. Only half of the largest U.S. merchants met the PCI compliance deadline of September 30, 2007.

Similarly, many European retailers have been slow to achieve PCI compliance (Leyden, 2008). Merchants and processors face significant costs of compliance and question the benefits they receive, resulting in PCI compliance waivers (Digital Transactions News, 2012). The standards themselves have been criticized because they do not address card network rules that require merchants to store card information to resolve disputed transactions or facilitate refunds. In addition, some merchants who have been certified as compliant have still been the victims of successful security breaches, raising concerns about the quality of the standard (Mott, 2007).

2.5 Summary and Conceptual Framework

This literature review has identified three operational response strategies to counter the payment card fraud challenge, that is; prevent, protect card data and respond and monitor fraud as and when it occurs. 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, collaborating on strategic data initiatives through global and regional fraud advisory councils, establishing and enforcing effective payment card data integrity standards, commercial banks in the country can ensure that fraud migrates to less secure areas.

A strategy is only as strong as the techniques employed. Creating a response strategy depends on the level of risk exposure an institution is exposed to. It requires an understanding of the goals of the organization and the value of each strategy

implemented in order to understand the associated costs and implications to administration, fraud reduction and potentially lost revenue. Effectiveness of each strategy is determined by the fraud rate cited in the organization by periodically determining the fraud loss to sales turnover, the point at which fraud is detected and the number of fraudulent transactions to genuine transactions.

This study will examine the card fraud risk exposure facing commercial banks in Kenya, the operational response strategies implemented, and the effectiveness of these response strategies towards combating payment card fraud. Lower fraud rates are expected in a bank that has successfully implemented the necessary techniques.

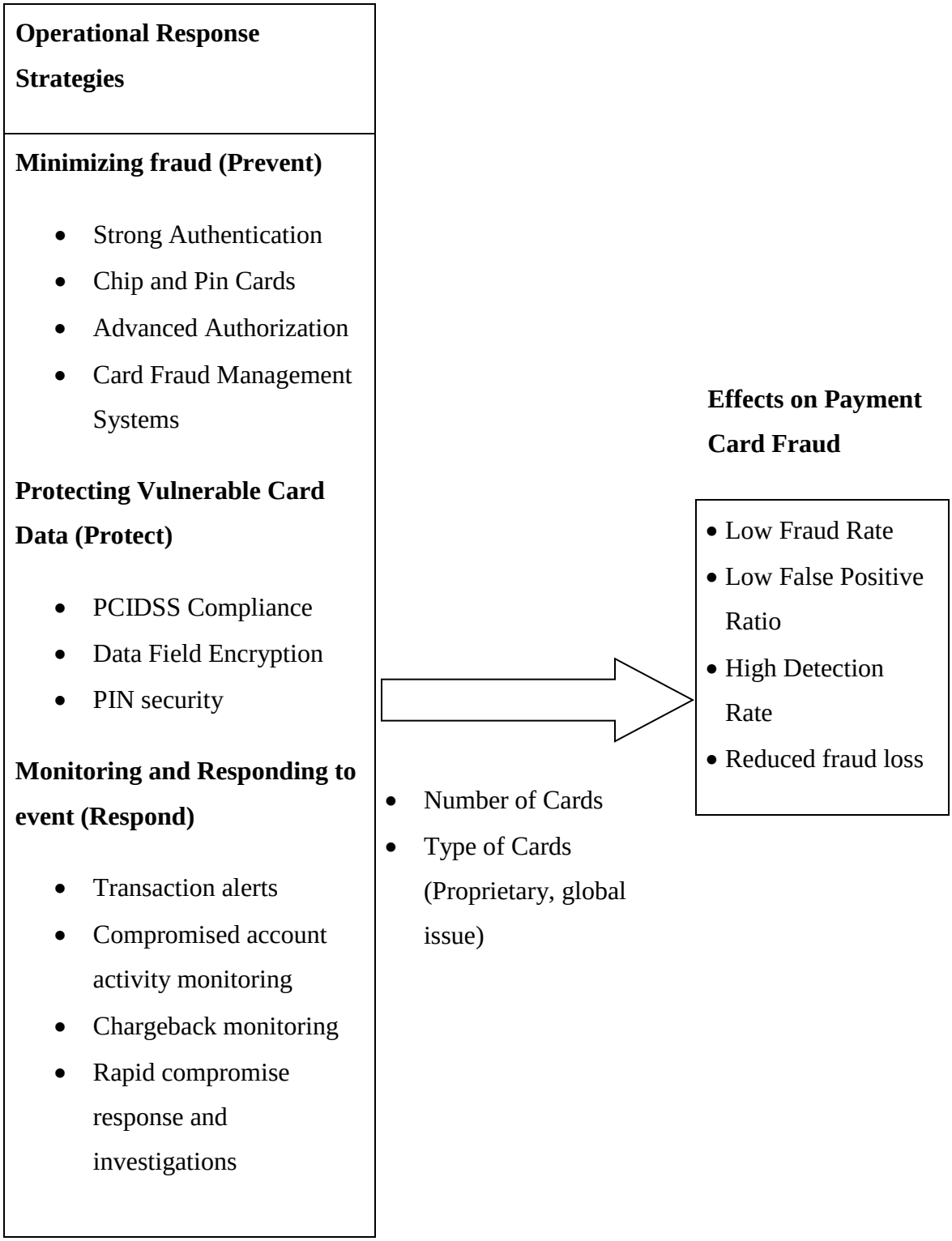


Figure 2.1: Conceptual Framework

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Research Design

An explorative research study was used because it provided a focused and detailed insight to the operational response strategies being employed by commercial banks in Kenya to effectively address the payment card fraud challenge.

3.2 Population

The target population consisted of 18 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 which consisted of Barclays Bank of Kenya, Chase Bank, Commercial Bank of Africa, Co-operative Bank of Kenya, Diamond Trust Bank Kenya, Equatorial Commercial Bank, Ecobank, Equity Bank, Fidelity Bank, Kenya Commercial Bank, I&M bank, Imperial Bank, National Bank of Kenya, NIC Bank, Paramount Bank, Prime Bank, Cfc Stanbic Bank and Standard Chartered Bank. The study focused on card center managers and risk managers with expert knowledge on cards and card fraud.

3.3 Data Collection

The study made use of both primary and secondary data. Primary data was obtained from card centers managers and their risk managers. This data captured management operational response strategies to payment card fraud and their level of effectiveness.

A questionnaire (Appendix III) in structured form was administered to collect primary data. The questionnaire instrument used had different sections to collect data on the respondents' demography, the card fraud exposure faced by the respondents' institution, the types of card fraud encountered, the operational response strategies to manage card fraud, the effectiveness of these strategies and the respondent's view of the level of support from regulators and legislators as they combat fraud.

The questionnaire was administered through face to face interaction with the respondent and electronic mail to card center head and risk managers.

Secondary data was collected by use of desk search techniques from published reports by the banks, Kenya Bankers Association, Kenya Credit and Debit Card Association, Banking Investigation and Fraud Unit of Central bank and Media reports relating to card fraud in Kenyan banks.

3.4 Data Analysis

Data analysis was performed on the completed questionnaire to answer the research question; what are the operational response strategies being employed by commercial banks in Kenya to combat fraud and how effective are they.

Number of strategies used by commercial banks in Kenya was 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.

Correlation analysis on the five point Likert data obtained was used to indicate the extent in which the strategies used are 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.

CHAPTER 4: DATA ANALYSIS AND FINDINGS

4.1 Introduction

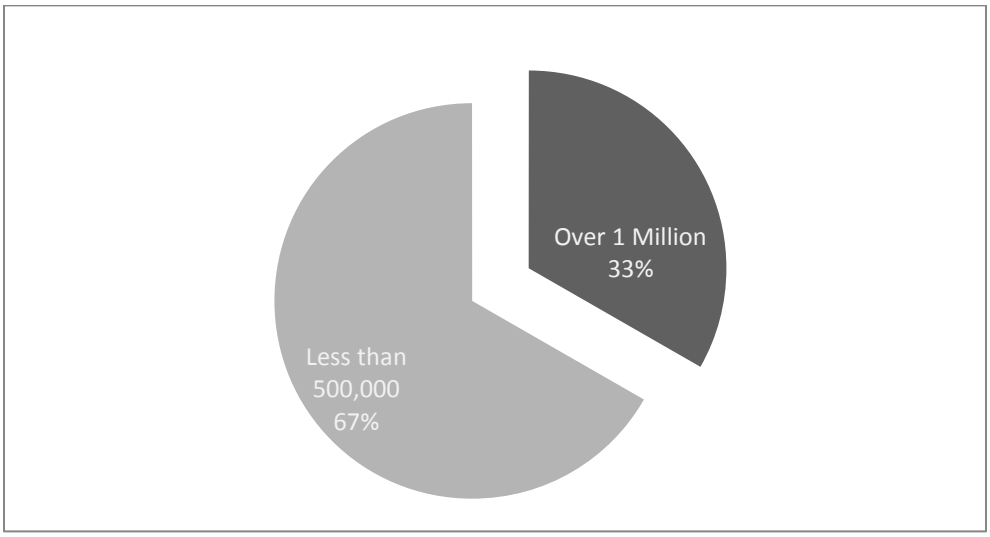
This chapter presents the results of the data analysis. The data from the completed questionnaires was summarized and tabulated in the form of percentages and frequencies. Bivariate correlations were computed to determine the degree of relationship between the operational response strategies employed by commercial banks and the various payment card fraud measures. Out of the 18 member banks of Kenya Credit and Debit Card Association, 11 banks responded which constituted 61% of the entire population. Babbie (1990) suggested that a response rate of 60% is good, therefore a response rate of 61% is considered sufficient to yield meaningful statistical analysis. The data was gathered exclusively from the questionnaire that was designed in line with the objectives of the study.

4.2 General Information

This section presents information gathered from the respondent banks regarding various factors relating to payment card fraud. The average number of cards and the preferred transaction channels indicates the card fraud exposure faced by the respondent banks. The perceived card fraud trend by transaction environment and the prevalence of the various fraud types is presented. This section also highlights 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 4.1 below indicates the number of cards issued by the respondent banks.

Figure 4.1 Number of Cards

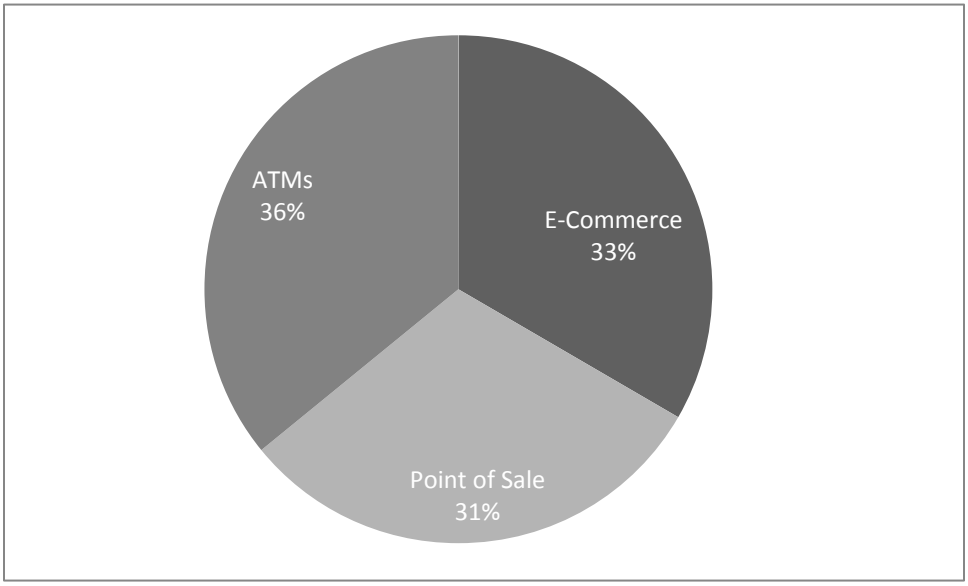


Source: Survey Data (October, 2013)

The figure indicates that 66.7% of the respondent banks issue less than 500,000 global payment cards, while 33.3% of the respondent banks issue over 1 million cards.

Figure 4.2 below indicates the preferred transaction channels used by cardholders of the respondent banks

Figure 4.2 Preferred Transaction Channels

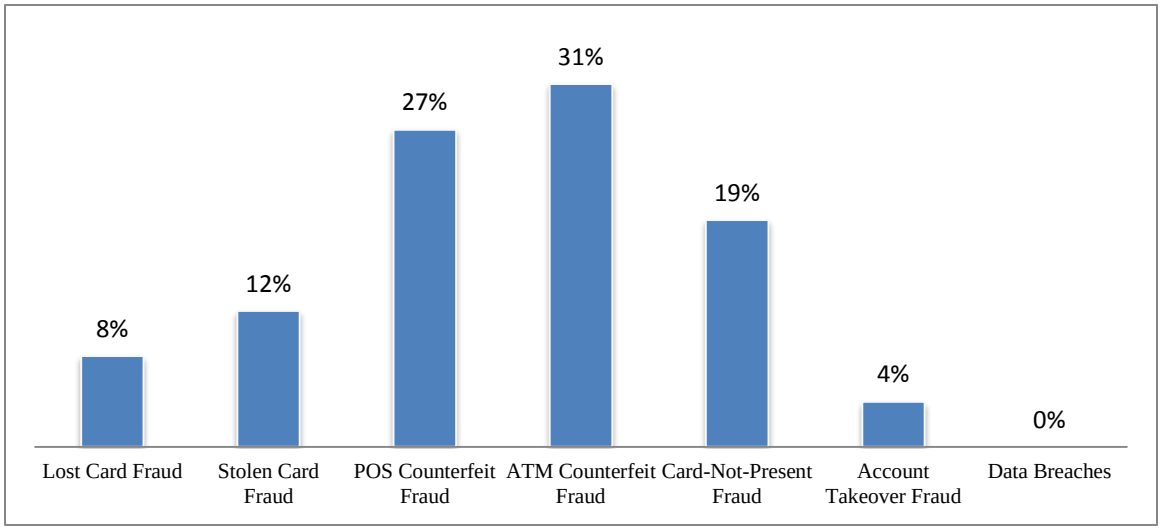


Source: Survey Data (October, 2013)

The figure indicates that most cardholders use their cards at Automated Teller Machines, there is a noted preference for e-commerce amongst the respondent banks.

Figure 4.3 below indicates the prevalence of the various types of payment card fraud faced by the respondent banks.

Figure 4.3 Prevalent Payment Card Fraud Types

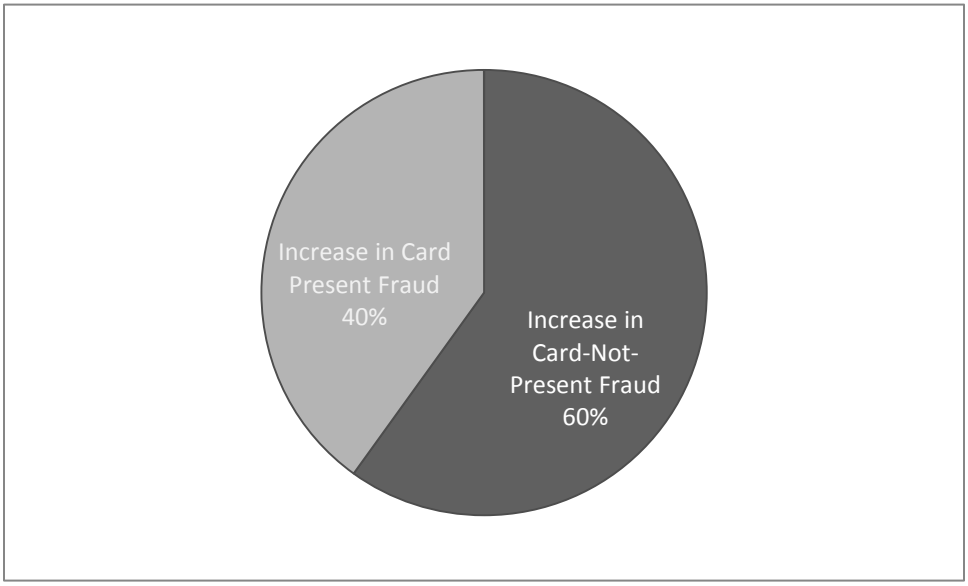


Source: Survey Data (October, 2013)

The figure indicates that counterfeit card fraud at ATM is the most prevalent payment card fraud type amongst the respondent banks.

Figure 4.4 below indicates the perceived increase of fraud depending on the transaction environment.

Figure 4.4 Transaction Environment Payment Card Fraud Trend

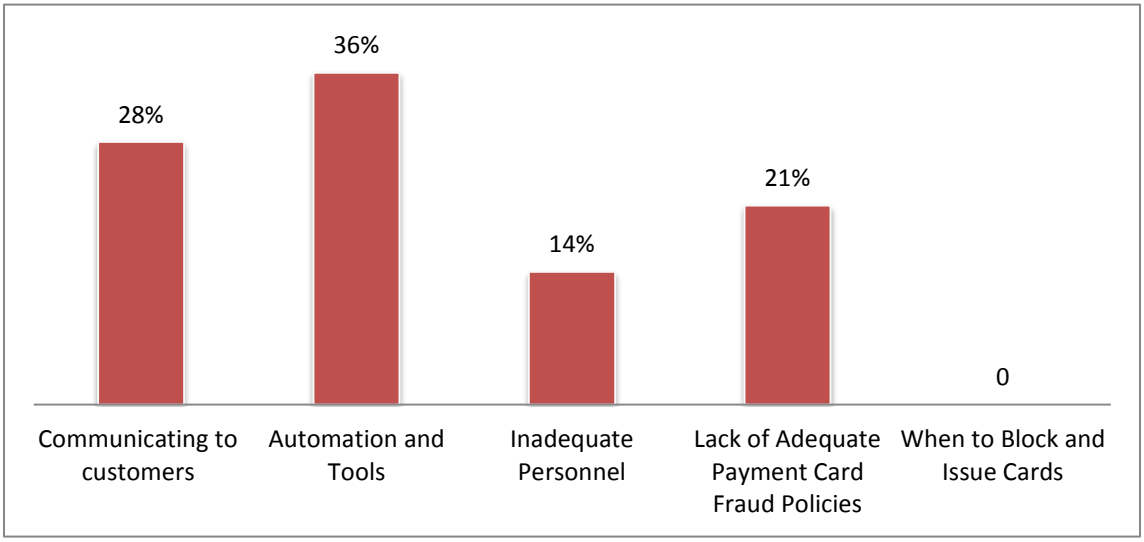


Source: Survey Data (October, 2013)

The figure indicates that 60% of the respondents indicate that card not present payment card fraud has increased in the current year to prior year, while 40% of the respondents indicate that card present payment fraud has increased.

Figure 4.5 below indicates degree of challenge faced by the respondent banks in tackling the fraud challenge.

Figure 4.5 Rank of challenges in managing payment card fraud

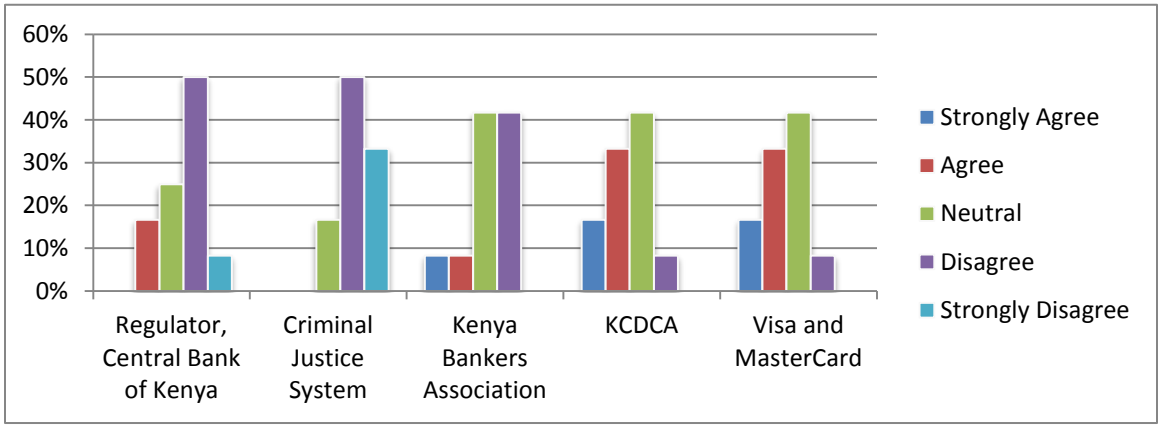


Source: Survey Data (October, 2013)

The figure indicates that lack of automation and fraud management tools is ranked as the greatest challenge facing respondent banks in addressing the fraud challenge.

Figure 4.6 below indicates the perceived level of support respondent banks view to have received from various stakeholders in card payments.

Figure 4.6 Perceived level of support



Source: Survey Data (October, 2013)

The figure indicates that 50% of the respondents find the regulator, CBK and the criminal justice system support in addressing payment card fraud to be inadequate. Efforts by the

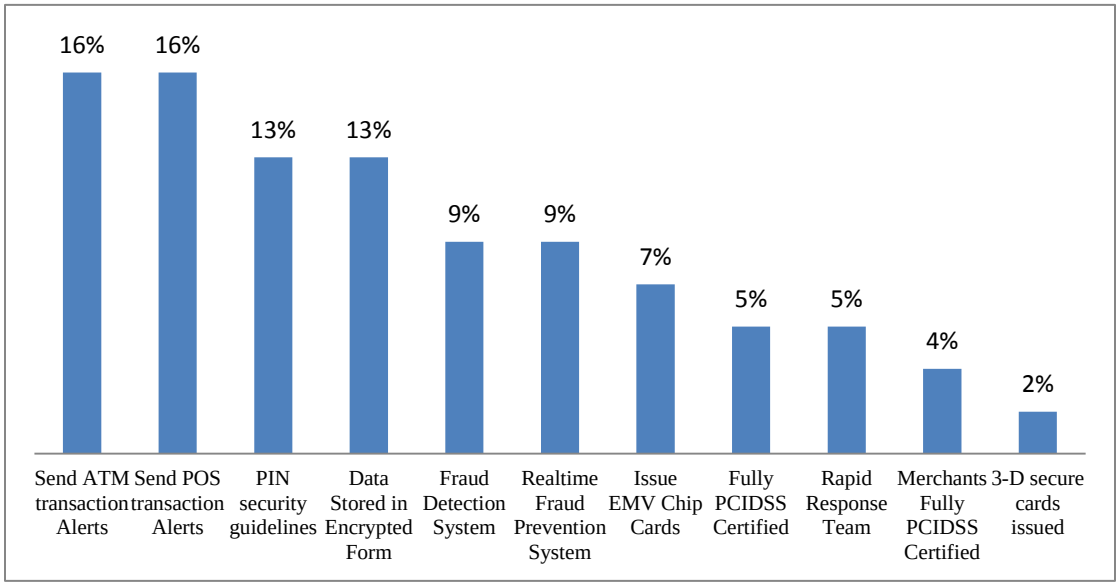
Kenya Debit and Credit Association, and the supporting card schemes are viewed to be effective, albeit slightly;

4.3 Operational response strategies

This section presents findings specific on the two objectives of the study that is, to determined the operational response strategies used by commercial banks to combat payment card fraud and the effectiveness of the various operational response strategies.

Figure 4.7 below highlights the extent with which the various operational response strategies are employed by the respondent banks in addressing the payment card fraud challenge

Figure 4.7 Operational Response Strategies

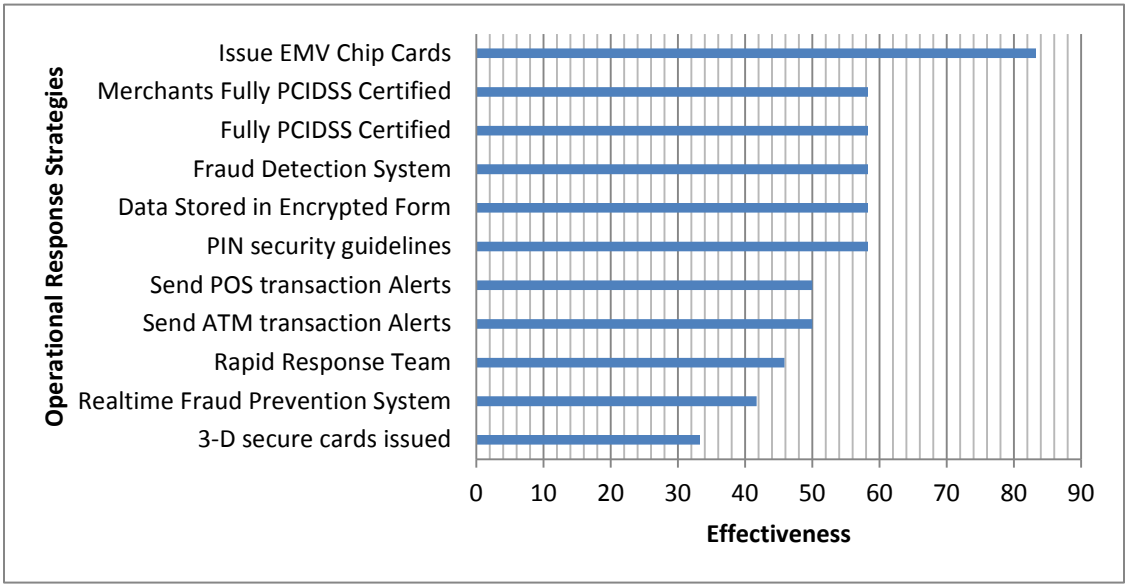


Source: Survey Data (October, 2013)

The figure indicates that that sending transmission alerts is the operational strategy adopted across the respondent banks in addressing the card fraud challenge. With only a few banks using 3-D secure technology.

Figure 4.8 below illustrates the perceived level of effectiveness of the various operational response strategies towards addressing the payment card fraud challenge.

Figure 4.8 Effectiveness of Operational Response Strategies



Source: Survey Data (October, 2013)

The figure indicates that most respondent banks view issuance of EMV chip cards as the most effective operational response strategy to tackle payment card fraud.

The Table 4.1 below indicates the extent in which the strategies used are associated with the payment card fraud measures in the commercial banks. It indicates the effect of applying individual strategies to address payment card fraud.

Table 4.1 Correlation of Operational Strategies to Payment Card Fraud Measures

Operational Response Strategy	Point of Detection (Spearman's rho)	Fraud Rate (Spearman's rho)	False Positive Ratio (Spearman's rho)
3-D secure cards issued	0.03	-0.56	0.054
Real-time Fraud Prevention System	0.47	-0.155	0.327
Rapid Response Team	0.64	-0.052	0.41
Send ATM transaction Alerts	0.616	0.67	0.216
Send POS transaction Alerts	0.616	0.67	0.054
PIN security guidelines	0.512	0.704	0.11
Data Stored in Encrypted Form	0.163	0.412	0.755
Fraud Detection System	0.585	0.7	0.327
Fully PCIDSS Certified	0.54	0.235	0.501
Merchants Fully PCIDSS Certified	0.369	0.168	0.133
Issue EMV Chip Cards	-0.061	0.296	0.041

Source: Survey Data (October, 2013)

4.4 Discussion on findings

The objectives of the study were to determine the operational response strategies used by commercial banks in tackling the payment card fraud challenge and their effectiveness. The results found out that the respondent banks use a mix of strategies to minimize fraud, protect cardholder data and to monitor and respond to payment card fraud events.

Sending transaction alerts has been adopted across all the respondent banks. In this era of advanced and affordable information communication channels, most banks require that

every cardholder possess a registered mobile phone number. Card authorization systems interface with mobile applications to ensure that an SMS alert is sent to a customer seconds or minutes after conducting a transaction at a point of sale teller or automated teller machine. When a cardholder receives an alert for an unrecognized or unauthorized POS or ATM transaction, they are required to contact their issuing banks on the numbers at the back of their cards or customer help-lines provided. The bank issuing bank considers one reported compromise event as an opportunity to identify other cards at risk or compromise terminals and take necessary measures. This response strategy has a high positive correlation to the point of detection fraud metric. Sending transaction alerts effectively addresses a banks fraud rate as seen in Table 4.1.

Adherence to PIN security guidelines ensures that PINs are securely processed, managed and transmitted to the cardholder. A customer is authenticated by the PIN keyed in while conducting a PIN based transaction such as a cash withdrawal at an ATM. Counterfeit fraud at ATMs is perpetrated by improper PIN management by the cardholder. Secure management of PINs and PIN data is effective in addressing payment card fraud. It is positively correlated to a banks rate of fraud. In this study the correlation coefficient with the banks fraud rate was at 0.704, indicating that insecure or non-compliance to PIN security guidelines can lead to increased fraud losses. It is least correlated to the rate at which fraud management solutions decline or approve transactions, but has a correlation coefficient of 0.512 to the point of detection.

Storing data in encrypted format, secures sensitive card data from unauthorized use and access. Card fraud schemes are based on fraudulent acquisition of card data. Correlation analysis indicates a correlation coefficient of 0.755. It has a direct correlation to the rate at which fraud management systems or authorization systems decline transactions. Correlation to fraud rate is at 0.412. From the data analysis, respondents view data security as effective in addressing the card fraud challenge. Most banks have put in place firewalls and information technology policies to guard against unauthorized data access.

Installing a fraud detection system significantly reduces payment card fraud losses with a correlation coefficient of 0.7 to fraud rate. A detection system utilizes inbuilt rules and scores to flag suspicious transactions for the attention of risk managers who then create

cases and take appropriate actions against compromised cards and terminals. It has correlation coefficient of 0.585 to the point of detection. It is rated as effective and ranked together with PCIDSS compliance and secure data storage in regard to effectiveness.

Few respondent banks have put in place a real-time fraud prevention system that proactively identifies fraudulent transactions and denies authorization. In regard to effectiveness, it has a positive correlation coefficient value of 0.57 to fraud detection but negatively correlated to a banks fraud rate since few banks have invested in it. As a response strategy it is ranked as not as effective as PCI compliance, transaction alerts, implementation of PIN security guidelines or fraud detection system.

Chip and PIN technology has been rated as the most effective response strategy against payment card fraud. However at the time of the study only three of the respondent banks had implemented it. Kenya Bankers Association and the regulator Central Bank of Kenya, requires all banks to have Chip capable transaction terminals and issue Chip cards by March, 2014. It is anticipated that fraud losses due to card present fraud will reduce dramatically. Issuance of chip cards has correlation coefficient of 0.296 to fraud rate. This is due to the number of banks currently issuing chip cards in the country, and the extent of the strategy's implementation can be recognized when all banks in the country comply with the KBA and CBK mandate.

PCIDSS compliance at bank and merchant has not been fully implemented by any bank. Compliance to PCIDSS guidelines has been rated as highly effective second only to issuance of chip cards. This strategy has a high correlation to the point of detection and rate at which fraud management systems decline transactions. It ensures the creation of secure networks and security policies designed to establish effective internal control environments. With full compliance banks will effectively manage data breaches and hacking, whose incidences are bound to increase as more Kenyans gain access to the internet and an increasing demand for computer knowhow.

The study established that having in place a rapid response team to a compromise event is effective in addressing the payment card fraud challenge. Rapid response teams comprise of a twenty four hour monitoring unit and investigators. Few of respondents have in place

an active and effective response team to monitor and respond to compromise events as they occur. The study was able to establish that fraud detection is advanced by having in place such a team with a positive correlation coefficient of 0.64. However it is negatively correlated to fraud rate since loss has already occurred before the team responds.

3-D secure technology has been implemented by very few banks in the country. Its efficacy is deemed least due to the level of adoption by commercial banks in the country. However it is perceived with a noted increase in the number of e-commerce transactions, commercial banks in the country will consider adopting it to counter card not present fraud.

Forging close relationships with stakeholders is critical to the success of the above strategies; however at the time of the study, 50% of the respondents felt that support offered by the criminal justice system and the regulator in addressing payment card fraud is inadequate. The criminal justice system has been faulted for weak legislation and light sentences. Some of the respondents indicated that banks bear the burden of proof in times while there is a knowledge gap in regard to payment card fraud that exists among prosecutors and the police. Lack of full cooperation from the bank fraud investigations department hampers response team efforts in delivering punitive sentences and successful prosecutions. The regulator has been faulted for not putting in place guidelines that relate specifically to payment cards and payment card fraud. Card schemes such as Visa and MasterCard continually engage issuing and acquiring banks on card risk management practices whilst providing operating regulations to aid banks in resolving fraud related disputes. Card schemes sponsor merchant training programs carried out by KCDCA, which perceives merchants as the first line of defense against payment card fraud.

The study was able to establish challenges facing commercial banks in addressing payment card fraud. Lack of automation was identified as the leading challenge in combating card fraud. Card fraud management systems require substantial investment to the perceived return. Most banks opt for adequate fraud management solutions which may not sufficiently address emerging fraud trends. The study further established that most banks have suffered reputational damage as a result of payment card fraud

incidences, therefore most banks are reluctant to communicate to their customers about a card fraud incident due to fears of litigation or migration of customers to competitors.

4.5 Summary of findings

The first objective of this study was to determine the operational response strategies employed by commercial banks in combating payment card fraud. The study was able to establish that banks in Kenya use a mix of various operational response strategies in varying degrees depending on their perceived impact in reducing fraud rates, detecting fraud and promoting card usage.

Sending transaction alerts has been adopted across all the respondent banks to ensure that the impact of fraud is minimized. Most banks have implemented PIN security guidelines in their card management processes. Banks store card data in encrypted form or mask it to deter fraudsters from acquiring information key to counterfeiting cards. Various banks have installed fraud prevention and detection systems to reduce the impact of fraud incidences. The study was able to establish that banks are yet to comply with the payment card industry data security standards (PCIDSS) which are essential in protecting card data wherever it is stored, processed or transmitted. The study further established that only a few banks issue chip cards as a counter to card present fraud. Some commercial banks in Kenya have in place a rapid response team comprising of investigators and a twenty four hour monitoring unit to detect and address it occurs. The study established that only one bank in the country has implemented 3-D secure technology on its cards at the time of the study.

The second objective of the study was to determine the effectiveness of the operational response strategies by commercial banks in combating payment card fraud. Effectiveness of the various strategies is determined by the impact of each strategy on fraud rate, detection rate and rate of decline and approval by authorization systems. The study was able to establish amongst the respondents, that in order to minimize fraud, issuing of chip cards was the most effective strategy in combating card present fraud. Due to the low uptake of the technology in the Kenyan banking sector, the impact of this strategy on fraud rates is yet to be fully determined. In order to protect card data, banks have implemented PIN security guidelines across board. Implementation of PCIDSS and PIN

security guidelines is rated as being effective by most of the respondents. The most effective response strategy in monitoring and responding to fraud events was installation of a fraud detection system and dispatch of transaction alerts.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

The value and number of transactions conducted using payment cards are gradually increasing; the avenues to conduct transactions are also on the increase. The transport sector is gradually adopting card payments, and as internet penetration deepens in the country, various merchants are setting up online stores to reach a wider market; the most likely mode of payment will be payment cards. Payment card fraud is a challenge that presents a visible challenge to such endeavors. It is developing as information communication technology advances and its impact is being felt by financial institutions and their customers. Proceeds from payment card fraud are being used to fund criminal activities, leading to unnecessarily high prices for goods and services and increased customer inconvenience.

This study has established that commercial banks are aware of the challenges and requirements necessary to minimize payment card fraud. Banks are currently utilizing a mix of strategies to combat fraud, however costs, lack of a regulatory and legislative framework hinders adoption and implementation of various strategies to effectively stem further losses due payment card fraud, the banks regard support from the regulator, criminal justice system and the legislature to be inadequate.

5.2 Recommendations

The government should put in place policies that make it mandatory for all card issuers to implement effective strategies that will curb payment card fraud. This will ensure that Kenya as a region is not targeted by fraudsters who migrate from secure to less secure areas. Adequate legislation against payment card fraud that appreciates the extent and impact of payment fraud will serve as a deterrent to criminals. The government should be at the forefront of promoting cashless transactions to reap some of the benefits accorded by payment cards. The study was able to establish support offered by Kenya Bankers Association in regard to payment card fraud is not sufficient. Being a stakeholder, KBA's support is expected to exceed that of foreign card schemes, sponsoring and lobbying for

government support in tackling payment card fraud, since most banks issue cards to their customers.

To minimize fraud, Kenyan banks need to adopt Chip and PIN technology as well as strong authentication techniques such as 3-D Secure. Protecting card data is critical to ensuring that access is authorized and restricted. Implementation of PCIDSS guidelines is key to achieving this goal. The current practice by banks to send out transaction alerts is commendable and a deterrent to would be fraudsters, fraud loss is also minimized. A convergence of monitoring and response strategies ensures fraud opportunities are minimized and curbed.

5.3 Limitations of the study

The study focused on members of the Kenya Credit and Debit Card Association (KCDCA) offering global payment cards, more insights would have been garnered from the other licensed commercial banks. Another limitation is the sample of the study because out of the eighteen (18) banks only eleven responded. The study would have given a better insight of the operational response strategies to payment card fraud if all the eighteen banks responded. The payment card industry in the country is still at its infant stages of development, with a gradual growth and confidence amongst cardholders, a mature industry would present an array of operational response strategies being adopted by not only commercial banks but other financial institutions or card issuance companies. Time was also limiting.

5.4 Suggestions for further research

Payment card industry in Kenya is still developing; it presents an opportunity for various studies in operational strategy development, competitive analysis amongst other relevant operational management topics.

REFERENCES

Abiage, J. N. (2011, May 5). *Internet fraud costs Kenyan banks $ 36 Million*. Retrieved June 17, 2013, from Africareview.com: http://www.africareview.com/Business---Finance/Internet-fraud-costs-Kenyan-banks-dearly/-/979184/1156782/-/usmbrdz/-/index.html

ACI Worldwide. (2010). *Stopping Card Fraud in its tracks.* Omaha: ACI Payment Systems.

American Express Company. (2013, January 01). *About American Express*. Retrieved April 22, 2013, from American Express: http://about.americanexpress.com/?inav=footer_about_american_express

Anderson, R. R. (2009). Security economics and european policy. In *Managing Information Risk and the Economics of Security* (pp. 55-80). Springer.

Babbie, E. (1990). *Survey Research Methods.* Belmont, CA: Wadsworth.

Braun, M. J. (2008). Understanding Risk Management in Emerging Retail Payments. *Federal Reserve Bank of New York, Economic Policy Review, vol. 14, no. 2*, 137-159.

CAJ News. (2013, June 13). *Nigeria wins war against card fraud*. Retrieved June 14, 2013, from News24Nigeria: http://m.news24.com/nigeria/Business/News/Nigeria-wins-war-against-card-fraud-20130614

Central Bank of Kenya. (2012). *Annual Report.* Nairobi: Central Bank.

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

Company, 2. A. (2013, January 01). *About American Express*. Retrieved April 22, 2013, from American Express: http://about.americanexpress.com/?inav=footer_about_american_express

Daily Nation. (2012, December 26). *Bank reassures customers after spate of ATM fraud in City.* Retrieved May 5, 2013, from Nation: http://www.nation.co.ke/business/news/bank-reassures-customers-after-spate-of-ATM-Card-fraud-in-

Daily Nation. (2012, May 19). *Bankers press for legal backing to recover billions lost to fraudsters.* Retrieved May 5, 2013, from Nation: http://www.nation.co.ke/business/news/1006/1409316/-/3hvgwbz/-/index.html

Daily Nation. (2013, January 8). *Banks, Clients grapple with high-tech card skimmers-Smart Company.* Retrieved May 5, 2013, from Nation: http://www.nation.co.ke/features/smartcompany/banks-clients--grapple-with-card-skimmers/-

Digital Transactions News. (2012, October 16). *PCI Waiver Expected To Spur Merchant Adoption of EMV Terminals*. Retrieved July 9, 2013, from Digital Transactions News: http://digitaltransactions.net/news/story/3730

Doody, H. (2008). *Fraud Risk Management: A Guide to Good Practice.* United Kingdom: Chartered Institute of Management Accountants.

Europol. (2012). *Payment Card Fraud in the European Union.* EU: Public Version.

Fico.Com. (2012, June). *Managing Card Compromises from the issuers perspective.* Retrieved from www.fico.com.

Gerry Johnson, K. S. (2008). *Exploring Corporate Strategy* (8th ed.). United Kingdom: Prentice Hall.

Global Payments data breach exposes card payments vulnerability. (2012, April 3). Retrieved from www.forbes.com.

Hernandez, W. (2009). Debate Lingers Over Definition Of 'End-To-End' Encryption. *ATM & Debit News*, 1.

Hub, C. (2012, Jan). *Credit Card & Debit Card Fraud Statistics*. Retrieved June 18, 2013, from Card Hub: http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/

KBA. (2013). *Bankers Association Kicks-off Consumer ATM awareness campaign*. Retrieved July 26, 2013, from www.kba.co.ke: http://www.kba.co.ke/consumer-information/atm-safety-campaign

KCDCA. (2012, January 1). *KBA Affliates.* Retrieved May 4, 2013, from Kenya Bankers Association: http://www.kba.co.ke/affiliates

Kwambukha, M. (2013, 4 8). *Kenya Bankers Set Deadline for Chip and Pin Technology*. Retrieved 8 25, 2013, from www.itwebafrica.com: http://www.itwebafrica.com/ict-and-governance/256-kenya/230841-kenya-bankers-set-deadline-for-chip-and-pin-tech

Lewis, N. S. (2008). *Operations Strategy* (2nd ed.). United Kingdom: Pearson Education Limited.

Leyden, J. (2008, June 24). *Merchants Call Credit Card Industry's Bluff on Compliance*. Retrieved from The Register: www.theregister.co.uk/2008/06/24/pci_dss_

MasterCard. (2011). *Advancing Fraud Management for More Secure Payments.*

Masuda, B. (1993). *Credit Card Fraud Prevention: A successful Retail Strategy.* R. V. Clarke.

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.* Unpublished MBA Project of the University of Nairobi.

Ministry of Economy and Finance. (2012). *Statistical Report on Payment Card Fraud.* Rome.

Montague, D. A. (2010). *Fraud Prevention Techniques for Credit Card Fraud.* Hoboken, NJ, USA: John Wiley & Sons, Inc.

Morgan, J. (2012). *Payments Fraud and Control Survey.* Bethsaida: Association for Financial Professionals.

Mott, S. (2007, September 7). *Why POS Merchants Don't Buy into Payment Security*. Retrieved from Digital Transactions News: www.digitaltransactions.net/newsstory.cfm?newsid=1503

Mwakidedi, J. M. (2009). *A survey of the factors affecting the use of credit cards : A case study of postbank* . Unpublished MBA Project of the University of Nairobi.

Noka, I. (2010, September 1). Innovation in Payment Card Fraud Managment. *The Business of Fraud Risk Management.* Visa Public.

PCI Security Standards Council. (2013, July 07). *PCI Security Standards Council*. Retrieved July 13, 2013, from PCI Security Standards Council: https://www.pcisecuritystandards.org/

Pearce, J. A. (1991). *Strategic Management: Formulation Implementation and Control.* Irwin McGraw- Hill.

Porter, M. (1985). *Competitive Strategy.* New York: The Free Press.

Porter, M. E. (1980). *Competitive Strategy: Techniques for Analyzing Industries and Competitors.* New York: The Free Press.

Scott, M. (1998). *Value Drivers.* Chichester: Wiley.

Siciliano, R. (2013, March 15). *Europol: Credit Card Fraud Spells Low Risk and High Profits*. Retrieved June 17, 2013, from https://www.iovation.com: https://www.iovation.com/blog/europol-credit-card-fraud-spells-low-risk-and-high-profits[6/16/2013 10:40:54 AM]

Situma, E. (2013, April 11). *Banks to adopt new ATM cards in fight against fraud*. Retrieved August 22, 2013, from http://www.businessdailyafrica.com: http://www.businessdailyafrica.com/Banks-to-adopt-new-ATM-cards-in-fight-against-fraud/-/1248928/1745746/-/11guukm/-/index.html

Smart Storage Systems. (2012). Encryption and Data Elimination. *Smart Storage Systems*, 6-7.

Sullivan, R. J. (2010). The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options. 101-133.

Sunday, F. (2013, February 26). *Card firms fight for a slice of East Africa Cashless Society.* Retrieved April 22, 2013, from Standard Digital News - Kenya: http://www.standardmedia.co.ke/?articleID=2000078144&story_title=card-firms-fight-for-a-slice-of-east-africa-cashless-society

Taylor, D. (2013, April 15). *Data Security Slugfest: Tokenization Vs End-to-End.* Retrieved from Storefront Backtalk website: www.storefrontbacktalk.com/supply-chain/data-security-slugfest-tokenization-vs-end-to-end-encryption/#comments

Trochim, W. M. (2006). *Nonprobability Sampling.* Retrieved from Research Methods Knowledge Base: http://www.socialresearchmethods.net/kb/sampnon.php

Visa. (2009). Data Field Encryption Version 1.0. *Visa Best Practices*, 1.

Visa. (2010). Best Practices to Optimize your Fraud Strategies. *Visa Issuer Tools and Best Practices*, 2.

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

Visa. (2011). *Visa International Operating Regulations.* United Kingdom: Visa International.

Visa. (2012). *Visa Europe Annual Report.*

Visa Europe. (2013, August 22). *PIN security*. Retrieved 2013 22, August, from www.visaeurope.com: http://www.visaeurope.com/en/businesses__retailers/payment_security/pin_security.aspx

Visa International. (2013, August 22). *Securing the future of digital payments*. Retrieved August 22, 2013, from www.visaonline.com:

https://www.cms.eu.visaonline.com/VE_CMSLogin/risk_management/accommodating_complexity.aspx

Walters, D. (2008). Strategic and Operational Drivers in Emerging Business Models: New Perspectives for the Economics of Production. *Oxford Business and Economics Conference Program* (pp. 25-26). Oxford, UK: Oxford.

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

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

Wikipedia. (2013, July 31). *3-D Secure*. Retrieved August 22, 2013, from www.wikipedia.com: http://en.wikipedia.org/wiki/3-D_Secure

Wikipedia. (2013, April 10). *Credit Card*. Retrieved April 22, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Credit_card#Benefits_to_merchants

Wikipedia. (2013, March 15). *Wikipedia*. Retrieved April 22, 2013, from Payment Card: http://en.wikipedia.org/wiki/Payment_card

Wilhelm, W. K. (2004). The Fraud Management Lifecycle Theory: A Holistica Approach to Fraud Management. *Journal of Economic Crime Management*.

Williams, D. A. (2007). Credit card fraud in Trinidad and Tobago. *Journal of financial Crimes*, 340-359.

Worthington, S. (1995). The Cashless Society. *International Journal of Retail and Distribution Management*, 31-40.

Yapputro, H. (2011). *Determining Credit Card Fraudulent* . Jakarta: HSEY Publishing.

INTRODUCTION LETTER

Jeremiah M. Munyua

University of Nairobi

P. O. Box 30197

Nairobi.

August 2013

Dear Sir/Madam,

RE: DATA COLLECTION

I am a postgraduate student at University of Nairobi undertaking a Master of Business Administration degree program majoring in Operations Management. One of my academic outputs before graduating is a research project and for this I have chosen the research topic "**Operational Response Strategies to Payment Card Fraud by Commercial Banks in Kenya**". You have been selected to form part of the study.

This is to kindly request you to assist me collect the data by responding to the interview guide. The information you provide will be used strictly for academic purposes and will be treated with utmost confidence. A copy of the final report will be available to you upon request. Your assistance will be highly appreciated.

Yours sincerely,

Jeremiah M. Munyua

QUESTIONNAIRE

QUESTIONNAIRE FOR MANAGEMENT STAFF IN SELECTED UNITS OF VARIOUS BANKS IN KENYA

This questionnaire seeks to collect information on the effectiveness of operational response strategies adopted by commercial banks in Kenya in combating payment card fraud. Kindly provide answers to all questions asked as it concerns your organization. All the information will be treated confidentially and used for academic purposes only.

INTERVIEW QUESTIONS

1. What department are you in? _____
2. How many active cards do you have in circulation?
   ☐ Less than 500,000 ☐ Between 500,000 and 1 Million ☐ Over 1 Million
3. Is your organization a member of Kenya Credit and Debit Card Association?
   ☐ Yes ☐ No
4. Do you issue Visa payment cards?
   ☐ Yes ☐ No
5. Do you issue MasterCard payment cards?
   ☐ Yes ☐ No
6. Please indicate the extent to which you agree or disagree with the following statements regarding your cardholders preferred transaction channel.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Most of our cardholders prefer to use their cards on POS					
Most of our cardholders prefer to use their cards on ATMs					
Our cardholders use their cards for internet (e-commerce) transactions					

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

	Strongly Agree	Disagree	Neutral	Agree	Strongly Agree
We have experienced attempted card fraud this year					
We have experienced actual card fraud this year					
Card fraud incidences have increased this year compared to last year					
We have had lost card fraud this year					
We have had stolen card fraud this year					
We have had counterfeit card fraud at a POS this year					
We have had counterfeit card fraud at ATMs this year					
We have had card-not-present fraud this year					
We have had account takeover fraud					
We have experienced a data breach on our card systems					
We have experienced a data breach on our merchant systems					
Card-not-present fraud has been on the increase in our organization					
Card present fraud has been on the increase in our organization					

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

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Disagree
We store card data in encrypted or unreadable format					
We are fully PCIDSS certified					
Our merchants are fully PCIDSS certified					
We comply with PIN security guidelines					
We use a real-time fraud prevention system					
We use a fraud detection system					
We send transaction alerts for ATM transactions					
We send transaction alerts for POS transactions					
We have in place a rapid compromise and investigations team					
We utilize 3-D secure on our cards					
We issue EMV-Chip Cards					

9. Rank the following strategies in terms of their effectiveness in combating payment card fraud in your organization from 1 to 5. (Where 1=Most Effective and 5=Least Effective)

	1	2	3	4	5
Issuing EMV chip cards					
Implementing 3-D secure technology					
Using advanced authorization systems					
Transaction monitoring					
Complying with PCIDSS requirements					

Implementing PIN security programs						
Sending transaction alerts						
Tracking compromised card activity						
Monitoring chargebacks						
Quick compromise response						
Investigations						

10. Please indicate the extent to which you agree or disagree with the following statements regarding your organization. (Where 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree and 5=Strongly Agree)

	1	2	3	4	5
We detect fraud as soon as it occurs					
Our card risk system declines most fraudulent transactions					
Our average monthly fraud loss to monthly sales turnover is low					

11. How would you rank the following challenges in managing card compromise event?

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

12. What challenges do you encounter in addressing the card fraud challenge in your organization?

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

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

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The regulator that is Central Bank of Kenya has provided support in combating card payment fraud					
The criminal justice system is well equipped to deal with card payment fraud					
KBA card security awareness programs are effective in reducing card payment fraud					
KCDCA education and training programs are effective in reducing card payment fraud					
The main card schemes in the country have provided adequate support in tackling card payment fraud in Kenya					
My organization has suffered reputation damage from card payment fraud incident reports					

Thank you very much for your cooperation.

LIST OF COMMECIAL BANKS IN KENYA

- ABC Bank (Kenya)
- Bank of Africa
- Bank of Baroda
- Bank of India
- Barclays Bank
- Brighton Kalekye Bank
- CFC Stanbic Bank
- Chase Bank (Kenya)
- Citibank
- Commercial Bank of Africa
- Consolidated Bank of Kenya
- Cooperative Bank of Kenya
- Credit Bank
- Development Bank of Kenya
- Diamond Trust Bank
- Dubai Bank Kenya
- Ecobank
- Equatorial Commercial Bank
- Equity Bank
- Family Bank
- Fidelity Commercial Bank Limited
- Fina Bank
- First Community Bank
- Giro Commercial Bank
- Guardian Bank
- Gulf African Bank
- Habib Bank
- Habib Bank AG Zurich
- I&M Bank
- Imperial Bank Kenya
- Jamii Bora Bank
- Kenya Commercial Bank
- K-Rep Bank
- Middle East Bank Kenya
- National Bank of Kenya
- NIC Bank
- Oriental Commercial Bank
- Paramount Universal Bank
- Prime Bank (Kenya)
- Standard Chartered Kenya
- Trans National Bank Kenya
- United Bank for Africa[2]
- Victoria Commercial Bank

Source: Central Bank of Kenya Annual Report, 2012 (Central Bank of Kenya, 2012)

KCDCA MEMBERS

- ☐ Barclays Bank of Kenya
- ☐ Chase Bank
- ☐ Commercial Bank of Africa
- ☐ Co-operative Bank of Kenya
- ☐ De la Rue Kenya
- ☐ Diamond Trust Bank Kenya
- ☐ Equatorial Commercial Bank
- ☐ Ecobank
- ☐ Equity Bank
- ☐ Fidelity Bank
- ☐ Kenya Commercial Bank
- ☐ I&M bank
- ☐ Imperial Bank
- ☐ Kenswitch
- ☐ National Bank of Kenya
- ☐ NIC Bank
- ☐ Paramount Bank
- ☐ Paynet Kenya Ltd
- ☐ Postbank Kenya
- ☐ Prime Bank
- ☐ CfC Stanbic Bank
- ☐ Standard Chartered Bank

Source: KCDCA, 2012