ADOPTION OF EUROPAY, MASTERCARD AND VISA TECHNOLOGY AND CARD FRAUD IN THE KENSWITCH NETWORK ENVIRONMENT

BY

ANTHONY SITUMA WAKHISI

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

NOVEMBER, 2015

DECLARATION

This is my original work and has not been submitted for examination in any other university or college.

Signature: ____________________________ Date: ______________________________

Anthony Situma Wakhisi
D61/P/7999/2000

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

Signature: ____________________________ Date: ______________________________

Joel Lelei
Lecturer
Department of Management Science
School of Business
University of Nairobi

DEDICATION

This paper is dedicated to my lovely wife Susan, my sons Ian, Immanuel and Nathan for their enormous 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 Kenswitch network forum.

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

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AC	Application Cryptogram
ARQC	Authorization Request Cryptogram
ATM	Automated Teller Machine
CBK	Central Bank of Kenya
CNP	Card-not-Present
CVM	Card Verification Method
DAC	Data Authentication Code
DSS	Data Security Standard
EMV	Europay MasterCard Visa
IC	Integrated Circuit
ICC	Integrated Circuit Card
ICT	Information Communication Technology
IHCF	Industry Hot Card File
KBA	Kenya Bankers Association
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
POS	Point of Sale

ABSTRACT

The purpose of this study was to determine the adoption of EMV technology and card fraud in the Kenswitch network environment. The study was guided by the following research objectives, to determine the extent of adoption of EMV technology in the Kenswitch network environment, to establish the challenges faced in adoption of EMV technology in the Kenswitch network environment and to establish the level of fraud experienced as a result of EMV implementation. The study clearly identifies the global trend in migration to EMV technology, the various challenges associated with adoption of EMV technology and the impact of adopting it. This research study used the descriptive survey research design. The target population of the study was 35 Kenswitch member institutions where census was used in this study. The study collected primary data through the use of questionnaire which generated both qualitative and quantitative data, where quantitative data analyzed using descriptive statistics. Based on the findings of the study, most of the Kenswitch members have adopted EMV technology to minimize payment card fraud. The members have experienced varied challenges in the adoption of EMV technology. Most of the commercial banks on the Kenswitch network have adopted EMV. The high adoption of EMV technology seems so because of the need for the institutions to address the payment card fraud menace. The study concludes that most of the financial institutions such as commercial banks had adopted EMV. The study also concludes that payment card industry has lagged behind other developing economies in adopting more secure chip-embedded EMV cards. Further the study concluded that Kenya financial industry and the merchant community have a once in a lifetime change to bring their payment infrastructure to a state-of-the-art level which addresses usability, functionality, security and cost requirements. Fraud rates remain fairly low in spite of fraud experienced in recent years.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Europay, MasterCard and Visa (EMV) is a global standard for payment cards based on chip technology established in 1994 by Europay International (acquired by MasterCard in 2002), MasterCard, and Visa. Today the EMV standard is managed by EMVCo, a consortium made up of six member organizations, namely American Express, Discover, JCB, MasterCard, Union Pay and Visa. The EMV specification can be used in both online and offline environments and supports both signature and PIN verification with PIN being the dominant verification method used to date (Green, 2006).

The EMV chip carries cardholder and account data and is programmed to make decisions about a transaction and control its outcome, that is approve or decline it. Chip cards can be produced as “chip-and-PIN”, “chip-and-signature” or “chip-and-none” which are all collectively called “chip-and-choice” (which allows the cardholder to use a personal identification number (PIN), a signature or neither a PIN nor a signature).Transactions are verified through the card verification method programmed into the chip. If the card is to have a PIN associated with it, the PIN is programmed into the embedded chip before the card is issued to the cardholder (Idowu, 2009).

The rise in card fraud is a big challenge for the banking industry and financial institutions in the global society. The fraudulent funds obtained are used to fuel organized crime worldwide through such activities as drug trafficking and terrorism which pose a threat to global peace security. However, the banking and related industries in collaboration with the card industry has started to address the problem by introducing various initiatives in the fight against card fraud. For example in 2004, the UK card industry under great pressure from Visa and MasterCard started the implementation of chip and PIN technology. By the end of 2005 about 107 million cards out of 141 million cards had been upgraded to chip and PIN which led to a 13% reduction of plastic card fraud (Figliola, 2015).

EMV must be considered in the context of the current transaction processing environment where the confidentiality of cardholder data from EMV transactions, along with sensitive authentication data from non-EMV transaction remains fundamental to ensuring the integrity of the payment system (Burns & Weir, 2008).While EMV can substantially reduce fraud in card-present transactions, it does not automatically satisfy PCI DSS requirements for the protection of cardholder and sensitive authentication data. Within this context of current EMV deployment, the need to protect the confidentiality of the cardholder and sensitive authentication data as prescribed by PCI DSS is still a critical part of the industry's overall effort to prevent that data being used for fraudulent transactions in other environments (Burns & Weir, 2008).

In the future, EMV may become the sole means of payment in a given face-to-face channel coupled with a globally adopted robust authentication process for card-not-present (CNP) transactions, the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. As a consequence, the PCI DSS would be update to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly (Gray & Ladig, 2015).

Today EMV and PCI DSS, as well as the PA-DSS, are complementary and form important layers in providing a holistic approach to the objectives of reducing overall card fraud and securing cardholder data in the payment industry. In those markets which have migrated or are in the process of migrating to EMV, payment industry stakeholders should use EMV and PCI DSS together to reduce card fraud and increase security (Idowu, 2009).

EMV Technology

Burns and Weir (2008) contend that EMV smartcards were designed and introduced to reduce card fraud occurring in magnetic stripe face-to-face environments, by using integrated-circuit (IC) based cards that use secret cryptographic keys to generate authentication and authorization data. As such, robust implementations of the EMV specifications can mitigate the risk of compromised card data being used to commit face-to-face card fraud.

To understand how current EMV acceptance and processing environments relate to the PCI DSS, one must examine the data elements present in EMV transactions and understand how this information may be used in a fraudulent manner. In addition, it is important to understand the limited protection inherent in non-EMV transactions and how this information is susceptible to fraudulent use should it be disclosed (Gray & Ladig, 2015).

The concept of EMV standard provides transaction security and global interoperability within an EMV transaction environment. EMV implementation that use card verification values which are different from those maintained in the magnetic stripe mitigate the risk of compromised EMV transaction data being used to create counterfeit cards. Likewise EMV actively prevents card-cloning attacks through the use of enhanced card authentication methods and when implemented in conjunction with PIN as a method of cardholder verification, limits the impact of lost/stolen/never-received categories of card fraud. However, EMV does not protect the confidentiality, nor prevent the compromise of certain transaction data elements (Idowu, 2009).

Most environments processing EMV transactions today are hybrid environments, handling both EMV and non-EMV transactions. In such circumstances protecting the confidentiality of cardholder and sensitive authentication data remains essential to ensuring the integrity of the payment chain (Katz, 2005).

Gray and Ladig (2015) contend that EMV standard provides transaction security and global interoperability within an EMV transaction environment. EMV implementations that use card verification values which are different from those maintained in the magnetic stripe mitigate the risk of compromised EMV cards. Likewise EMV actively prevents card-cloning attacks through the use of enhanced card authentication methods, and when implemented in conjunction with PIN as a method of cardholder verification, limits the impact of lost, stolen or never-received categories of card fraud.

Stix (2004) asserts that EMV is the sole method of effecting payment in a given face-to-face channel. In a mature EMV environment this could involve a migration to an EMV-only card which would reduce the hybrid environment threat while still allowing transmission of the cardholder PAN and other sensitive data in clear-text. For environments which do not migrate to an EMV-only card, but where EMV is the only method for face-to-face payment, the use of differing card verification values maintained on the chip and in the magnetic stripe is essential.

Bjoklund (2007) predicts that in the future EMV may become the sole means of payment in a given face-to-face channel, coupled with a globally adopted robust authentication process for card-not-present (CNP) transactions, then the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. As a consequence the PCI DSS would be updated to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly.

Today EMV and PCI DSS, as well as the PA-DSS, are complementary and form important layers in providing a holistic approach to the objectives of reducing overall card fraud and securing cardholder data in the payment industry. In those markets which have migrated or are in the process of migrating to EMV, payment industry stakeholders should use EMV and PCI DISS together to reduce card fraud and increase security (Ron, 2008)

1.1.2 Adoption of EMV

The EMV standard, in its simplest form is a global standard for a smart card chip-based payment application. This includes all levels of interaction at the physical, electrical, data and applications levels used for authenticating chip credit and debit card transactions (Ewald, 2015). The EMV technology provides support for a wide variety of other applications including secure log on access to bank websites, loyalty programs, identity verification and much more. In addition, the card issuers can increase customer service levels, acquire new cardholders, achieve top-of-wallet status with international travellers, increase international transaction market share and increase interchange revenue with global transactions (Sullivan, 2009).

A significant part of the business case for EMV adoption is based on reduction in various instances of card fraud. If the issuers act quickly they can relieve the portion of their card fraud liability that is caused by counterfeit cards. Conversely if merchants upgrade to EMV-capable system, they can dramatically reduce the likelihood that they will incur any card fraud losses related to their acceptance of counterfeit cards (Murdoch, 2007).

EMV equipped chip cards are powered by an embedded microprocessor which provides enhanced security features that current magnetic stripe cards cannot. The microprocessor or “chip” is secured behind a 1cm square contact on the front of the card. The chip enables contact and/or contactless technology to process secure payments. Additional benefits of EMV cards include faster processing than magnetic stripe cards and increased data storage for cardholder information. Secondary ecosystem players such as ATM and terminal manufacturers and chip manufacturers play a role. Players become more important in the EMV landscape when reviewing adoption and co-innovation risks (Nilson, 2012).

1.1.3 Challenges in the Adoption of EMV

Interestingly the timing of the EMV rollout allows Visa and MasterCard to minimize a few of the major risks around both EMV and mobile adoption. However, there are challenges in the adoption of EMV. One of the major challenges in the adoption of EMV by merchants, issuers and ATM deployers, is that the cost of moving to EMV is extremely high in the face of unproven consumer demand and an uneven distribution of costs/benefits that arise for each of the stakeholders. Visa and MasterCard have created a way of dealing with these issues, by simply forcing players to play the game (Bustos, 2011).

Another challenge is that the revenue generated from payment services can be significant for some payment providers, and a change in payment security standards can affect those revenue streams (Murdoch, 2007). For example estimates show that banks make more revenue from signature debit compared to PIN debit. Because the EMV and X9.59 standards would essentially eliminate signature debit, bank revenue for payment services could be reduced (Levi & Kaya, 2001).

An inferior security standard can be difficult to displace in a network market once it is in place. Customers decide to adopt a new product based on the number of others that use the product and the perceived benefits of shifting to a new product (Greenstein & Stango, 2007). Thus, a large installed base of an existing product is a barrier to adopting a new product with a superior technology. In the payments market, the larger the number of consumers and merchants using a particular security standard, the higher the perceived security benefit must be to justify a switch (Meacham, 2008).

1.1.4 EMV and Card Fraud

Card fraud occurs when an imposter takes over a payment account. An account takeover may occur when a hacker obtains a consumer’s user ID and password to access an online banking account and then performs fraudulent transactions. The share of signature and PIN debit fraud due to account takeover is also common (Sullivan, 2009).

According to Murdoch, Drimer, Anderson and Bond, (2010) fraudsters' cost-benefit calculations for exploiting other flaws in the EMV specifications will also change. Computer experts have uncovered potential weaknesses on EMV payment cards. For example, fraudsters could tap into the middle of a payment communication link, alter and divert the payment message to a confederate, and fool the payment approval system into accepting a fraudulent payment. These exploits are prototypes that are difficult to implement and there are no reports of their use other than as demonstrations. However, the payoff to payment fraud is high enough that fraudsters are likely to research these alternatives and possibly develop technology to make them practical (Murdoch, 2007).

Dynamic authentication helps prevent card fraud at the transaction level. It stops fraudsters from making fraudulent payments merely by replaying the data from a payment card that uses the same verification code for every transaction. Under a dynamic data authentication protocol, such as approach would not be successful because fraudsters cannot generate the ever-changing verification codes needed for successive transactions (Anderson, 2008).

The robust technology behind chip cards, particularly EMV offer a solution to help merchants and issuers manage a variety of card fraud types including counterfeit and lost/stolen cards (when a PIN is required). The chip is able to store significantly more information than the magnetic stripe. This provides a successful solution to the counterfeit card fraud endemic, but fraudsters quickly adapt to new security measures and increase their focus on committing other types of card fraud. While EMV technology does not combat all types of card fraud (including lost/stolen, never-received categories, and account takeover), its ability to greatly reduce fraudsters' ability to produce counterfeit payment cards is a substantial benefit merchants and issuers need to reduce card fraud at the POS (Nilson, 2012).

1.1.5 Kenswitch Limited

Kenswitch is a registered limited company that was set up by a consortium of banks under the National Payments Systems modernization and reform process of the Central Bank of Kenya, to provide to the financial community a shared payments infrastructure so as to facilitate the use of debit cards for the bank's customers. Kenswitch network has over 1,800 ATMs and over 3,000 point of sale (POS) terminals which are currently distributed in over 110 towns around Kenya. Kenswitch operates payment switch that allows its member institutions (card issuers and card acquirers) and merchant processors to communicate and corporate to provide a wide range of payment services. Currently, Kenswitch has 36 member institutions (See Appendix II) on its network.

Kenswitch acts purely as a switch that facilitates interconnectivity amongst the different member institutions. The core functions of Kenswitch are managing a network of terminals, routing transactions to the appropriate member and/or terminal, seeking authorizations for customer transaction requests, card production and timely, accurate clearing of settlement data. With Kenswitch acting as the central switch, the adoption and implementation of EMV is essential to provide a secure payments network environment that will lend support to its members to achieve their business goals and provide their customers with secure payments. Kenswitch has invested substantially in upgrading its payments infrastructure to meet the EMV technology requirements for its members in transaction acquiring and switching and also payment card issuance. Kenswitch has developed a local standard for an EMV financial payment application that allows its members to transition from the standard magnetic stripe card to an EMV card that conforms to the EMVCo card specifications.

Growing cases of card fraud and cyber-crime means that financial institutions need to urgently invest in detection and preventive mechanisms as today's fraudsters are increasingly sophisticated. According to data from the Banking Fraud Investigations Department (BFID), financial institutions reported Ksh1.49 billion ($17.52 million) stolen from customers' accounts between April 2012 and April 2013. In 2013, the Kenya banking industry proactively adopted the EMV compliance standard for payments cards in the market for the ultimate benefit of local payment card industry. The move was unprecedented in the region and came at a significant cost, however, it was agreed that all banks, institutions and payment switches operating in the country would upgrade their systems for the ultimate benefit of local payment card industry.

1.2 Research Problem

The global trend towards the great migration of EMV chip brings together various stakeholders in Kenya's banking and payments technology sectors in an effort to hasten the switch to EMV cards. The payment cards are replacing paper-cheque as the primary means of paying for goods and services and like all other payments, payment cards have their own security vulnerabilities that need to be resolved collectively by the whole payment card industry (Ogony, 1999).

It is understood and accepted that different markets in various regions around the world are at different stages of EMV roll-out and maturity. Those markets which are not yet in a mature state will be working toward achieving the recommendations of the payment card brands and EMVCo. For environments which do not migrate to an EMV-only card, but where EMV is the only method for face-to-face payment, the use of differing card verification values maintained on the chip and in the magnetic stripe is essential.

Boston retail partners (2015) study suggests that while only 10 percent of retailers currently support EMV card payments, an additional 35 percent plan to do so by October 2015, the deadline for EMV migration. Sullivan (2009) observed in his research study that cards with an EMV chip use dynamic data, and the chip creates a unique transaction code for each payment transaction. The ability to use dynamic data provides valuable security as a transaction is initiated and processed at a point-of-sale. Punch (2013) contends in his research study that though some card brands began migrating to the EMV standard in the early 2000s, magnetic stripe payment cards are still the norm in the unites states.

In the recent past the banking sector in Kenya has witnessed a rapid growth, issuing thousands of credit cards and millions of debit cards to their customers. The frequency in which customers use these cards for various transactions raised concerns of whether customers had lost control over their finances (Ogony, 1999).

Several local studies on this area have provided very little understanding on the impact of the use of debit and credit cards, and more so the EMV cards on customers' cash flow management control. Simiyu, Momanyi, Naibei and Odondo (2012) undertook a study on credit and debit card usage and cash flow management control by customers. (Mayabi (2011) studied the factors influencing use of credit cards in Kenyan commercial banks in Nairobi County, Kenya. All these studies were relevant to the specific fields but none clearly explored the challenges encountered in EMV implementation in financial sector, or in broader banking industry. The global payment system continues to transition from magnetic-stripe to chip technology due to the increased security it provides. In particular, many regions including Kenya are transitioning to the EMV standard to combat the high rate of card cloning fraud that is easily achieved with the current magnetic stripe technology.

Therefore a knowledge gap exists on challenges encountered in EMV implementation at Kenswitch. This necessitates the need for this research study to be undertaken. It is on this basis that this study will be conducted to answer the questions; What is the extent of adoption of EMV? What are the challenges encountered in EMV implementation? and What level of card frauds have been experienced in the local payments card industry after implementing EMV?

1.3 Research Objectives

This study was guided by the following objectives:

i. To determine the extent of adoption of EMV technology in the Kenswitch network environment.

ii. To establish the challenges faced in adoption of EMV technology in the Kenswitch network environment.

iii. To establish the level of fraud experienced as a result of EMV technology implementation in the Kenswitch network environment.

1.4 Value of the Study

The findings of this study will benefit various groups of people. The management of Kenswitch will benefit substantially from this study, since it will assist the management in identifying the challenges faced in implementing the EMV technology in the Kenswitch network environment. They will be able to determine whether the existing EMV technology being used in the Kenswitch network environment is efficient in ensuring that problems are identified and addressed early enough before they impact negatively on the organization. They will also serve to inform both current and future EMV technology users on evaluation and implementation by Kenswitch and its members.

Researchers and academicians will benefit from this research study, as it will add to the body of knowledge in EMV technology and specifically on how financial institutions and the banking industry in general respond to the challenges by this new technology in their environment. This study will also apply to ICT policy, theory and practice by emphasizing that institutions employ corporate, business and functional ICT technology in addressing the emerging technological advancement in the microchip technology, and more specific the EMV technology, and its challenges in the extent of implementation.

The study will also be important to banking industry stakeholders as its documentation and evaluation of Kenswitch's implementation of the EMV technology will serve as a reference point for similar or related studies in the banking industry. In addition other stakeholders such as microfinance institutions, commercial banks, building societies and other financial institutions whose interest lie in provision of secure card payment services will benefit a great deal.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter focuses mainly on previous literatures that have been written by various scholars, researchers and authors. The key points of discussion are: EMV technology implementation, concept of EMV technology, the challenges facing EMV implementation and the benefits accrued from the use of EMV technology in payment transactions.

2.2 EMV Technology

EMV places significant prominence on the actions of the chip. All parameters and choices are driven by software that is loaded on the chip. The software called a “payment application” dictates how a payment is acquired and processed. Moreover the application determines how to communicate with the terminal through the use of encrypted keys that must be loaded at the terminal and by the downstream participants in the payment authorization (Bidgoli, 2012).

Chip cards are essentially miniature computers with an operating system, multiple interfaces and applications that process information through the use of an embedded microprocessor and a gold or silver-coloured contact place mounted on the front of the card. EMV cardholders insert a card into the reader, spurring dialogue between the card and terminal that validates the card, terminal and issuer through the exchange of secure cryptograms enabling a more secure transaction (Ewald, 2015).

EMV currently supports four cardholder verification methods (CVMs). These are based on card issuer preference and different terminal capabilities. First, there is signature verification, which compares the cardholder signature on the receipt to the signature on the back of the card. Second, there is online PIN encrypted and verified online by the card issuer. Third, there is offline PIN, which is verified offline by the EMV card and only passes along the result of the transaction. Fourth and finally there is no CVM option, which typically occurs with low-value transactions or for transactions at unattended POS locations. From the cardholder perspective the personal preference for using PIN or signature will continue to be supported for the foreseeable future (Gray & Ladig, 2015).

Although EMV is often equated with “chip and PIN” they are not the same thing. Chip and PIN is just one possible implementation of the EMV technology. In fact the technical specification for EMV-enabled cards do not require a PIN, or a signature, or any other form of cardholder identity verification. Rather, the issuing bank specifies which cardholder verification services are required for a transaction with rules it places on the chip. Regardless, it is widely accepted that the combination of card validation via the chip, and cardholder authentication with a PIN provides the greatest protection against common consumer-level attacks like fraudulent use of lost or stolen cards, counterfeit cards and skimming (Kim & Vasarhelyi, 2012).

Ron (2008) posits that a technical specification that outlines and ensures the global interoperability between the chip cards and the ATMs and point of sale terminals at retail outlets led to the development of a universal standard known as EMV, by a consortium that was formed between Europay, MasterCard and Visa in 1994. The standard enables a microprocessor chip at the point of sale terminal or ATM machines to allow chip cards to communicate with readers and software thus ensuring the international acceptance of the technology.

The payments industry is moving towards global interoperability with chip technology that provides form factor flexibility with value-added service capabilities and increased security. The EMV payments infrastructure includes a network message field that transports chip data between the card and the issuer. The field must be added to the authorization request, authorization response and, in some cases the clearing and settlement data.

2.3 Adoption of EMV

Factors such as the need for improved security in the wake of significant card compromises, the fraud liability shifts announced by Visa and MasterCard, and the need for a better experience for international travellers are driving the financial services market to migrate to EMV. To best mange this complex changing landscape, financial institutions have begun to leverage the benefits of chip-based cards and control the associated investment through a practical transitional approach to EMV migration (Figliola, 2015).

The EMV solution is now being adopted in the debit processing. However through groups like the EMV migration forum, the industry has collaborated to develop a solution that is viable and that supports the requirements of the Durbin Amendment. The increasing number of networks coming on board will enable debit card issuers to offer merchants (Sullivan, 2009).

EMV technology for credit is a more mature solution, while EMV debit offering is still in its infancy, so financial institutions that are credit card issuers should consider starting with a compliant EMV credit card that offers basic features. The right approach to implementation of an EMV card program is critical in reducing the overall investment of time and expense.

Fundamentally, the integrity of the payments systems must be protected. Migrating to chip supports this objective and can provide a foundation on which to build additional enhancements for card-not-present fraud. The current drivers to migrate to EMV do ultimately fall back to either fraud or marketing-related drivers (Arnfield, 2006).

Implementation of the EMV standard has prompted some card networks to shift liability for fraud from card issuers to other payment participants, which can reduce the incentive of card issuers to limit fraud (Anderson et al., 2001). This has broad consequences because card networks and issuers have a great degree of control over security protocols in payment authorization.

2.3.1 EMV Risk Management

The developed and developing countries have taken various initiatives in preventing and reducing card fraud in their countries by EMV technology in the following manner: the adoption of chip and PIN technology, the use of tactical programmes that assist in creating awareness among retailers on card fraud problems, the provision of incentives and financial rewards for the capture of fraudulent cards and any information leading to the capture of card fraud criminals, the development of token-based authentication to be used in card-not-present environment, cardholder education on safe handling of cards and

PIN numbers, the use of fraud detection computer systems by banks, the lowering of floor limits and the use of industry hot card file (IHCF) to check every card transaction for cards being used fraudulently (Ron, 2008).

The EMV specifications define features to allow card issuers to manage the risk of when to support offline transactions or if to support offline transactions at all. Payment brands enhance the EMV specifications with additional flexibility and offer issuers a comprehensive set of configuration parameters to allow an EMV card to perform (or not perform) an offline EMV transaction. Offline risk management parameters on the card are defined by the issuers and usually consist of offline limits expressed in two different ways: number of consecutive offline transactions, or cumulative amount of offline transactions. When either of these limits is exceeded the issuer forces the transactions online and/or the card declines the transaction (Green, 2006).

Figliola (2015) examines whether changing the EMV chip cards in the US would be beneficial, whether changing to EMV chip cards would actually reduce card fraud. He contends that adopting EMV chip cards without installing appropriate technology to read the chip cards does nothing to reduce card fraud. EMV chip cards have both an embedded microchip and a magnetic stripe. Machines in the US currently only read the magnetic stripe and do not process the embedded microchip, which means chip cards used on current machines in the US currently provide no additional protection against card fraud.

EMV provides a significant opportunity to manage down the risk of card transactions. Use of the chip cryptogram to properly handle chip card and POS authentication means that valuable fraud resources need not be directed to checking out the authenticity of transactions which are obviously not counterfeit. The technical platform provided by EMV is very powerful. However it is crucial that banks also consider how EMV, and in particular the introduction of PIN, impacts cardholders (Nilson, 2012).

One purpose of a security standard is to ensure compatibility. For example, the EMV standard must be used with compatible card reader. Most payment card readers are not compatible. A payment network establishes its own security features, which can make its payment instrument either compatible with the hardware and communications systems of other payment networks (Ward, 2006). Compatibility alone however may not ensure a more towards a stronger payment authentication standard. In markets where network externalities and economies of scale are strong, the industry is likely to emerge as an oligopoly (few firms) where there is one dominant firm (Wiseman, 2000).

A dominant firm with loyal customers will likely be uninterested in establishing a common security standard, despite the efficiencies and enhanced social welfare that might accompany a common standard, because the firm may perceive a competitive advantage to incompatibility (Wiseman, 2000). If the benefits of standardization are strong enough, we may observe a coalition form to establish standards, as has happened with EMV. But gaining consensus can be difficult (Khu-Smith & Mitchell, 2002).

2.3.2 EMV Transaction Security

EMV is an open-standard set of specifications for smart card payments and acceptance devices. EMVCo, owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa, manages, maintains and enhances the EMV specifications, to ensure global interoperability of chip-based payment cards with acceptance devices including point of sale terminals and ATMs. In addition to storing payment information in a secure chip rather than on a magnetic stripe, using EMV improves the security of a payment transaction by adding functionality in three key areas: card authentication - protecting against counterfeit cards and skimming (i.e. to produce a copy of an authentic card), cardholder verification - authenticating the cardholder and protecting against lost and stolen cards, and transaction authorization - using issuer-defined rules to authorize transaction (Gray & Ladig, 2015).

Card authentication protects the payment system against counterfeit cards. Card authentication methods are defined in the EMV specifications and the associated payment brand chip specifications. Card authentication can take place online, offline or both. Online card authentication requires the transaction to be sent online for the issuer to authenticate and authorize in the same way magnetic stripe transactions are sent online. The important difference is the chip card's use of symmetric key technology to generate an application cryptogram (AC). This cryptogram type called Authorization Request Cryptogram (ARQC) is validated by the issuer during the online transactions.

Cardholder verification authenticates the cardholder. Use of personal identification number (PIN) used to authenticate the cardholder and protect against the use of a lost or stolen card. EMV supports four types of CVMs, allows the use of multiple CVMs and defines the conditions under which they may be used: offline PIN, online PIN, signature verification, and No CVM (Bidgoli, 2012).

A cardholder's confidential data is more secure on a chip-embedded payment card than on a magnetic stripe card. Chip-embedded cards support dynamic authentication whereas data on magnetic stripe cards is static. Thus data from traditional mag stripe cards can be easily copied (skimmed) with a simple and inexpensive card reading device. Skimming enables criminals to make counterfeit cards for use at point-of-sale (POS) devices or in the CNP environment. Chip technology is effective in combating such counterfeiting through the introduction of dynamic values for each transaction (Idowu, 2009).

According to Figliola (2015) Visa, MasterCard, and American Express have developed and adopted proprietary security measures to make CNP more difficult to perpetrate: Verified by Visa, SecureCode, and SafeKey respectively. All the three are based on the 3-D secure protocol and are only used for internet-based purchases. They work by redirecting the payment transaction to the issuer's website to perform user authentication by requiring the cardholder to provide additional credentials before approving a transaction. The merchant, the cardholder, and the card issuer all must use the system for it to work.

Burns & Weir (2008) noted that security is a balance between confidentiality, authentication and integrity versus convenience, cost and reliability. They used the cost benefit analysis in their argument on the introduction of chip and PIN technology into the market. The cost of the EMV transaction and the current slow pace of adoption, as well as other issues in varying stages of being resolved, may hamper efforts of securing EMV transactions.

2.4 EMV Challenges

One of the biggest obstacles in implementing EMV is cost. POS systems capable of reading EMV cards can cost hundreds of dollars apiece. Ron (2008) estimates that across the U.S., merchants will need to either replace or upgrade an estimated 13 million POS systems to be ready for EMV card transactions. This is a big expense that will be passed down to the consumer. In addition, card-issuing banks will need to spend tens of millions to upgrade their networks and internal systems if they want to be ready for PIN debit and PIN credit transactions.

The EMV standard can be implemented in a variety of ways. A majority of EMV implementations around the world require cardholders to enter a PIN as an authentication measure when conducting a transaction. But EMV can also be implemented in less secure ways like simply as a chip card without a PIN, or as a chip card requiring either a signature or a PIN to authenticate the cardholder. MasterCard and Visa have left it largely to the card-issuing banks in the U.S. to decide which route they want to take.

Canada first began moving to EMV in 2003. More than 10 years later, only about 85% of the country's POS systems can take EMV cards. Meanwhile, in countries where merchants have almost completely shifted to EMV-enabled POS systems, the banks have been slow to issue smartcards (Burns & Weir, 2008). Migrating the U.S. payment system to EMV will take years, and by the time the process is complete, most payments would have shifted to mobile and online applications (Figliola, 2015).

Adopting EMV chip cards without installing appropriate technology to read the chip cards does nothing to reduce fraud. There have been some concerns in the U.S. about whether EMV chip cards will actually reduce fraud.

2.5 Card Fraud

Ron (2008) contends that while EMV helps mitigate card fraud at POS, it does not protect cardholder data once the payment method and consumer are validated. The cardholder and the card itself have now been validated through EMV but the actual card data is sent in the clear unless the merchant has layered on an encryption and tokenization solution to protect and remove sensitive card data from the merchant environment. A layered approach to card fraud and security is the only way to truly be protected. Two important layers include: card data security - a strong encryption and tokenization solution can bolster the security of the entire payment transaction and reduce PCI compliance efforts, card fraud protection – layer EMV with encryption and tokenization plus online fraud detection and prevention tools.

Although the migration to the chip technology gives the banks a vital tool in the fight against fraud, it is not the technology alone that creates a total solution. Rather, it is the way the bank uses the opportunity. By following the above simple steps, banks can deliver on the business case for the investment in chip and give a better service to their cardholders. For example offering PIN change functionality at ATMs enhances the likelihood of cardholders remembering their PIN without writing it down for a fraudster to discover (Murdoch, 2007).

According to data from the UK payments administration, EMV chip-and-PIN has been successful at reducing certain types of card fraud, especially domestic counterfeit and lost or stolen card fraud. Total card fraud in the UK began declining in 2005 as the chip-and-PIN movement gained traction.

As global experience demonstrates the adoption of chip technology to reduce card fraud at the POS but can also drive higher card-not-present (CNP) fraud. In tandem with bringing in EMV at the POS, the issue of CNP fraud needs to be addressed strategically with additional security layers such as fraud protection solutions and increased verification methods (Green, 2006).

Card fraud can be conducted in a number of ways, but it always begins with the theft of card information. The scale of the theft can range from small, such as stealing a wallet, to large such as skimming or a data breach. Data breaches can be carried out in more than one way (and for reasons other than committing fraud), but the most common method is hacking into a POS system used to make card-based purchases. These breaches are called "POS intrusions" (Burns & Weir, 2008). In 2013, 75% of breaches in the travel/hospitality sector and 31% in the retail sector were POS intrusion aimed at stealing credit and debit card data. Consumer financial card fraud due to data breaches of card information is an on-going problem in most countries. The majority of breaches are carried out against point-of-sale (POS) systems, and are facilitated by what many consider to be the weak link in retail sales payment process (Kim & Vasarhelyi, 2012).

2.6 Empirical Review

Stix (2004) researched on understanding credit card fraud. They described the various ways in which a credit cardholder may be a victim of card fraud, the impact of fraud on the credit cardholders, the merchants and the issuer banks, and also discovered in details the various card fraud prevention technologies. They suggest the adoption of EMV chip technology in credit cards.

Bustos (2011) contend that EMV, that is integrated on chip cards are being promoted in a big way in the western world as safe smart cards. In their research they found a lacuna in the system due to a protocol flaw which can circumvent the security net, and proves that these cards are not totally safe in the hands of techno savvy person. The researchers provided a solution to the card issuers to improve the technology and come out with the next improved version of EMV cards.

Green (2006) researched on the swipe and spend economy. They discussed the beginning of credit card usage with their recent marketing techniques and how it has affected credit card users of all ages from the teenagers to the senior citizens. Emphasis is given on reforms to ease the credit crunch on the average credit cardholder as well as the financial well-being of the world wide economy.

Gray and Ladig (2015) researched on the theory of credit card networks being a survey study. He discusses the benefits and costs that accrue to various parties involved in online transactions carried out using credit cards, viz credit cards users, merchants, issuers, acquirers and the networks on which the credit cards are used. He also studied the economic models affecting the inter-related bilateral relationships and offered some guidelines to policy makers.

Bjoklund (2007) focuses on the question of why merchants accept credit cards in a model of Cournot competition for merchants. He allows consumer demands to be elastic and free entry of merchants. The research finds that competing merchants will accept credit cards and when doing so enables them to earn higher margins. This result arises, to the extent consumers are willing to pay more for goods, when they have the ability to purchase by credit cards. Industry output increases when credit cards are accepted.

Sullivan (2009) highlights the experience of the United States in adopting computer-chip payment cards which shows the EMV payment cards offer capabilities for strengthening authentication and preventing card fraud. The degree of payoff from adopting the cards only emerges over time, however, because authentication methods tend to evolve and improve during a transaction period.

Ewald (2015) studied the mass adoption of EMV across Europe and observed that some participants of the US payment industry to believe that the US requires an identical EMV environment in order to achieve comparable levels of security. The US payments ecosystem of today is greatly different from the European of today ecosystem of the early1990s. He also observed that comparatively lower telecommunications costs in the US allow for the use of a zero floor limit for online authorization as they do in other markets where online authorization is prevalent.

2.7 Summary of Literature Review and Knowledge Gap

The literature review indicates that adoption of EMV provides capability for strengthening authentication of payment cards and prevention of card fraud. The global experience demonstrates that the adoption of EMV technology continues to be embraced. The right approach to implementation of an EMV card program is critical in reducing the overall investment of time and expense.

The adoption of EMV technology comes along with various challenges as many global players in the payment card industry strive to implement EMV technology. One of the biggest obstacles in implementing EMV is cost. POS systems capable of reading EMV cards can cost hundreds of dollars apiece. Lack of appropriate technology when installing EMV, is also a challenge that institutions face since the chip card reader failures to respond.

EMV helps mitigate card fraud at POS but it does not protect cardholder data once the payment method and consumer are validated. A layered approach to card fraud and security is the only way to truly be protected. Offering PIN change functionality at ATMs enhances the likelihood of cardholders remembering their PIN without writing it down for a fraudster to discover

The need to adopt and implement EMV in the Kenswitch network environment can prevent card fraud. The adoption and implementation of EMV on the Kenswitch network environment began in 2012 and is taking a considerable duration of time to fully implement.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter deals with the research methodology of the study. It addresses the research design, data collection and data analysis.

3.2 Research Design

This research study used the descriptive survey research design. The descriptive research design is a method of collecting information by interviewing or administering a questionnaire to a sample of individuals (Saunders et al., 2009).

3.3 Population of Study

The population of this study includes all the Kenswitch member institutions. Kenswitch currently (2015) has 35 member institutions participating in the Kenswitch network.

3.4 Data Collection

The main tool for data collection for this study was a questionnaire (See Appendix I). Each questionnaire had four sections; A, B, C and D. Section A sought demographic information, Section B captured data on the extent of adoption of EMV, Section C concerned the challenges in adoption of EMV and Section D will concerned the level of fraud experienced as a result of implementation of EMV. The target respondents were all the heads of departments of the Kenswitch member institutions responsible for operationalizing the implementation of EMV.

3.5 Data Analysis

Once the questionnaires were collected from the respondents, they were checked for errors, corrected, then coded and the data entered into a computer for analysis. Demographic data was analyzed via frequency and percentages. Data for the first objective was analyzed via means and standard deviation. Data for the second and third objective was analyzed via means and standard deviation. The results of the analysis were presented using tables, bar graphs and pie-charts.

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents a summary of finding, conclusion and recommendation. Results have been discussed in line with research objective stated earlier in chapter one. Data collected was collated and reports were produced in form of tables and figures and qualitative analysis done in prose.

4.2 Response Rate

Table 4.1 illustrates the response rate of the respondents that participated in the survey. The study targeted 35 respondents at Kenswitch Network in collecting data on adoption of EMV technology. However, out of 35 questionnaires distributed 29 respondents completely filled in and returned the questionnaires contributing to 83%. This is a reliable response rate for data analysis as Mugenda & Mugenda (2003) pointed that for generalization a response rate of 50% is adequate for analysis and reporting, 60% is good and a response rate of 70% and over is excellent. Only 17% of the respondents did not respond to the questionnaire as they were not available to fill them in at the required time. The response rate demonstrates enthusiasm of the respondents' to partake in the survey that the study sought.

Table 4.1 Response Rate

Response	**Frequency**	**Percentage (%)**
Filled in questionnaires	29	83
Un returned questionnaires	6	17
Total	**35**	**100**

4.3 Demographic Characterization of the Respondents

The analysis relied on the information from the respondents so as to classify the different results according to their knowledge and responses.

4.3.1 Working Duration

Figure 4.1 illustrates working duration of the respondents in their respective organization. From the findings, most (37%) of the respondents had worked in the organization for a period of 1-4 years, 34% had worked for a period of 5-9 years, 26% had worked for a period of more than 10 years while the rest (3%) had served in the organization for a period of less than 1 year. This implies that most of the respondents of this study had worked for an ample time within the organization, thus they were conversant of the information that the study sought pertaining to the organization.

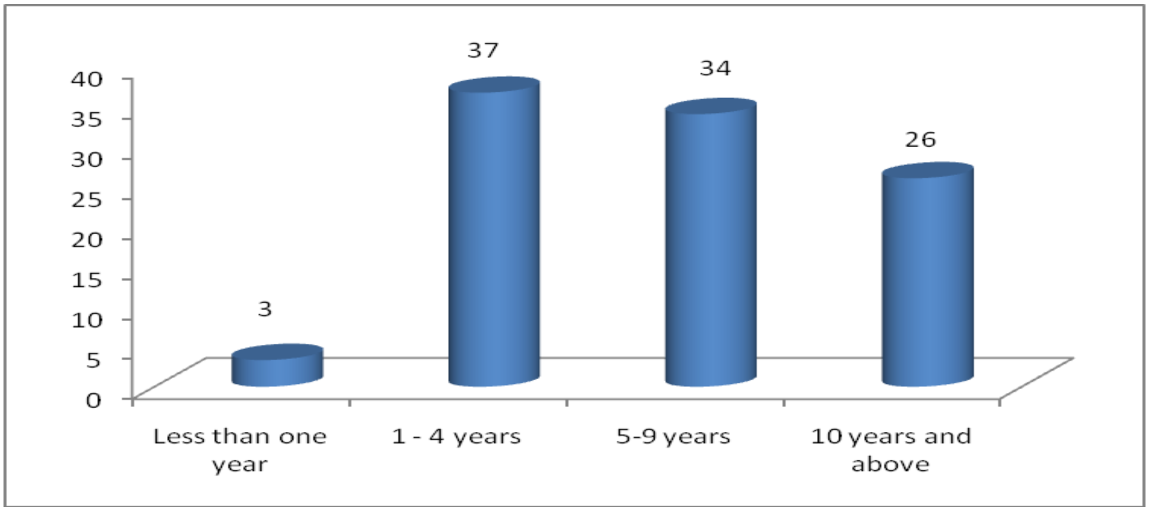

Figure 4.1 Work Duration of Respondents

4.4 Adoption of EMV

The analysis looked into the category of institutions that have adopted EMV, the number of cards issued, the extent of adoption of EMV and the challenges faced.

4.4.1 Category of the Institution

Table 4.2 shows the result of the study on the categories of the institution that have adopted EMV technology. From the findings, majority (87%) of the respondents represented commercial banks, 10% represented microfinance banks while 3% represented a mortgage lender. This implies that most of financial institutions have adopted EMV Technology.

Table 4.2 Categories of Institutions

Type of Institution	Frequency	Percent
Commercial Bank	26	87
Microfinance Bank	3	10
Mortgage Lender	1	3
Total	**30**	**100**

4.4.2 Number of Employees

Further the study also sought to establish the size of the companies in terms of number of employees. The results in of the findings are as shown in table 4.3, 53% of the organizations had between 101-300 employees, 23% had 301-500 employees, 13% of the respondents had above 700 employees, 7% of the respondents had between 501–700 employees while 3% had less than 100 employees.

Table 4.3 Size of the Company in Terms of Number of Employees

Range	Frequency	Percent
Below 100	1	3
101 – 300	16	53
301 – 500	7	23
501–700	2	7
Above700	4	13
Total	**30**	**100**

4.4.3 Number of Payment Cards Issued

The study further aimed to investigate the number of payment cards issued by the organizations. From the findings as shown in figure 4.2, 37% of the respondents indicated that their organization had issued between 1-10,000 payment cards, 30% had issued between 10,001-20,000 payment cards, 13% over 40,000, 17% had issued between 30,001 to 40,000 while 3% had issued between 20,001 to 30,000.

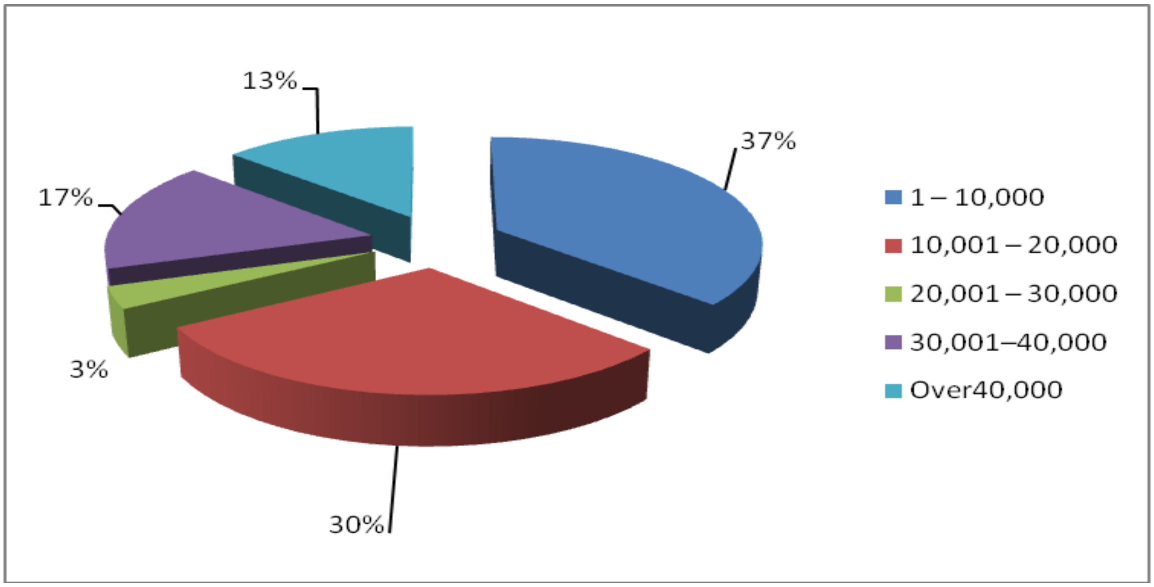

Figure 4.2 Payment Cards Issued

4.4.4 Adoption of EMV within Organizations

Table 4.4 shows the finding of the study on whether organization had adopted EMV Technology. From the findings, majority (67%) of the respondents indicated that their organization had adopted EMV technology while 33% indicated that their organization had not adopted EMV technology.

Table 4.4 Adoption of EMV Technology

EMV Adoption	Frequency	Percent
Yes	20	67
No	10	33
Total	**30**	**100**

4.4.5 Extent of Implementing EMV Technology within Organizations

Figure 4.3 summarizes results of the finding on the extent to which organizations have implemented EMV technology. Most (37%) affirmed that organization had implemented EMV to a little extent, 17% to a moderate extent, 3% to a large extent and 17% to a very large extent as shown in each case, while 27% indicated that their organization had not implemented EMV.

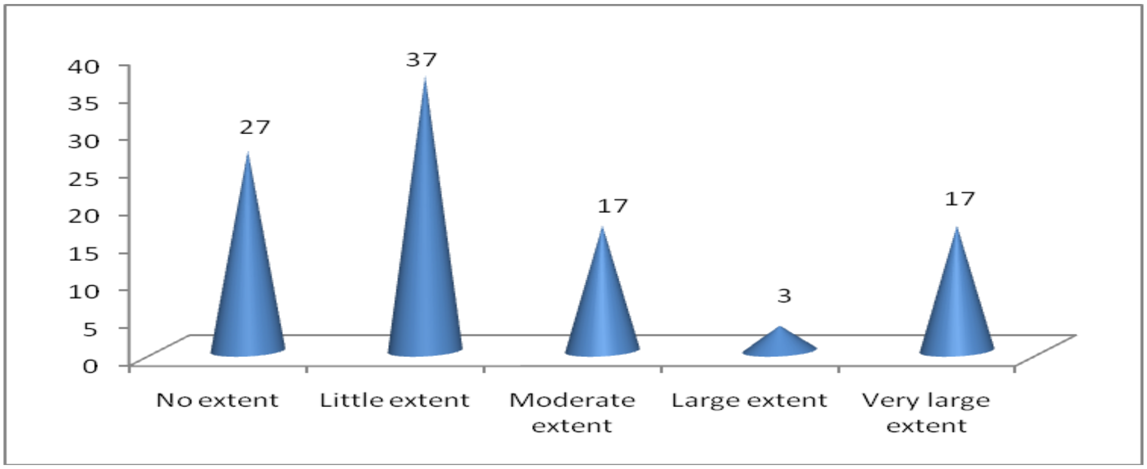

Figure 4.3 Extent to which Organizations have Implemented EMV technology

4.5 Challenges of EMV

The researcher requested the respondent to indicate the challenges the organization experience in implementing EMV. The responses were on a scale 1 – Not at all, 2 – Little extent, 3 – Moderate extent, 4 – Large extent and 5 – Very large extent. On the basis of the responses, means and standard deviations were calculated. Table 4.5 summarizes the findings of the study. Means and standard deviation are used to interpret the study findings. Their scores are interpreted according to the scale, for example a mean score of 3.97, 3.76 and 3.72 respectively indicates that devising a launch strategy, identifying and optimizing ATM/POS hardware software and making changes to the physical structure are the main challenges that organization experienced during the implementation of EMV to a large extent. Likewise, a mean score of 0.63 and 3.50 respectively explains that how to handle technological transition and determination of functionality to be offered to EMV chip card users also acts as a major challenges that organization face to a large extent when implementing EMV a indicated by mean score of 3.63 and 3.50 respectively.

On the other hand a mean score of 3.22, 3.06 and 3.02 respectively, mean that determination of testing requirements, changes to business process, changes to technical infrastructure, changes to technical infrastructure, determination of certification requirements and choice of chip application to use hinders implementation of EMV within organization to a moderate extent. From the finding, this implies that identifying and optimizing ATM/POS hardware software and making changes to the physical structure are the main challenges that organization experienced during the implementation of EMV adoption to a great extent. Technological transition and determination of functionality to be offered to EMV chip card users does not affect EMV adoption significantly.

Table 4.5 Challenges Experienced by Organization on Implementation of EMV

	Mean	**STDev**
Focus on future proofing of investment (making allowances (to the extent possible) for mobile payments, contactless interface, offline transactions, and NFC transactions)	3.53	1.11
Preparation of project timeline and identification of migration cost(establishing the project resources required, establishing the cost of migrating to EMV, board or management approval of related expenses)	3.44	1.29
Determination of training requirements (training for developers, technical support staff, customer service staff, customers)	3.38	1.16
Brand preservation (Reusing the magnetic stripe card design or new card design)	3.38	1.10
Determination of testing requirements (regression testing, stress and load testing, disaster recovery)	3.31	0.82
How to perform chip authentication (perform own authentication or use the services of a network)	3.25	1.37
Changes to technical infrastructure (ensure transaction processing hardware and/or software has capability to process EMV data)	3.22	0.91
Changes to business process (review card production process, key management, liability shift)	3.28	1.01
Determination of certification requirements (requirements of association and/or local/regional switch network)	3.06	0.91
Choice of chip application to use? (use association chip application (e.g. Visa or MasterCard) or develop proprietary ICC application)	3.03	1.12
Devising a launch strategy (how to roll-out EMV, identify location for controlled deployment of EMV device(s))	3.97	0.82
Identifying & optimizing ATM/POS hardware and software (identify existing terminal device and/or software to be upgraded or replaced)	3.76	1.20
Changes to physical structure (changes that need to be made to physical structures to accommodate new ATM devices)	3.72	1.02
How to handle technological transition (adopt big-bang or phased approach)	3.63	1.21
Determination of functionality to be offered to chip card users (same transaction set as magnetic stripe users or enhanced)	3.50	0.72

4.6 EMV Related Fraud

The researcher requested the respondent to indicate the challenges the organization experience in implementing EMV. The responses were on a scale 1 – Not at all, 2 – Little extent, 3 – Moderate extent, 4 – Large extent and 5 – Very large extent. On the basis of the responses, means and standard deviations were calculated. Table 4.5 summarizes the findings of the study. Means and standard deviation are used to interpret the study findings. Their scores are interpreted according to the scale, for example a mean score of 4.75, 4.59, 4.58 and 4.41 respectively, most of the respondents pointed that they have experienced account takeover fraud, they have experienced card skimming at retail merchant POS, they have experienced not received issued card fraud and that they have experienced lost card fraud to a great extent.

On the other hand, a mean score of 3.94, 3.88, 3.78, 3.72 and 3.69 respectively indicates that transactions conducted using stolen personal information such as ID document, driver’s license, passport, card PIN, Internet banking passwords, have experienced theft of card data, have experienced false application fraud, they have experienced card theft and that have experienced ATMs that are tampered with or damaged to a large extent. The finding implies that customers have experienced account takeover fraud, they have experienced card skimming at retail merchant POS, they have not received issued card fraud and that they have experienced lost card fraud to a great extent. Likewise, personal information such as ID document, driver’s license, passport, card PIN, Internet banking passwords, theft of card data, false application fraud, card theft and ATMs that are tampered with or damaged also forms the security challenges that customers experience to a large extent.

Table 4.6 Europay MasterCard and Visa Related Fraud

	Mean	STDev
We have experienced counterfeit card fraud	3.47	0.879
We have experienced lost card fraud	4.41	0.979
We have experienced stolen card fraud	3.16	1.019
We have experienced card skimming around ATMs	3.77	1.051
We have experienced card-not-present fraud	3.00	1.107
We have experienced identity/personal information fraud	3.94	1.045
We have experienced theft of card data	3.88	0.833
We have experienced not received issued card fraud	4.58	0.100
We have experienced an increase in card present fraud	3.78	0.099
We have experienced account takeover fraud	4.75	0.016
We have experienced card theft	3.72	1.924
We have experienced false application fraud	3.78	0.085
We have experienced ATMs that are tampered with or damaged	3.69	0.821
We have experienced card skimming at retail merchant POS	4.59	0.256

4.7 Discussion on Findings

The objective of the study was to determine the adoption of EMV technology and card fraud in the Kenswitch network environment. The results found out that some of the institutions have adopted EMV technology while others have not. The study shows that most of the commercial banks on the Kenswitch network have adopted EMV. This finding conform to Figliola (2015) that financial institutions have begun to leverage the benefits of chip-based cards and control the associated investment through a practical transitional approach to EMV migration in order to improve security in the wake of significant card compromises. This was expected to be the case following the requirement by the Kenya Bankers Association (KBA) and the Central Bank of Kenya (CBK) that the banking sector migrates to EMV technology. Likewise, Anderson (2001) indicated that adoption of EMV has broad consequences because card networks and issuers have a great degree of control over security protocols in payment authorization. The study also reveals that the institutions experienced various challenges in implementing the EMV technology. This was expected as the EMV technology was new to the market players and there was lack of experienced human resource to provide direction on implementation.

The high adoption of EMV technology seems so because of the need for the institutions to address the payment card fraud menace. It is anticipated that fraud losses due to card present fraud will reduce dramatically. Migrating to chip supports this objective and can provide a foundation on which to build additional enhancements for card-not-present fraud. The current drivers to migrate to EMV do ultimately fall back to either fraud or marketing-related drivers (Arnfield, 2006). The study reveals that card fraud is still present and this is probably so because the payments infrastructure is still going through adoption phase. The extent of the impact of adoption of EMV will be fully appreciated when all banks in the country comply with the KBA and CBK mandate. The increasing number of networks coming on board will enable debit card issuers to offer merchants (Sullivan, 2009).

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of the data findings on adoption of EMV technology and card fraud in the Kenswitch network environment. The chapter is structured into summary of findings, conclusions, recommendations and area for further research.

5.2 Summary of the Findings

The objectives of this study were to determine the extent of adoption of EMV technology in the Kenswitch network environment, to establish the challenges faced in adoption of EMV technology in the Kenswitch network environment and to establish the level of card fraud experienced as a result of EMV implementation.

From the study findings it was clear that most of the commercial banks and microfinance banks had adopted EMV technology with most of these institutions having between 101-300 employees. Most of the organizations had issued between 1-10,000 payment cards while 30% had issued between 10,001-20,000 cards this implies that organization had adopted EMV technology.

To the challenges of adopting EMV, the study established that devising a launch strategy (how to roll-out EMV, identify location for controlled deployment of EMV device(s), identifying and optimizing ATM/POS hardware and software is the main challenges organizations face in implementing EMV and changes to physical structure (changes that need to be made to physical structures to accommodate new ATM devices) are some of the challenges that affects adoption of EMV to a large extent.

On the EMV related fraud, the study established that most of the respondents strongly agreed that they have experienced account takeover fraud, they have experienced card skimming at retail merchant POS, they have experienced not received issued card fraud and that they have experienced lost card fraud.

5.3 Conclusions

The study sought to find out adoption of EMV technology and card fraud in the Kenswitch network environment. Based on the findings, the study concludes that most of the financial institutions such as commercial banks had adopted EMV where more than 20,000 EMV cards are in circulation and are accepted at most EMV terminals across the country. The study also concludes that payment card industry has lagged other developing economies in adopting more secure chip-embedded EMV cards. Most banks are opting to implement chip and signature authorization citing consumer convenience as the driver, along with concerns the overall process change could slow down transactions as retail employees and customers adjust to EMV terminals and processing. The adoption of EMV is due to realization that the card is not just about chip cards, it’s about a modern, multifaceted and highly secure payment infrastructure. It works in the brick-and-mortar world but for payments and strong authentication in non-face-to face situations such as on the internet or with phone based services.

To the challenges of adopting EMV, the study concludes Kenya financial industry and the merchant community have a once in a lifetime change to bring their payment infrastructure to a state-of-the-art level which addresses usability, functionality, security and cost requirements. EMV provides this technological basis and the learning from other market migrations offer guidance for the Kenya market participants. In order to make the migration feasible for all stakeholders it must follow a comprehensive and holistic plan that is managed rigorously.

On the EMV card and fraud, the objective verification of cardholder PIN by the chip not only reduces fraud based on lost & stolen cards, it also simplifies the merchant checkout procedure, relieves the merchants of much paperwork and reduces the complexity of exception handling and chargebacks. Although EMV allows signature or even no cardholder verification as options, e.g. for low value payments, it is strongly suggested to take advantage of the chip to verify the PIN at the POS so it does not to have to be transported across the network. Fraud rates remain fairly low in spite of massive retail payments breaches in recent years that have exposed, by most estimates, over a hundred million consumer card accounts. As such, card issuers and the card networks have historically chosen to accept and absorb fraud as a cost of doing business. But the relentlessness of retail POS breaches is exacting a significant cost above and beyond fraud losses.

5.4 Recommendations

The study recommends that organizations should embrace EMV since EMV reduces card fraud resulting from counterfeit, lost and stolen cards. EMV also provides interoperability with the global payments infrastructure – consumers with EMV chip payment cards can use their card on any EMV-compatible payment terminal. EMV technology supports enhanced cardholder verification methods and, unlike magnetic stripe cards, EMV payment cards can also be used to secure online payment transactions.

EMV chip card transactions improve security against fraud compared to magnetic stripe card transactions that rely on the cardholder's signature and visual inspection of the card to check for features such as hologram. The use of a PIN and cryptographic algorithms such as Triple DES, RSA and SHA provide authentication of the card to the processing terminal and the card issuer's host system.

Financial institutions in Kenya are one of the few markets globally that does not have a comprehensive EMV migration plan agreed upon by all stakeholders. The market participants still have to convince themselves as a whole that a market wide migration makes sense from a business case and payments system integrity perspective.

5.5 Limitations of the Study

The study focused on members of the Kenswitch Network who issue payment cards. More insight would have been garnered from the other financial institutions that are not part of the Kenswitch network. Another limitation is the sample of the study because out of the 35 Kenswitch members only 29 responded. The study would have given a better insight into the adoption of EMV if all the 35 institutions responded. Time was also limiting.

5.6 Areas of Further study

The study suggests that further research should be done on the factors affecting the use of EMV in order to give both negative and positive sides that can be reliable. The study also suggests further research to be done on the factors influencing the choice for EMV adoption among the financial institutions such as bank so as to give a reliable finings that can be used across the financial institutions.

REFERENCES

Anderson, R. (2008). *Protocols security engineering.* 2nded. New York: Wiley and Sons.

Anderson, R., Bohme, R., Clayton, R., & Moore, T. (2008).*Security economics and European policy: in managing information risk and the economics of security*. Berlin: Springer.

Arnfield, B. (2006). Selling smart cards to Canada's merchants. *Card Technology,* 6(2), 17-32.

Bidgoli, H. (2012). The introduction of biometrics security into organizations: a managerial perspective. *International Journal of Management,* 29(2), 687-695.

Bjoklund, C. (2007). *Successful cash flow management.* San Francisco: Butterworth Publishers.

Boston Retail Partners (2015). *Mobile technology: transforming the consumer experience.*

Burns, S. & Weir, G. R. S. (2008).*Trends in smartcard fraud.* Berlin: Springer.

Bustos, L. (2011). *Who needs 3D secure? Verified by Visa and MasterCard SecureCode examined.*

Ewald, D. (2015). *The adoption of EMV technology in the US*. New York: Datacard Group.

Figliola, P. M. (2015). *The EMV chip card transaction: background, status and issues for congress.* US: Congressional Research Service.

Gray, D. & Ladig, J. (2015). The implementation of EMV chip and technology to improve cyber security accelerates in the US following target corporation's data breach. *International Journal of Business Administration,* 6(2), 60-67.

Green, J. (2006). Bankcard profitability study. *Cards and Payments,* 14(2), 31-37.

Greenstein, S. & Stango, V. (2007). Introduction to card security: standards and public policy. Cambridge: Cambridge University Press.

Idowu, A. (2009). An assessment of fraud and its management in Nigeria commercial banks. *European Journal of Social Science,* 10(5), 634-649.

Katz, R. (2005). *Electronic payment in the rise in Kenya.* Nairobi: financial services.

Khu-Smith, V. & Mitchell, C. J. (2002). Using EMV cards to protect E-commerce transactions. Berlin: Springer.

Kim, Y. & Vasarhelyi, M. A. (2012). A model to detect potentially fraudulent/abnormal wires of an insurance company: an unsupervised rule-based approach. *Journal of Emerging Technologies in Accounting,* 9(1), 95-110.

Levi, A. & Kaya, C. (2001).*CONSEPP: convenient and secure electronic payment protocol based on X9.59.* California: Los Alamitos.

Mayabi, R. I. (2011). *Factors influencing use of credit cards in Kenyan commercial banks in Nairobi County, Kenya.* Unpublished MBA project. Nairobi: University of Nairobi.

Meacham, J. D. (2008). Credit card fraud: how big is the problem. *Practical E-Commerce,* 23.

Mugenda, O. M., & Mugenda, A. G. (2003). *Research Methods: Quantitative and Qualitative Approaches.* Nairobi: Act Press.

Murdoch, S. J. (2007). *Chip and PIN (EMV) relay attacks.* New York: Security Group.

Murdoch, S. J. (2007). *EMV flaws and fixes: vulnerabilities in smart card payment systems.* COSIC Seminar.

Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2010). *Chip and PIN is broken.* Cambridge: University of Cambridge.

Nilson, R. (2012) *Security issues linked to developments in French and European card payment schemes.* Annual Report, Bank of France, 67-76.

Ogony, J. E. (1999). *Factors affecting use or non-use of plastic money and attitudes towards plastic money.* Nairobi: standards chartered bank newsletter.

Ron, B. (2008). Consumer's use of debit cards: patterns and preferences and price responses. *Journal of Money, Credit and Banking,* 40(1), 149-172.

Saunders, M., Lewis, P., & Thornhill, A. (2009).*Research methods for business students.* Upper Saddle River NJ: Pearson Education.

Simiyu, J. S., Momanyi, G., Naibei, K. I. &Odondo, A. J. (2012). Credit and debit card usage and cash flow management control by customers: evidences from commercial banks customers in Kisumu City, Kenya. *Africa Research Review,* 6(4), 157-172.

Stix, H. (2004). *How do credit cards affect cash demand? Survey data evidence.* Vienna: Oestterreichiche National Bank.

Sullivan, R. (2009). *The benefits of collecting and reporting payment fraud statistics for the United States.* Kansas: Federal Reserve Bank of Kansas city.

Ward, M. (2006). EMV card payments: an update. *Information Security Report*, 11(3), 89-92.

Wiseman, A. E. (2000). *Network effects, the internet economy: access, taxes, and market structure*. Washington, DC: Brookings Institution Press.

APPENDICES

Appendix I: Questionnaire

This questionnaire has been designed for the sole purpose of collecting data on the challenges encountered in EMV implementation in the Kenswitch network environment that includes Kenswitch Limited and its member institutions. The data collected is purely for academic purpose and will be treated with utmost confidentiality.

Instructions:

i. Do not write the name of your organization anywhere on this questionnaire.

ii. Please cross [☒] where appropriate or fill in the required information in the space provided.

Section A: Demographic Information

1. What is your current position in the organization?

   ____

2. In which department of the organization are you working?

   ____

3. How long have you worked at the organization.

   a) Less than one year……... ☐

   b) 1 - 4 years ……………... ☐

   c) 5 - 9 years ……………... ☐

   d) 10 years and above ……. ☐

Section B: Adoption of EMV

4. What type of institution is your organization?

   a) Commercial Bank ……... ☐

   b) Microfinance Bank ……. ☐

   c) Mortgage Lender ……… ☐

   d) Non-Bank ……………… ☐

5. What was the asset base of your organization in Kenya shillings as at December 2014?

____

6. How many employees does your organization have?

   a) Below 100 …………..… ☐

   b) 101 – 300 ………...….… ☐

   c) 301 – 500 ……....……… ☐

   d) 501 – 700 ……………… ☐

   e) Above 700 ……..……..… ☐

7. What is the number of payment cards issued by your organization?

   a) 1 – 10,000 ………………☐

   b) 10,001 – 20,000 ……….. ☐

   c) 20,001 – 30,000 ……..… ☐

   d) 30,001 – 40,000 ……….. ☐

   e) Over 40,000 …….……... ☐

8. Has your organization adopted EMV?

   ☐ Yes ☐ No

9. To what extent has your organization implemented EMV?

   a) No extent ……………… ☐

   b) Little extent …………… ☐

   c) Moderate extent ………. ☐

   d) Large extent …………… ☐

   e) Very large extent ……… ☐

Section C: Challenges of EMV

10. Please indicate the extent to which the organization faces in each of the following challenges in implementing EMV. Use a scale of **1 to 5** (**1** – Not at all, **2** – Little extent, **3** – Moderate extent, **4** – Large extent, **5** – Very large extent)

Challenges	**Not at all**	**Little extent**	**Moderate extent**	**Large extent**	**Very large**
Identifying & optimizing ATM/POS hardware and software (identify existing terminal device and/or software to be upgraded or replaced)	□	□	□	□	□
Changes to physical structure (changes that need to be made to physical structures to accommodate new ATM devices**)**	□	□	□	□	□
Changes to technical infrastructure (ensure transaction processing hardware and/or software has capability to process EMV data)	□	□	□	□	□
Devising a launch strategy (how to roll-out EMV, identify location for controlled deployment of EMV device(s))	□	□	□	□	□
How to handle technological transition (adopt big-bang or phased approach)	□	□	□	□	□
Determination of functionality to be offered to chip card users (same transaction set as magnetic stripe users or enhanced)	□	□	□	□	□
Determination of certification requirements (requirements of association and/or local/regional switch network)	□	□	□	□	□
Determination of testing requirements (regression testing, stress and load testing, disaster recovery)	□	□	□	□	□
Determination of training requirements (training for developers, technical support staff, customer service staff, customers)	□	□	□	□	□

Challenges	**Not at all**	**Little extent**	**Moderate extent**	**Large extent**	**Very large**
Changes to business process (review card production process, key management, liability shift)	□	□	□	□	□
Preparation of project timeline and identification of migration cost (establishing the project resources required, establishing the cost of migrating to EMV, board or management approval of related expenses)	□	□	□	□	□
Focus on future proofing of investment (making allowances (to the extent possible) for mobile payments, contactless interface, offline transactions, and NFC transactions)	□	□	□	□	□
Brand preservation (Reusing the magnetic stripe card design or new card design)	□	□	□	□	□
Choice of chip application to use? (use association chip application (e.g. Visa or MasterCard) or develop proprietary ICC application)	□	□	□	□	□
How to perform chip authentication (perform own authentication or use the services of a network)	□	□	□	□	□
Others: (specify and rate accordingly)					
	□	□	□	□	□
	□	□	□	□	□

Others: (specify and rate accordingly)					
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□

Section D: Fraud

11. To what degree do you agree with each of the following statements as regarding EMV related fraud in your organization? Use a scale of **1 to 5** (**1** – Strongly disagree, **2** – Disagree, **3** – Neither agree nor disagree, **4** – Agree, **5** – Strongly agree)

Fraud	**Not at all**	**Little extent**	**Moderate extent**	**Large extent**	**Very large**
We have experienced card theft (card stolen before being issued to the customer)	□	□	□	□	□

Fraud	**Not at all**	**Little extent**	**Moderate extent**	**Large extent**	**Very large**
We have experienced theft of card data (card data in our card management system was breached)	□	□	□	□	□
We have experienced counterfeit card fraud (fraudulent card transaction conducted using illegally manufactured card that uses personal information stolen from the magnetic stripe of a genuinely issued card)	□	□	□	□	□
We have experienced card-not-present fraud (fraudulent transaction where neither the card nor the card holder is present at the ATM/point of sale location)	□	□	□	□	□
We have experienced lost card fraud (fraudulent transaction conducted on a valid issued debit or credit card after the card holder lost his or her card)	□	□	□	□	□
We have experienced stolen card fraud (fraudulent card transaction conducted on a valid issued debit or credit card stolen from a legitimate owner)	□	□	□	□	□
We have experienced false application fraud (fraudulent transactions are conducted on an account where the card was acquired by falsifying a card application)	□	□	□	□	□
We have experienced account takeover fraud (a perpetrator poses as the legitimate account holder and takes over someone's account and then uses the account for their own benefit)	□	□	□	□	□
We have experienced not received issued card fraud (fraudulent transactions from validly issued credit and debit cards that are intercepted before they reach the authentic customers)	□	□	□	□	□

Fraud	**Not at all**	**Little extent**	**Moderate extent**	**Large extent**	**Very large**
We have experienced identity/personal information fraud (fraudulent transactions conducted using stolen Personal Information e.g. ID document, driver's license, passport, card PIN, Internet banking passwords)	□	□	□	□	□
We have experienced card skimming around ATMs (perpetrators insert a skimming device in ATM to copy magnetic stripe data and a recording device to capture PIN entry sequence, or approach unsuspecting ATM users prior to or after concluding a transaction and use shoulder surfing to obtain customer's PIN)	□	□	□	□	□
We have experienced ATMs that are tampered with or damaged (a customer is confronted with an ATM that is damaged or tampered with, the perpetrator approaches the customer and uses social engineering tactics to take the customer's ATM card and escort the customer to another ATM in order to assist the customer to make a withdrawal.)	□	□	□	□	□
We have experienced card skimming at retail merchant POS (Criminals collude with staff working at retail outlets such as waiters or cashiers. The card fraud perpetrators provide business staff with hand held skimming devices and reward them for skimming customers' cards)	□	□	□	□	□
We have experienced an increase in card present fraud (card fraud has continued to increase even after implementing EMV)	□	□	□	□	□
Others: (specify and rate accordingly)					
	□	□	□	□	□

Others: (specify and rate accordingly)	**Not at all**	**Little extent**	**Moderate extent**	**Large extent**	**Very large**
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□

Thank you for your co-operation!

Appendix II: Kenswitch Member Institutions

1. ABC Bank
2. Bank of Africa Kenya
3. Chase Bank (Kenya)
4. Commercial Bank of Africa
5. Consolidated Bank of Kenya
6. Co-operative Bank of Kenya
7. Credit Bank
8. Ecobank Kenya
9. Equatorial Commercial Bank
10. Equity Bank
11. Family Bank
12. Faulu Microfinance Bank
13. Fidelity Commercial Bank
14. First Community Bank
15. Giro Commercial Bank
16. Guardian Bank
17. Gulf African Bank
18. Housing Finance
19. I&M Bank
20. Imperial Bank
21. Indo-Africa Finance
22. Jamii Bora Bank
23. Kenya Commercial Bank
24. Kenya Post Office Savings Bank
25. Kenya Women Microfinance Bank
26. K-Rep Bank
27. Middle East Bank Kenya
28. Mobile Pay
29. National Bank of Kenya
30. NIC Bank
31. Oriental Commercial Bank
32. Rafiki Microfinance Bank
33. Sumac Microfinance Bank
34. Transnational Bank
35. UBA Kenya Bank