THE EFFECT OF E-PAYMENTS ON THE OPERATIONAL RISK MANAGEMENT IN THE BANKING INDUSTRY: A CASE OF COMMERCIAL BANKS IN KENYA

BY
SIMON P.W. MWANGI

UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

SUMMER 2019
THE EFFECT OF E-PAYMENTS ON THE OPERATIONAL RISK MANAGEMENT IN THE BANKING INDUSTRY: A CASE OF COMMERCIAL BANKS IN KENYA

BY
SIMON P.W. MWANGI

A Research Project Report Submitted to the Chandaria School of Business in Partial Fulfillment of the Requirement for the Degree of Masters of Business Administration (MBA)

UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

SUMMER 2019
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University - Africa in Nairobi for academic credit.

Signed: ___________________________ Date: ___________________________

Simon P.W. Mwangi (ID No. 635700)

This research project report has been presented for examination with my approval as the appointed supervisor.

Signed: ___________________________ Date: ___________________________

Prof. Timothy C. Okech

Signed: ___________________________ Date: ___________________________

Dean, Chandaria School of Business
ABSTRACT

The general objective of the study was to examine the effect of e-payments on the operational risk management of Kenyan commercial banks. The study was guided by the following specific objectives: to examine the effect of card payments on the operational risk management of Kenyan commercial banks, to determine the effect of electronic cash on the operational risk management of Kenyan commercial banks, and to examine the effect of e-wallets on the operational risk management of Kenyan commercial banks.

This study made use of a descriptive research design. The population for this study comprised of the senior management employees of the 45 commercial banks that operated in Nairobi - Kenya who were approximately 505. For this study, the sampling frame was the list of senior management employees of the 45 Kenyan commercial banks and was obtained from the respective banks. Stratified sampling technique was used in the study to divide the population into homogeneous groups, where simple random sampling was used to select respondents. Yamane (1967) formula was used to determine the sample size for the study to 83. The primary data was collected using structured questionnaires which were piloted using 10 respondents. Collected data were analyzed using the Statistical Package for Social Sciences (SPSS). Measures of central tendencies including percentages, means, and standard deviation were used during analysis. Inferential analysis was also used in the study. Correlation analysis was used to investigate the relationship between the various causative factors of operational risks in commercial banks. Linear regressions analysis including model summary, analysis of variance (ANOVA) and regression coefficients were used to observe how each of the independent variables (card payments, electronic cash, and e-wallets) influenced operational risks in commercial banks. Final analyzed data was presented using figures and tables.

The study showed that commercial banks competed with nonbank entities to provide retail payment services, and the expansion of card services significantly increases their potential operational risk. Retail payment-related systems affected the reputation of the banks in terms of meeting regulatory and consumer protection obligations since they were responsible for risks associated with the activities of the third-party service providers they had contracted, as well as being responsible for the credit risk exposure of the services being performed.
The study revealed that the banks had developed electronic cash payment instruments which provided options for pre-funded accounts that facilitated the ability to use online auction payments. Liquidity risk in the payment system could arise from the inability of the banks to meet their obligations when they were due, and this would result in opportunity costs for the banks. Legal disputes that occurred, caused systemic risk to the banks’ payment systems, and thus, the banks had legal measures that ensured they had complied with laws and regulations pertinent to e-payment systems.

The study showed that the banks provided a digital wallet where customers made money transactions and payments, although they had outsourced these retail payment-related services to third parties to enhance their in-house services. The banks had a continuity plan in place that was capable of maintaining acceptable retail payment-related customer service levels, however, e-wallets exposed commercial banks to transaction risks from fraudulent activities, however, the banks had system measures in place that verified the authenticity of the payer and transaction information integrity.

The study concludes that the commercial banks had a wide range of plastic money that their customers made use of, and they relied on third-party service providers to conduct card payment processing. Electronic money represented liabilities on the balance sheet of the banks because the value of electronic money could diminish if the liabilities of the issuer were higher than the value of the assets. The banks had adequate due diligence processes that monitor their service providers for compliance, and they maintained effective control over customer and financial institution information accessed by these service providers.

The study recommends the commercial banks in Nairobi to ensure that they put in place strategies to manage the credit and liquidity risks that come from settlement of retail payments of these cards, by preparing themselves for issues that may arise from incomplete settlements, by setting aside funds to cater of these needs when they do arise.
ACKNOWLEDGMENT

The author would first like to thank God for His blessings granted during the entire period while undertaking this study.

He is very grateful for the invaluable support accorded by family and friends.

Thirdly, he would also like to thank his supervisor Prof. Timothy C. Okech for guidance through this research project report and certifying that he completed it in the desired manner and for his many words of encouragement and support throughout the research period.

Lastly, he offers his sincere regards and blessings to all of those who supported in all ways and manner during the time of the study.
# TABLE OF CONTENTS

STUDENT'S DECLARATION ................................................................. ii  
ABSTRACT ......................................................................................... iii  
ACKNOWLEDGMENT .......................................................................... v  
TABLE OF CONTENTS ...................................................................... vi  
LIST OF TABLES .............................................................................. viii  
LIST OF FIGURES ............................................................................ ix  
LIST OF ABBREVIATIONS .............................................................. x  

CHAPTER ONE ................................................................................... 1  
1.0 INTRODUCTION ........................................................................... 1  
1.1 Background of the Study .............................................................. 1  
1.2 Statement of the Problem ............................................................ 5  
1.3 General Objective ................................................................. 6  
1.4 Specific Objectives ...................................................................... 6  
1.5 Significance of the Study ............................................................ 6  
1.6 Scope of the Study ................................................................. 7  
1.7 Definition of the Terms ............................................................... 7  
1.8 Chapter Summary ....................................................................... 8  

CHAPTER TWO .................................................................................. 9  
2.0 LITERATURE REVIEW .............................................................. 9  
2.1 Introduction ............................................................................... 9  
2.2 Card Payments and Operational Risk Management of Commercial Banks ........................................................................................................ 9  
2.3 Electronic Cash and Operational Risk Management of Commercial Banks .............................................. 14  
2.4 E-Wallets and Operational Risk Management of Commercial Banks ......................................................... 18  
2.5 Chapter Summary ....................................................................... 22  

CHAPTER THREE ............................................................................... 24  
3.0 RESEARCH METHODOLOGY ................................................... 24  
3.1 Introduction ............................................................................... 24  
3.2 Research Design ......................................................................... 24  
3.3 Population and Sampling Design ............................................... 25
3.4 Data Collection Method........................................................................................................... 27
3.5 Research Procedures..................................................................................................................... 27
3.6 Data Analysis Methods.................................................................................................................. 29
3.7 Chapter Summary ....................................................................................................................... 29

CHAPTER FOUR ............................................................................................................................. 30

4.0 RESULTS AND FINDINGS ........................................................................................................ 30
4.1 Introduction ................................................................................................................................ 30
4.2 Response Rate and Demographic Information .......................................................................... 30
4.3 Card Payments and Operational Risk Management of Commercial Banks ..................... 34
4.4 Electronic Cash and Operational Risk Management of Commercial Banks ..................... 38
4.5 E-Wallets and Operational Risk Management of Commercial Banks .................................. 42
4.6 Chapter Summary ....................................................................................................................... 46

CHAPTER FIVE .............................................................................................................................. 47

5.0 DISCUSSIONS, CONCLUSIONS, AND RECOMMENDATIONS ........................................ 47
5.1 Introduction ................................................................................................................................ 47
5.2 Summary .................................................................................................................................... 47
5.3 Discussions ................................................................................................................................. 49
5.4 Conclusions ................................................................................................................................. 55
5.5 Recommendations ....................................................................................................................... 56

REFERENCES .................................................................................................................................. 58

APPENDICES .................................................................................................................................... 63
APPENDIX I: QUESTIONNAIRE ....................................................................................................... 63
APPENDIX II: NACOSTI RESEARCH PERMIT ............................................................................. 67
LIST OF TABLES

Table 3.1 Population Distribution ................................................................. 25
Table 3.2 Sample Size Distribution ................................................................. 27
Table 3.3 Cronbach Alpha Reliability Test Results ........................................... 28
Table 4.1 Descriptive Analysis for Card Payments & Operational Risk Management .... 35
Table 4.2 Correlations between Card Payments and Operational Risk Management ...... 36
Table 4.3 Model Summary for Card Payments and Operational Risk Management ...... 37
Table 4.4 ANOVA for Card Payments and Operational Risk Management ............. 37
Table 4.5 Coefficient for Card Payments and Operational Risk Management ............ 38
Table 4.6 Descriptive Analysis for Electronic Cash & Operational Risk Management ... 39
Table 4.7 Correlation Analysis for Electronic Cash and Operational Risk Management . 40
Table 4.8 Model Summary for Electronic Cash and Operational Risk Management ...... 41
Table 4.9 ANOVA for Electronic Cash and Operational Risk Management ............. 41
Table 4.10 Coefficient for Electronic Cash and Operational Risk Management .......... 42
Table 4.11 Descriptive Analysis for E-Wallet and Operational Risk Management ........ 43
Table 4.12 Correlation Analysis for E-Wallet and Operational Risk Management ........ 44
Table 4.13 Model Summary for E-Wallet and Operational Risk Management ............ 45
Table 4.14 ANOVA for E-Wallet and Operational Risk Management .................... 45
Table 4.15 Coefficient for E-Wallet and Operational Risk Management ................. 46
LIST OF FIGURES

Figure 4.1 Response Rate .................................................................................................................. 30
Figure 4.2 Gender of Respondents ................................................................................................. 31
Figure 4.3 Age Bracket of Respondents .......................................................................................... 31
Figure 4.4 Position of Respondents ................................................................................................ 32
Figure 4.5 Department of Respondents .......................................................................................... 32
Figure 4.6 Respondents’ Years with the Bank ............................................................................... 33
Figure 4.7 Education .......................................................................................................................... 33
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH</td>
<td>Automated Clearinghouse</td>
</tr>
<tr>
<td>ANOVA</td>
<td>Analysis of Variance</td>
</tr>
<tr>
<td>ATM</td>
<td>Automatic Teller Machine</td>
</tr>
<tr>
<td>CBA</td>
<td>Commercial Bank of Africa</td>
</tr>
<tr>
<td>CBK</td>
<td>Central Bank of Kenya</td>
</tr>
<tr>
<td>CRBs</td>
<td>Credit Reference Bureaus</td>
</tr>
<tr>
<td>EFT</td>
<td>Electronic Fund Transfer</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FDIC</td>
<td>Federal Deposit Insurance Corporation</td>
</tr>
<tr>
<td>HRMS</td>
<td>Human Resource Management Systems</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IT</td>
<td>Information and Technology</td>
</tr>
<tr>
<td>KBA</td>
<td>Kenya Bankers Association</td>
</tr>
<tr>
<td>KRAs</td>
<td>Key Risk Assessments</td>
</tr>
<tr>
<td>KRI</td>
<td>Key Risk Indicators</td>
</tr>
<tr>
<td>MFBs</td>
<td>Microfinance Banks</td>
</tr>
<tr>
<td>MRPs</td>
<td>Money Remittance Providers</td>
</tr>
<tr>
<td>ODFI</td>
<td>Originating Depository Financial Institution</td>
</tr>
<tr>
<td>ORM</td>
<td>Operational Risk Management</td>
</tr>
<tr>
<td>ORMF</td>
<td>Operational Risk Management Framework</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>POS</td>
<td>Point-of-Sale</td>
</tr>
<tr>
<td>RCSA</td>
<td>Risk and Control Self-Assessment</td>
</tr>
<tr>
<td>RDFI</td>
<td>Receiving Depository Financial Institution</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act</td>
</tr>
<tr>
<td>SPSS</td>
<td>Statistical Package for Social Sciences</td>
</tr>
<tr>
<td>SSA</td>
<td>Sub-Saharan African</td>
</tr>
<tr>
<td>SWW</td>
<td>Second World War</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USIU-A</td>
<td>United States International University – Africa</td>
</tr>
</tbody>
</table>
CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Study

The rapid development of electronic commerce or e-commerce in parallel with the widespread use of the Internet led to the emergence and development of payment mechanisms through the Internet. Payments made through the Internet grew rapidly and became an important part of the products and services offered by various institutions, especially commercial banks (Cheng, Hamid & Cheng, 2014). Electronic payments or e-payments are financial transactions made without the use of any paper documents. It is a mode of payment based on the electronic network. E-payments became one of the most critical issues in successful business and financial services (Kim, Tao, Shin & Kim, 2014).

Along with the increase of internet users, the e-payment system has been growing rapidly today, while good e-payments have a number of advantages over the traditional payment methods (Junadi & Fenrianto, 2015). E-payment provides convenience, trust and time savings, and also service providers would benefit from faster payment and better tracking of accounts (Cheng, Hamid & Cheng, 2014). Debit card, credit card, electronic cash, e-wallets are some popular e-payment instruments (Rachna & Singh, 2016).

Practically, there are two distinct types of e-payment systems: accounts-based and electronic transition-based payments (Rachna & Singh, 2016). E-payment usage, particularly card-based payment instruments not only sidesteps are popular due to the problems in carrying a large sum of money (Dzemydiene, Naujikienė, Kalinauskas & Jasiunas, 2015). The basic online payment process includes customer action, payment authentication by the operator (for example credit card’s number, ids, passwords) and payment to the seller’s account. Therefore, e-payments provide successful transaction between the parties (Vos, Marinagi, Trivellas, Eberhagen, Skourlas & Giannakopoulos, 2014). In addition to that, the bank sector participates as an issuer and acquirer. The issuer holds payer’s account and acquirer holds payee’s account and assets, and good e-payment systems ensure the effectiveness of monetary policy and facilitate smooth and stable economy (Seng, 2016).
The difference between cash transaction and an e-payment is that e-payment transaction often involves multi-parties such as payment intermediaries, authorizers, and payment clearers and settlers. At this stage, there are some negative impacts on reducing the performance of e-payment systems by increasing the risk involved with e-payment (Seng, 2016). Furthermore, Rachna & Singh (2016) mentioned that e-payment systems have received different acceptance level throughout the world, where, some methods of e-payments are highly adopted while others are relatively low. Though, both customers and service providers can benefit from the e-payment system which leads to increase national competitiveness. In the long run, the successful implementations of e-payment system depend on how the risk dimensions are perceived by consumers as well as sellers (Cheng, Hamid & Cheng, 2014).

Throughout the e-payment process, the operational risk arises from the loss of system breakdowns and incursions of system exposes (Macaulay, 2016). Failures such as disconnection, time-out of information and communications technology (ICT) service would result in disruption to normal business transactions and it would affect to the economic activities in a country (Arif & Hinti, 2014). Operational risk also arises due to a lack of understanding of security and confidentiality (AL-ma Aitah & Shatat, 2015). In addition, the operational risk arises from the potential loss due to significant insufficiencies in the system design which lead to reliability or integrity issues. It may impair the system’s ability to complete settlement, create liquidity pressures for the system as a whole, curtail the system’s ability to monitor and manage its credit exposures and result in errors, delays, or frauds in system operation (Seng, 2016). Arif & Hinti (2014) argued that the definition of operational risk is a challenge. Rachna & Singh (2016) in their review, concluded that malfunctioning Information and Technology (IT) systems and telecommunication failures, categorized as operational risk, are the usual source of the problem affecting local bank’s Automatic Teller Machine (ATM) network. The risk may be heightened if the customers are not adequately educated about the importance of security precautions (Seng, 2016).

Operational risk losses have often led to the downfall of financial institutions, with more than 100 reported losses exceeding US$100 million in recent years (Schmidt, 2016). The regulators of financial companies and banks are demanding a far greater level of insight
and awareness by directors about the risks they manage, and the effectiveness of the controls they have in place to reduce or mitigate these risks (MetricStream, 2019). Further, compliance regulations, like Basel II and Sarbanes-Oxley Act (SOX), mandate a focus on operational risks, forcing financial organizations to identify, measure, evaluate, control and manage this ubiquitous risk (Schmidt, 2016). This has led to an increased emphasis on the importance of having sound operational risk management (ORM) practice in place, especially when dealing with internal capital assessment and allocation process (MetricStream, 2019). This makes ORM one of the most complex and fastest-growing risk disciplines in financial institutions.

Under the revised recommendations of the Basel Committee on Banking Supervision (2005) transposed in European legislation (Directives 48/2006 and 49/2006) and national legislation (NBR Regulation NSC no. 24/29 of 14.12.2006), operational risk is defined as the risk of loss generated by the use of processes, systems and inadequate human resources, or who have not served properly, or external events and actions, and the operational risk includes legal risk. Macaulay (2016) states that intensification of operations for individuals and small traders, increased economic trade, the increased use of automated technologies, and the increased use of external sources and of sophisticated techniques for reducing the risk market risk have generated increasing operational risk.

The banking system in the United States (US) and banks are regulated by the Federal and state governments. The Federal Bank and other regulatory authorities like the Securities and Exchange Commission (SEC) make new and stricter regulations for Banks in the wake of the financial crisis. As per Federal Deposit Insurance Corporation (FDIC) Statistics, there are 5,542 FDIC insured institutions which include 4,833 commercial banks and 709 savings banks as of 30 June 2018 (Wall Street, 2019). The US banking system has several types of banks which are categorized as follows: savings banks, credit unions, commercial banks, savings, and loans banks and investment banks (Gupta, 2013).

Banks represent a dense network in Europe. According to the European Central Bank, as of March 2015, the European Union (EU) counted 7,233 credit institutions. They play a crucial role in business financing, whereby, 80% of European business activities are funded by banks (European Banking Federation, 2014). The banking systems of the EU
countries presents varied characteristics, including features from the Anglo-Saxon market-based system - prevalent in the US, United Kingdom (UK) and the Netherlands - and more bank-based system, prevalent in Germany and in most of continental Europe. In recent years, the demarcation lines of this common classification of financial systems have become increasingly blurred and it is nowadays generally accepted that bank intermediation and capital market funding activities are complementary (Gupta, 2013). This pluralistic structure of EU banking systems, the varied nature of corporate governance arrangements and different business models represent a strength of the EU.

The banking sector of most Sub-Saharan African (SSA) countries is underdeveloped despite series of reforms (Allen, Carletti, Cull, Qian, Senbet & Valenzuela, 2014; David, Mlachila & Moheeput, 2014). Standley (2014) observes that most banking sector depth indicators in SSA are low compared to other regions of the world. The low institutional quality in most SSA countries is a plausible reason for their lower levels of banking sector development. Anayiotos & Toroyan (2009) opine that the banks in the majority of the SSA countries conduct business within an environment characterized by weak institutional quality. A recent ranking by Krause (2016) shows that most countries in SSA rank low on institutional quality. The underdeveloped nature of banking sector of most SSA is a plausible reason for the economic backwardness in the region.

In the Kenyan scenario, the banking sector has not spared either with a number of banks incurring losses attributed to operational failures. To counter this, banks have deployed Operational Risk Management Framework (ORMF) that defines risk management techniques used to minimize operational risks or failures such as Risk and Control Self-Assessment (RCSA), loss data reporting, Key Risk Assessments (KRAs), Key Risk Indicators (KRIs) and reporting (Basel Committee on Banking Supervision, 2005).

Additionally, other government agencies such as the Central Bank of Kenya (CBK) have come in with risk management guidelines to regulate banks risk management process (CBK, 2017). However, despite all these techniques, banks have continued to experience operational risk failures resulting in huge financial losses, insolvency, and poor customer service. This is an indication that more is required in adopting quality management principles, which foster mind shift to quality performance in an organization (Basel
Committee on Banking Supervision, 2005). Hence the need to examine the effect of e-payments on the operational risk management of Kenyan commercial banks.

1.2 Statement of the Problem
Literature review lacks a critical mass of empirical evidence on the effects of e-payments on ORM for commercial banks. For instance: Yang, Hsu, Sarker & Lee (2017) examined factors enabling ORM in a financial institution. The study focused on a financial institution in Taiwan and found that the rationality of risk formalization and quantification in finance shapes the implementation of ORM in the financial sector. The study did not dwell on the effects of e-payments on ORM.

Adekunle & Taiwo (2013) whilst investigating the constraints and solutions in the implementation of an electronic payment system in the Federal Republic of Nigeria found that e-payment system was better than the old system of cash and cheques and that the government should institute standardized regulatory frameworks and policies to support the implementation of an e-payment system in Nigeria. The study did not focus on how e-payments affected ORM in banks.

Wanjohi (2014) analyzed fraud causes, fraud types, and fraud prevention and control in Kenyan banks by focusing on the Commercial Bank of Africa (CBA). The study found that opportunity and weak controls were the main contributors to fraud at CBA and that internal fraud bank staff was the predominant fraud type. It proposed the use of audits, information security, and Human Resource Management Systems (HRMS) as fraud prevention and control measures. The study did not exhaustively address the extent of card fraud and all forms of card fraud.

As observed, these studies (Yang et al., 2017; Adekunle & Taiwo, 2013; Wanjohi (2014) have failed to bring to the fore the effect of e-payments on the operational risk management of commercial banks. Given the fact that e-payments are significantly growing in the Kenyan economy, the partnership between providers and commercial banks has to be strengthened. Therefore, there was a need to understand how e-payments affected the operational risk management of Kenyan commercial banks, thus a need for this study.
1.3 General Objective
The general objective of the study was to examine the effect of e-payments on the operational risk management of Kenyan commercial banks.

1.4 Specific Objectives
The study was geared towards finding the following:

1.4.1 To examine the effect of card payments on the operational risk management of Kenyan commercial banks.
1.4.2 To determine the effect of electronic cash on the operational risk management of Kenyan commercial banks.
1.4.3 To examine the effect of e-wallets on the operational risk management of Kenyan commercial banks.

1.5 Significance of the Study
1.5.1 Management of the Kenyan Banks
The findings of the study contribute to the body of knowledge on operational risks posed by card payment models and offer recommendations for adoption by Kenyan banks to enhance e-payments in the Kenyan market. In the light of the knowledge and information that has been made available by this study, the banks may be able to see how the trends affect their total risk exposure and overall profitability and may use this information into engender appropriate strategies to mitigate the risks or lobby for new regulations that might be required in banking as a result of market dynamics.

1.5.2 Industry Regulators-Kenya Bankers Association, Central Bank of Kenya
The findings of the study may be crucial to the regulators as they provide information on prevailing market trends in card payments and hopefully guide future policy formulation for the sector. Regulators who include Kenya Bankers Association (KBA), CBK and various card associations. The Policymakers may develop appropriate policies and alternative actions based on empirical evidence and data.

1.5.3 Researchers and Academicians
The findings act as a reference point in academia for any other inquisitive study further exploring the subject of card payments in Kenya. Scholars may find the study helpful as a
resource of knowledge and insight while others may utilize it for future research on the banking industry and the card payment sector in particular.

1.6 Scope of the Study
This research focused on all commercial banks in Kenya who were members of the KBA and were based in Nairobi County. The study mainly focused on collecting management information, and data relevant from senior employees at the banks in the e-payment departments or any other senior employees with responsibilities regarding e-payments. The research was carried out as from July 2019 to September 2019.

The researcher encountered some limitations in the course of the research in terms of data access limitations where the information held by senior management was considered sensitive to the bank and was not easily available. This was mitigated by assuring the respondents of anonymity and confidentiality, together with an official letter from the institution United States International University – Africa (USIU-A), which affirmed the purpose of the study.

1.7 Definition of the Terms
1.7.1 Electronic Payments
Electronic payments or e-payments are financial transactions made without the use of any paper documents, i.e. it is a mode of payment based on electronic network (Kim et al., 2014).

1.7.2 Operational Risk
Operational risk is defined as the risk of loss generated by the use of processes, systems and inadequate human resources, or who have not served properly, or external events and actions, and the operational risk includes legal risk (Basel Committee on Banking Supervision, 2005).

1.7.3 Operational Risk Management (ORM)
ORM is defined as the preparation, identification, assessment, mitigation, and reporting of operational risks in a financial institution and its context (Basel Committee on Banking Supervision, 2005).
1.7.4 Card Payment
Card payment is the use of a card to make a payment for a sale of goods or services by the use of an electronic terminal or channel, and it involves three intermittent processes which are: authentication; authorization and settlement (Vos et al., 2014).

1.7.5 Electronic Cash
Electronic cash also known as eCash, is a digital money product that provides a way to pay for products and services without resorting to paper or coin currency, i.e. it is money kept in electronic form which allows a buyer to pay for goods and services on the internet without using a credit card (European Banking Federation, 2014).

1.7.6 E-Wallets
E-wallet also known as the digital wallet is a type of pre-paid account in which a user can store their money for any future online transaction and is protected with a password (European Banking Federation, 2014).

1.8 Chapter Summary
Chapter one gives background and statement of the problem, general and specific objectives of the study, significance of the study, as well as the scope of the study and defined the terminologies used in the study. Chapter two reviews the existing literature on e-payments and operational risks drawn from books and journals. Chapter three offers the research methodology used in the study. Chapter four presents the findings and results of the study, and chapter five gives the summary, discussion, conclusions, and recommendations.
CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter provides the literature review of the study for the effect of e-payments on the operational risk management of commercial banks. The chapter was guided by the study objectives that set to examine the effect of card payments on the operational risk management of commercial banks, to determine the effect of electronic cash on the operational risk management of commercial banks, and to examine the effect of e-wallets on the operational risk management of commercial banks.

2.2 Card Payments and Operational Risk Management of Commercial Banks

Card payments also known as plastic money has its roots in the US and its origins can be traced to the Second World War (SWW). The evolution of the various types of plastic money that are known today already begun with the introduction of the vouchers system of payment that was used during the SWW (Hellen, 2013). According to Tanai (2014), plastic money is a generic term for all types of bank cards, credit cards, debit cards, smart cards, ATM cards, and charge cards. The term is used predominantly in reference to the hard-plastic cards that are used every day in place of actual banknotes.

A contrast can be drawn between banks that have a wide range of plastic money to those that have limited or non-existent use of plastic money. Credit and debit card overdraft loans account for one of the highest rates of consumer debt growth (Michael, Bodmer & LeMasters, 2009). Credit card and debit card lending is based on pre-authorized lines of credit that can be taken down as the consumers take cash or make purchases from merchants who accept credit cards (Hellen, 2013). Plastic money may be held responsible for inflation, the huge increase in personal indebtedness, the destruction of the basic virtues of thrift spending and the growth of the acquisitive society (Tanai, 2014).

Usually, card payments link to an existing account relationship with a financial institution for both payee and payer. Consumers may use credit, debit, or stored-value cards to initiate retail payments in face-to-face or remote transactions. The payee receives funds after the payment clears, but consumers actually pay before the transaction on a stored-value card, at the same time of the transaction for an online debit card, and after a
transaction on a credit card (Michael et al., 2009). Both credit and signature-based debit card transactions are processed in batch mode at the point-of-Sale (POS), and settlement is delayed until the batches are processed at the end of the day. Personal identification number (PIN)-based debit card transactions, although processed in real-time at the POS, typically settle at the end of the day using the Automated Clearinghouse (ACH) (Hohl, 2016).

Financial institutions rely on third-party service providers to conduct card payment processing. Third-party processors provide a range of retail payment-related services, including card issuing services, merchant services, account maintenance, and authorization services, transaction routing and gateway services, off-line debit processing services, and clearing and settlement services (ISACA, 2015). Although merchant acquiring financial institutions may use third parties to perform many acquiring activities, the acquiring financial institution is responsible for all third-party processor and merchant activity (Hellen, 2013).

2.2.1 Strategic Risk

Strategic risk is the risk associated with the financial institution’s future business plans and strategies. This risk category includes plans for entering new business lines, expanding existing services through mergers and acquisitions, and enhancing infrastructure (for example, physical plant and equipment and information technology and networking) (Tanai, 2014). Financial institutions also increasingly compete with nonbank entities to provide retail payment services. This competition benefits the consumer through enhanced product offerings at a lower cost (Cheng et al., 2014). Conversely, it places additional pressure on financial institutions to protect profitability through the development of new products and services while managing additional marketing, research, and development costs (Macaulay, 2016).

Strategic plans that include a significant market expansion or the addition of new products may expose financial institutions to increased risk. For example, expanding Internet banking services to include electronic bill presentment and payment services, expanding existing bankcard issuing programs, or entering the merchant bankcard processing business significantly increase the potential risk to the financial institution.
(Urban, 2016). Strategic plans should demonstrate that management has assessed the risks and documented the institution’s program to mitigate them. Strategic plans should address the institution’s capability to provide the service (Cheng et al., 2014).

Many retail payment system services are transaction-intensive and priced competitively based on volume. Financial institutions providing large-scale bankcard issuing and merchant services, as well as other transaction-intensive retail services, should maintain a competitive operating environment (Urban, 2016). This often requires significant investments in information technology. Strategic plans should reflect these investments and link business-line goals and objectives with planned information technology enhancements (Macaulay, 2016).

2.2.2 Reputation Risk
Reputation risk is the risk that negative publicity regarding an institution’s business practices will lead to a loss of revenue or litigation. For retail payment-related systems, reputation risk is linked with customer expectations regarding the delivery of retail payment services, and whether the institution is meeting its regulatory and consumer protection obligations relating to those services (Hohl, 2016).

An institution’s reputation, particularly the trust afforded it by customers and counterparties can be irrevocably tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly. In addition, financial institutions are responsible for risks associated with the activities of third-party service providers with which they contract. For example, deficiencies in security and privacy policies that result in the release of customer information by a service provider may result in reputation damage (ENISA, 2016).

2.2.3 Credit Risk

2.2.3.1 Credit Risk
Credit risk is the risk that a party will not settle an obligation for full value. Each retail payment instrument has a specific settlement process that depends on the entities involved (Gupta, 2013). Multiple financial institutions, third-party entities, as well as the payer and payee are involved with creating, processing, and settling the transaction. If a financial
institution uses a third-party service provider, it is responsible for the credit risk exposure for the services performed. Financial institutions should have procedures in place to manage the credit risk of third parties using their accounts to settle transactions (Vos et al., 2014).

Non-cash retail payments, including the inter-institution settlement of cash withdrawals through shared ATMs, are usually settled on a deferred basis. With the deferred settlement, there is a risk that the paying institution or some intermediate party will fail before inter-institution settlement occurs. This deferred settlement, rather than real-time settlement, mitigates but does not eliminate the credit risk (ENISA, 2016).

When an institution supplies funds, it usually does not submit payment for settlement unless the payer’s financial institution verifies that funds are available in the payer’s account. Otherwise, there is credit risk exposure (Hohl, 2016). When an institution receives funds in a retail payment transaction, it may suffer credit risk from granting funds availability for account transfers not properly authorized. The ACH established rules requires each Originating Depository Financial Institution (ODFI) to conduct appropriate creditworthiness monitoring, establish exposure limits, and periodically review the limits applicable to specific customers (Urban, 2016).

2.2.3.2 Returns
Returns are another source of credit risk. Checks and direct debit transfers can be returned if the payer’s institution chooses not to honor the presentment because of insufficient funds, forgery, fraud, or other payment irregularities. The return time frames vary for different payment instruments (Vos et al., 2014). For an ACH debit, the ODFI grants funds availability to the originator on settlement day. The credit exposure exists until the Receiving Depository Financial Institution (RDFI) can no longer return the ACH debit. If not properly authorized, the return time frame rules can extend to 60 days from the settlement date (Urban, 2016).

Bankcards have specific procedures for chargebacks, which are amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account (Gupta, 2013). The acquiring financial institution relies on the creditworthiness of the merchant, but if
the merchant declares bankruptcy, commits fraud, or is otherwise unable to pay its chargebacks, the acquiring financial institution must pay the issuing financial institution (Vos et al., 2014).

2.2.3.3 Settlement Lags

The settlement of retail payment transactions, i.e., the transfer of funds between the parties, discharges the payment obligation. The risk that settlement of retail payment transactions will not take place as expected can result in both credit and liquidity risks (Macaulay, 2016). Financial institutions should understand and manage credit and liquidity risks related to the settlement of retail payments. This should include preparing for potential credit and liquidity issues resulting from the incomplete settlement or operational problems (Cheng et al., 2014).

Settlement lags occur when financial institutions, due to failure or the inability to fund their obligations, do not settle their obligations when due. Settlement lags result in credit risk until final settlement occurs (Hellen, 2013). Any payment activity undertaken on the basis of “unsettled” payment messages remains conditional, resulting in risk. Settlement lags may also result in liquidity risk. Until a settlement is completed, a financial institution is not certain what funds it will receive through the payment system. As a result, it may not be sure whether its liquidity is adequate (ISACA, 2015). If an institution overestimates the funds it will receive when settlement takes place, it may face a shortfall. If the shortfall occurs close to the end of the day, an institution could have significant difficulty finding an alternative liquidity source (ENISA, 2016).

Financial institutions often allow their corporate customers to incur intraday or “daylight” overdrafts. In principle, an institution engaging in this practice is extending credit to its customer. In most cases, the overdraft is eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day (Tanai, 2014). Daylight overdrafts constitute an extension of credit - no matter how long they remain unpaid. An institution’s credit policies should include provisions for approving and monitoring daylight overdraft lines to customers (Macaulay, 2016).
2.3 Electronic Cash and Operational Risk Management of Commercial Banks

Electronic cash also known as eCash, is a digital money product that provides a way to pay for products and services without resorting to paper or coin currency, i.e. it is money kept in electronic form which allows a buyer to pay for goods and services on the internet without using a credit card (European Banking Federation, 2014). According to Elly (2012), electronic cash/ money is the money balance recorded electronically on a “stored-value” card. These cards, “smart cards,” have a microprocessor embedded which can be loaded with a monetary value. Another form of electronic money is network money, “software that allows the transfer of value on computer networks, particularly the internet. Like a traveler’s check, a digital money balance is a floating claim on a private bank or other financial institution that is not linked to any particular account (Berentsen, 2014). This money is issued by both public and private institutions worldwide and is raising a concern about the future ability of central banks to set money supply targets (Tak, 2014).

Financial institutions and retailers have also developed electronic cash payment instruments. Individuals can transfer electronic cash value to other individuals or businesses (Dzemydiene et al., 2015). Most electronic cash applications exist on the Internet. Consumers can use the cash payment instruments for purchases at retailers’ Web sites or they can transfer cash to other individuals through e-mail. Pre-funded accounts consumers may use for on-line auction payments or with participating retailers are among the most recent applications (Kim et al., 2014). Individuals use a credit card or signature-based debit card number to refund the Web certificate or electronic account, and recipients redeem the value with the issuer. There are few existing markets for electronic cash payment instruments, and merchant acceptance and consumer use are generally low (Isabelle, Traore & Everaere, 2015).

2.3.1 Consumer and Merchant Risk

In principle, in a market economy, it is the task of the creditor to assess the creditworthiness of his/her debtor (Kasiyanto, 2016). As regards credit institutions, most customers cannot assess the quality of these institutions due to the asymmetric availability of information and a lack of understanding of the technical security features of the payment systems they offer. This is one of the reasons why a prudential supervisory framework is applied to credit institutions (Berentsen, 2014).
Electronic money represents liabilities on the balance sheet of the issuer, created against the provision by customers of cash or scriptural money, which are payable at par to the entities accepting electronic money as payment (the merchants). Therefore, these liabilities represent an asset for the customers which can be used for payment purposes (Elly, 2012). As with deposits, prepayments made to the issuers of electronic money are not left idle but are invested in order to obtain asset returns. As is the case with the value of bank deposits, the value of electronic money could diminish, or even disappear, if the liabilities of the issuer are higher than the value of the assets (Kasiyanto, 2016). Thus, the financial integrity of the issuer would be jeopardized if the investment policy it pursued was not adequately sound. The risks for the issuer are more likely to be triggered by liquidity strains (if assets are liquidated with heavy losses) than by credit risk. Since the issuance of electronic money amounts in economic terms to deposit-taking, the application of a prudential supervisory framework to electronic money issuers would also be justified (Isabelle et al., 2015).

In addition, central banks could be subject to moral hazard problems if economic agents were wrong to assume that they might support issuers of electronic money financially in order to protect the public’s confidence in the currency (Berentsen, 2014). It is also possible that some customers will not see clear differences between the protection they receive with traditional bank deposits and the protection they will receive (if any) with prepayments to electronic money issuers (Dzemydiene et al., 2015).

2.3.2 Liquidity Risk

Liquidity risk is the current and potential risk to earnings or capital arising from a financial institution’s inability to meet its obligations when they come due without incurring unacceptable losses (Parshotam & Gulati, 2015). Liquidity risk related to payment systems is the risk that the financial institution cannot settle an obligation for the full value when it is due but only at some unspecified time in the future (Urban, 2016).

Liquidity problems can result in opportunity costs, defaults on other obligations, or costs associated with obtaining the funds from another source for some period of time. In addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period (Parshotam & Gulati, 2015).
2.3.3 Counterfeit and Fraud Risk

The inadequate management of operational risk and a lack of technical security make an electronic money scheme vulnerable to counterfeit and fraud. If counterfeit money were able to be introduced into the scheme, it could lead to an increase in claims against the issuer which would no longer be backed by the available assets (Rachna & Singh, 2016). Thus, the financial integrity of the issuer would be threatened. This vulnerability might be greater for software-based money schemes, which, in general, rely mainly on cryptography, whereas card-based schemes can also use the protection of a tamper-resistant chip (Isabelle et al., 2015).

In the fast-developing technical world, the risk of counterfeit and fraud can hardly be excluded. Therefore, if a scheme lacks means detecting counterfeits and fraud, it will not be able to take appropriate countermeasures (Elly, 2012). This problem is less significant for schemes in which electronic money transactions are processed in a way similar to that in which sight deposits are handled by credit institutions. If the scheme is based on a book-entry principle, according to which each loading and, in the end, each payment operation triggers a debit or credit position in the account of the issuer(s), criminal attacks can be detected at an early stage and countermeasures can be taken (Janson, 2014).

By contrast, if electronic money units are transferable from customer to customer without these transactions being subsequently recorded by the issuer or a clearing system, the systems might entail a higher degree of operational risk, since it is not possible to have a complete audit trail of transactions at all times, and the source and exact quantity of any counterfeit electronic money or false value triggered by security deficiencies might not be known (Berentsen, 2014). Even those schemes which do not permit customer-to-customer transactions may truncate or amalgamate the data transferred to the issuer or clearing system, which would result in an incomplete audit trail (Janson, 2014).

Another area of criminal abuse associated with electronic money schemes relates to money laundering and tax evasion. Should electronic money schemes offer the possibility of executing anonymous transfers of large sums of money, they could be increasingly used for such criminal purposes (Tak, 2014). In fact, it cannot be excluded that market forces alone might foster the development of those schemes whose features are more
“attractive” for money laundering purposes (such as anonymity of transactions, the possibility of making customer-to-customer transactions, the impossibility of tracing individual transactions) (Macaulay, 2016).

2.3.4 Legal Risk

Legal risk is the risk arising from failure to comply with statutory or regulatory obligations. Legal risk also arises if the rights and obligations of parties involved in payment are subject to considerable uncertainty, for example, if a payment participant declares bankruptcy (Goczek & Witkowski, 2016). Legal disputes that delay or prevent the resolution of payment settlement can cause credit, liquidity, or reputation risks at individual institutions (Tee & Ong, 2016). Though unlikely, these disputes can also potentially cause systemic risk to the payments system. Such legal problems are more likely to result from the failure of a financial institution than the default of an individual payer. Individual default is more prevalent and has often been addressed in existing law (Tak, 2014).

Legal risk can result from a financial institution’s failure to comply with the bylaws and contractual agreements established with the bankcard associations, clearinghouses, and other counterparties with which it participates in processing, clearing, and settling retail payment transactions. Legal risk also arises from noncompliance with existing consumer protection statutes, regulations, and case law governing retail payment transactions (Nguyen & Nguyen, 2016).

Legal measures should ensure compliance with specific laws and regulations pertinent to retail payment systems. They should also ensure compliance with general consumer protection rules that allocate responsibility and establish the minimum procedural measures that must be fulfilled before shifting the responsibility to another party (Goczek & Witkowski, 2016). Contractual terms may further define responsibilities within the legal framework, and contracts between financial institutions, customers, and third-party service providers may further integrate risk-sharing responsibilities applicable to payments made through a specific clearing or settlement arrangement (Tee & Ong, 2016; Nguyen & Nguyen, 2016).
The bylaws and agreements between clearinghouse participants and bankcard associations include specific responsibilities and liabilities (Tak, 2014). Financial institutions should assess the risks of agreeing to such bylaws and agreements. Financial institutions and third-party service providers that do not comply with the appropriate bylaws and agreements of bankcard associations and clearinghouses can be fined or lose their memberships (Janson, 2014).

2.4 E-Wallets and Operational Risk Management of Commercial Banks

E-wallet also known as a digital wallet is a type of pre-paid account in which a user can store their money for any future online transaction and is protected with a password (European Banking Federation, 2014). It is a virtual wallet in a smartphone, in which money is stored in the form of virtual money. So overall, it is a digital wallet out of which one can make money transactions and payments. It has a combination of software and hardware on certain devices and all seek to replace the use of traditional credit/debit cards with mobile phones (Yang et al., 2017). One can pay money using smartphone applications, text messages, social media or websites.

In this setup, agents are playing the main role. These agents are application providers, mobile network operators, mobile device manufacturers, terminal providers, and third-party agents. The client connects with a mobile network using an application provider. Application provider contains credit/debit cards details, mobile balance, bank account details for payment transaction (Parshotam & Gulati, 2015). Mobile network operators provide services for making purchases, transfer money, pay bills, etc. Other common services include third party payments, online services access, etc. Some mobile device manufacturers traditionally produce mobile phones with payment functions (Hohl, 2016). Third-party agents acting as retail outlets to deal directly with a customer for reducing services cost. Third-party agents have sub-agents by the permission of law. Cash merchant agents provide cash-in and cash-out facility but not allows other banking transactions such as account open/close, loan, check, etc (Urban, 2016).

2.4.1 Vendor and Third-Party Management

Some financial institutions rely on third-party service providers and other financial institutions to provide retail payment system products and services to their customers.
Many retail payment services are directly related to core processing financial institution operations (e.g., accessing demand deposit accounts through the use of financial institution-issued bankcards) and maybe run in-house through the use of purchased turnkey systems (Berentsen, 2014). However, institutions contract many retail payment-related services to third parties either to enhance the services performed in-house or to offer new retail payment services that are otherwise not cost-effective (Parshotam & Gulati, 2015).

To ensure retail payment operations are conducted appropriately, financial institutions should have appropriate contract provisions and adequate due diligence processes. They should also monitor service providers for compliance (Yaokumah, Kumah & Okai, 2017). Effective monitoring should include a review of select retail payment transaction items to ensure they are accurate and processed timely (Hohl, 2016). The integrity and accuracy of retail payment transactions posted to customer accounts depend on the use of proper control procedures throughout all phases of processing, including outsourced functions (Parshotam & Gulati, 2015).

Regardless of whether the financial institution’s control procedures are manual or automated, internal controls should address the areas of transaction initiation, data entry, computer processing, and distribution of output reports (Janson, 2014). These control considerations apply to process checks as well as an electronic bank card, debit card, and ACH transactions. The financial institution must also maintain effective control over service provider access to customer and financial institution information consistent with existing legal frameworks (Goczek & Witkowski, 2016).

**2.4.2 Business Continuity Risk**

For financial institutions offering basic retail payment products and services (e.g., bankcard issuance, check item processing, branch ATM access, and Internet banking services), business continuity plans should include appropriate recovery targets for each retail product (Francisco, Francisco & Juan, 2015). The recovery targets should consider the reliance on any third-party vendors in meeting their objectives. Vendor management programs should include provisions for the disruption and restoration of service at service
providers, including the consideration of service provider test plans (Rachna & Singh, 2016).

For financial institutions and service providers with complex retail payment operations, business continuity plans should enable restoration of service within time frames that are reasonable for internal business units as well as other dependent financial institutions and counterparties (Kasiyanto, 2016). Financial institutions providing significant card issuing, merchant processing, Electronic Fund Transfer (EFT)/POS, ACH, and retail payment-related Internet banking services should also test these plans periodically with customer financial institutions and counterparties to ensure plans are sufficient (Tee & Ong, 2016).

Effective business continuity planning is an important component in managing operational risk. Financial institutions and technology service providers should develop, implement, and test appropriate disaster recovery and business continuity plans capable of maintaining acceptable retail payment-related customer service levels (Francisco et al., 2015). Business continuity plans should be based on business impact analyses and the relative importance of retail payment system products and services to the financial institution (Kasiyanto, 2016).

2.4.3 Information Security

Financial institutions must implement the appropriate physical and logical security controls to ensure retail payment system transactions are processed, cleared, and settled in an accurate, timely, and reliable manner (Isabelle et al., 2015). Retail payment systems contain confidential customer information subject to security guidelines. The board and management are responsible for protecting the confidentiality, integrity, and availability of these systems and data (ENISA, 2016). The privacy risk combined with the fund transfer capability should cause these systems to rank high in all institutions’ information security risk assessments. Those risk assessments should consider physical and logical security controls for the origination, approval, transmission, and storage of retail payment systems transactions (ISACA, 2015).

Physical controls should limit access to those staff assigned responsibility for supporting the operations and business line centers processing retail payment and accounting
transactions (Junadi & Fenrianto, 2015). Physical controls should also provide for the ability to monitor and document access to these facilities.

Institution management should assign appropriate logical access controls to staff responsible for retail payment-related services and should base access rights on the need to separate the duties of personnel responsible for originating, approving, and processing the transactions (Zvelo, 2016). Appropriate identification and authentication techniques include requiring unique authenticators for each staff member with strong password requirements if the institution has not implemented more robust authentication techniques (Francisco et al., 2015).

Logical access controls should restrict access on a need-to-know basis and assign access to retail payment applications and data based on functional job duties and requirements. Logical access control should also protect network access (Krause, 2016). An institution’s risk assessment should require it to protect retail payment systems from unauthorized access through appropriate network configuration, firewalls, or intrusion detection (Tee & Ong, 2016). The assessment should review the security of all third-party service providers as well. Some institutions accomplish this by isolating all payment-related applications and systems from other production applications (Goczek & Witkowski, 2016).

A critical element in ensuring retail payment systems integrity is appropriately identifying and authenticating retail payment system customers. Transaction authorization (e.g., the approval of a funds transfers or guarantee of funds) is an essential precondition leading to the interbank transfer of funds (Junadi & Fenrianto, 2015). Financial institutions should establish an adequate internal control environment for the issuance of bank cards and related PIN. These controls should minimize bankcard processing errors and fraud and protect the confidentiality of customer and institution information (Yang et al., 2017).

2.4.4 Transaction Risk
Transaction risk is the risk of incurring a financial loss due to human or technical errors and fraud. Transaction risk can arise from the failure to follow or complete one or more steps in the prescribed authorization process (Hellen, 2013). Transaction risk includes the risks associated with the failure of communications, the breakdown of data transport or
processing, internal control system deficiencies, human errors, or management failure (Hoofnagle, Urban & Li, 2014). As a result, the financial institution could experience delays or disruptions in processing, clearing, and settling retail payment transactions, that could lead to credit and liquidity problems at other financial institutions (Urban, 2016).

Transaction risk can also arise from fraud. A financial institution’s exposure to transaction risk from fraud is the risk that a wrongful or criminal deception will lead to a financial loss for one of the parties involved (Rachna & Singh, 2016). Currency and checks are more vulnerable to loss or direct theft, whereas fraud is the primary concern in bankcard payment transactions (Hoofnagle et al., 2014). Fraud is a significant concern for ACH, especially one-time ACH debit transactions. The continuing growth of check-to-ACH conversion presents many new fraud risks (Isabelle et al., 2015).

Newer retail payment mechanisms, particularly using the Internet, are also subject to fraud risk. The creation of fraudulent electronic transactions could lead to financial losses if fraudulent balances are successfully exchanged for a readily transferable form of money, such as currency, or other assets (Janson, 2014). Operational risk controls should include information system, procedural, administrative, and legal measures to prevent or limit financial loss as a result of transaction risk (Elly, 2012).

System measures include monetary and time limits (per transaction, per payment instrument, per client), and personal authentication and encryption techniques to ensure the authenticity of the payer and transaction information integrity (Berentsen, 2014). Additional controls include the use of certified tamper-resistant equipment (e.g., EFT/POS terminals), logical access controls to verify transactions, on-line verification of account balances, logging of all transactions and attempts to make a transaction, and the use of serial numbers and check digits (Hoofnagle et al., 2014).

2.5 Chapter Summary
This chapter has provided a literature review on the effect of e-payments on the operational risk management of commercial banks. The chapter was guided by the study objectives that set to examine the effect of card payments on the operational risk management of commercial banks, to determine the effect of electronic cash on the
operational risk management of commercial banks, and to examine the effect of e-wallets on the operational risk management of commercial banks. The next chapter focuses on the study’s research methodology.
CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction
This section forms chapter three of the study, and it constructs a framework on how the study was performed. It outlines the type of research design used, the population of the study, the sampling techniques, data collection method, research procedure, and data analysis method.

3.2. Research Design
Research design constitutes the blueprint for the collection, measurement, and analysis of data and it also defines research design as the plan and structure of investigation so conceived as to obtain answers to research questions (Maxwell, 2012. Kothari (2014) opines that a research design constitutes decisions taken by a researcher regarding what, where, by how much and by what means concerning an inquiry or a research study. This study made use of a descriptive research design.

A descriptive survey research design was used for this study since the research was structured employing the use of standardized data, interviews, and questionnaire as measurement tools. Saunders, Lewis, & Thornhill (2013) posit that the survey strategy is associated with a deductive approach and allows for the collection of large data from a sizable population. It is also generally perceived as authoritative and easy to comprehend. The purpose of descriptive research is to portray an accurate profile of the phenomena of interest (Garson, 2012).

For practical purposes in this study, a descriptive approach was employed to determine the relationship between e-payments and operational risk management of commercial banks. The dependent variable for the study was operational risk management while the independent variable(s) of the study were e-payment factors (card payments, electronic cash, and e-wallets). Descriptive design was used because it allowed for the use of a survey study, as well as its focus, is the determination of the relationship between the study constructs, in this case, the relationship between e-payments and operational risk management of commercial banks.
3.3 Population and Sampling Design

3.3.1 Population
The research population describes the total collection of elements of interest from which data can be gathered and about which inferences can be made (Cooper & Schindler, 2014). That said, a population can include people, events, cases, records or institutions that meet the criteria for data collection (Saunders et al, 2013). The population for this study comprised of the senior management employees of the 45 commercial banks that operated in Nairobi - Kenya who were approximately 505 as indicated in Table 3.1.

Table 3.1 Population Distribution

<table>
<thead>
<tr>
<th>Position</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top-Level Managers</td>
<td>98</td>
<td>19.4</td>
</tr>
<tr>
<td>Middle-Level Managers</td>
<td>149</td>
<td>29.5</td>
</tr>
<tr>
<td>Low-Level Managers</td>
<td>258</td>
<td>51.1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>505</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Source: Commercial Bank Staff List (2019)

3.3.2 Sampling Design
Sampling design describes the process by which some elements of the population are selected for study so that conclusions can be drawn about the entire population (Cooper & Schindler, 2014). The sample design for this research comprised of the sampling frame, sampling technique, and the study’s sample size.

3.3.2.1 Sampling Frame
According to Saunders et al. (2013), the sampling frame consists of the complete list of all population elements from which data is collected or a probability sample is drawn. This may comprise the entire population or a part of it. For this study, the sampling frame was the list of senior management employees of the 45 Kenyan commercial banks and was obtained from the respective banks.

3.3.2.2 Sampling Technique
The sampling technique is the method by which a group of people, events, cases, institutions, or behavior necessary to perform a study is selected (Cooper & Schindler,
Stratified sampling technique was used in the study. Stratified sampling technique is a non-probability sampling technique that comprises of the division of the population into different groups that are known as strata that are homogeneous in nature. Then the researcher applies the selection of individual population units from each sub-divided group/segment according to the research purpose (Cooper & Schindler, 2014). The study made use of stratified sampling to certify that the sample size of the study was evenly distributed across the study strata. The population of the study was divided into three categories/strata: top-level managers, middle-level managers, and low-level managers. After which, simple random sampling was employed to select the population units from each stratum.

### 3.3.2.3 Sample Size

Garson (2012) terms a sample size to signify a subset of sampling units from a given population. The sample size is a representative portion of the sample is chosen for examination and the findings are interpreted to reflect the characteristics of the entire population (Cooper & Schindler, 2014). The Yamane (1967) formula was used to determine the sample size for the study. This formula was used because it enabled the researcher to formulate a sample size that was logically established and accounted for the margin of errors involved with the sample size selection of 83 respondents. The formula that was applied was as follows and the sample size distribution was as shown in Table 3.2:

\[
n = \frac{N}{1 + N(e)^2}
\]

Where:
- \(n\) = Selected Sample Size
- \(N\) = Total Population
- \(e\) = Error Value (0.1)

Thus:

\[
n = \frac{505}{1 + 505(0.1)^2}
\]

\[
n = \frac{505}{6.05}
\]

\[
n = 83
\]
Table 3.2 Sample Size Distribution

<table>
<thead>
<tr>
<th>Position</th>
<th>Number</th>
<th>Percentage</th>
<th>Sample Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top-Level Managers</td>
<td>98</td>
<td>19.3</td>
<td>16</td>
</tr>
<tr>
<td>Middle-Level Managers</td>
<td>149</td>
<td>30.1</td>
<td>25</td>
</tr>
<tr>
<td>Low-Level Managers</td>
<td>258</td>
<td>50.6</td>
<td>42</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>505</strong></td>
<td><strong>100</strong></td>
<td><strong>83</strong></td>
</tr>
</tbody>
</table>

3.4 Data Collection Method

The primary data was collected using structured questionnaires. Harris & Brown (2010) assert that the use of questionnaires is suitable since the responses are gathered in a standardized manner, and the method is objective. Commonly, it is quicker to collect information using questionnaires with the potential to gather data from a large portion of a group within a short span of time.

The questionnaire format for the study had four sections. The purpose of the first section was to provide general information deemed relevant for this study. The second section sought to examine the effect of card payments on commercial banks’ operational risks. The third section sought to identify the effect of electronic cash on commercial banks’ operational risks. The fourth section examined the effect of e-wallets on commercial banks’ operational risks.

The questionnaire made use of closed-ended questions. The closed-ended questions were in the form of a Likert scale that guided the respondents to select co-opted options based on their level agreement on a five-point summated rating scale denoted as 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, and 5=Strongly Agree. The strength of the respondents’ attitude was reflected in the assigned score, individual scores were then totaled for an overall measure of the responses whether favorable or unfavorable towards the object of observation.

3.5 Research Procedures

The questionnaire was developed with the aim of collecting data that facilitated response to the effect of e-payments on the operational risk of commercial banks in Kenya. The questionnaire was piloted before the actual administration of the instrument to the target
population. This was conducted with the aim of refining the instrument and testing its validity and reliability. The pilot test involved the researcher distributing the questionnaire to 10 respondents and collecting their feedback on the instrument.

Reliability was tested using the Cronbach Alpha test using the Statistical Package for Social Sciences (SPSS). According to Cooper & Schindler (2014), the required threshold for questionnaire items that have 6 and above items is >0.7 while for those that have 5 and below is >0.5. Since the questionnaire contained 10 items per section, thus, the reliability threshold for the study’s questionnaire was >0.7. Table 3.3 provides the results of the questionnaire. The table indicates that all questionnaire items had coefficients of 0.740, 0.750, and 0.813 for card payments, electronic cash, and e-wallets effect on operational risk management of commercial banks respectively. These questionnaire items were all >0.7, meaning the instrument was reliable for data collection for the study.

<table>
<thead>
<tr>
<th>Table 3.3 Cronbach Alpha Reliability Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Items</td>
</tr>
<tr>
<td>Card Payments and Operational Risk Management of Commercial Banks</td>
</tr>
<tr>
<td>Electronic Cash and Operational Risk Management of Commercial Banks</td>
</tr>
<tr>
<td>E-Wallets and Operational Risk Management of Commercial Banks</td>
</tr>
</tbody>
</table>

Ethical considerations were employed in the study. The first ethical consideration was to seek permission for the study. The researcher got in touch with managers of the commercial banks and sought their permission to conduct research before providing them with the questionnaires. The second ethical consideration required the study respondents to remain anonymous. Respondents were not required to give their personal details to guarantee confidentiality and anonymity. The third ethical consideration was professionalism. The researcher ensured that the collected data was handled properly and used for academic purposes only.
The study employed the use of research assistants who facilitated the collection of data. The research assistant was engaged to distribute physical hard-copies of the questionnaire and to pick them up once they were filled after a period of one week. A cover letter detailing the purpose of the study and assuring confidentiality of respondent information was used as a strategy to ensure objective, truthful and factual responses were collected from the respondents.

**3.6 Data Analysis Methods**

Data analysis involves the process of editing and reducing accumulated data to a manageable size, developing summaries, identifying patterns, and applying statistical techniques to deduce and verify conclusions (Cooper & Schindler, 2014). Once received, the data was subjected to physical verification by checking for missing data or unfilled sections of the questionnaire and edited or discarded as necessary. Only sections that were properly filled were deemed useful. After the cleaning and editing, data was coded using statistical software application. The statistical software that was used to analyze the data collected was SPSS.

The coded data were analyzed using mean and standard deviations which were measures of central tendency. Inferential analysis was also used in the study. Correlation analysis was used to investigate the relationship between the various causative factors of operational risks in commercial banks. Linear regressions analysis including model summary, analysis of variance (ANOVA) and regression coefficients was used to observe how each of the independent variables (card payments, electronic cash, and e-wallets) influenced operational risks in commercial banks. Final analyzed data was presented using figures and tables.

**3.7 Chapter Summary**

The chapter covers the methodology that was used in this study. It highlights the research design, data collection, population, and sampling techniques, and data analysis processes adopted. Chapter four presents the findings and results of the data collected and analyzed.
CHAPTER FOUR

4.0 RESULTS AND FINDINGS

4.1 Introduction

This chapter is the results and findings of the collected and analyzed data. The chapter was guided by the questionnaire structure, where section 4.2 is the demographics result, section 4.3 are the results for card payments and operational risk management of commercial banks, section 4.4 are the results for electronic cash and operational risk management of commercial banks, section 4.5 are the results for e-wallets and operational risk management of commercial banks, and section 4.6 is the chapter summary.

4.2 Response Rate and Demographic Information

The section focused on the study’s response rate and provision of demographic data of the responses. These were presented using figures, and it provides the analysis for the response rate, and the respondents’ gender, age, position in the firm, the department they work in, years with the bank, and their level of education.

4.2.1 Response Rate

During the data collection period, the researcher and his assistants managed to distribute 83 questionnaires to the bank managers. During the data cleaning process, 55 questionnaires were found to be valid for use, out of the 78 that were received from the population. This provided the study with a response rate of 66.3% which was acceptable for this study.

![Figure 4.1 Response Rate](image_url)
4.2.2 Demographic Information of Respondents
This section provides the analysis for the demographic information of respondents, particularly their gender, age, position in the firm, the department they work in, years with the bank, and their level of education, using figures.

4.2.2.1 Gender of Respondents
The study asked the respondents to indicate their gender, and the results were presented in Figure 4.2. These results showed that 63.6% were male and 36.4% were female. This shows that commercial banks in Nairobi were managed by males, and there was a significant number of females in their management as well. This may be explained by the nature of the work involved.

![Figure 4.2 Gender of Respondents](image)

Figure 4.2 Gender of Respondents

4.2.2.2 Age of Respondents
The study respondents were requested to indicate their age bracket and the response obtained was as shown in Figure 4.3. The result indicates that 34.5% were aged between 41-45 years, 29.1% were 46 years and above, 27.3% were between the ages of 36-40 years, 9.1% were aged between 31-35 years, and none was below the age of 30 years. This is indicative of the fact that most bank managers were above the age of 36 years, which may be explained by the years it took to ascend the corporate ladder.

![Figure 4.3 Age Bracket of Respondents](image)

Figure 4.3 Age Bracket of Respondents
4.2.2.3 Position of Respondents

The study asked the respondents to indicate their respective positions in the banks, and the results were presented in Figure 4.4. These results indicate that 49.1% of the respondents were in the middle-level management, 34.5% were in the low-level management, and 16.4% were in senior management. This shows that all levels of management within the commercial banks in Nairobi were covered, resulting in a comprehensive study result.

![Figure 4.4 Position of Respondents](image)

4.2.2.4 Department of Respondents

Respondents were requested to indicate their respective department within the bank, and the results were presented in Figure 4.5. This result shows that 20% were from operations, 12.7% were from finance, compliance, corporate banking, and were branch managers respectively, 10.9% were from retail banking, 7.3% were from risk department, and 5.5% were from legal and information and technology departments. This shows that all departments were covered, resulting in a comprehensive study result.

![Figure 4.5 Department of Respondents](image)
4.2.2.5 Respondents’ Years with the Bank

The study respondents were requested to indicate the number of years they had worked for their respective banks, and the response obtained was as shown in Figure 4.6. The result indicates that 41.8% had worked for 16-20 years, 29.1% had worked for 21 years and above, 21.8% had worked for 11-15 years, and 7.3% had been with their bank for 6-10 years. The study shows that all the respondents had been with their respective firms for over 5 years making them very reliable for this study.

Figure 4.6 Respondents’ Years with the Bank

4.2.2.6 Education Level of Respondents

The study respondents were asked to specify their highest level of education, and the response obtained was as shown in Figure 4.7. The result shows that 50.9% had attained their undergraduate degrees, 40% had attained their Master’s degrees, 5.5% had attained college diplomas, and 3.6% had doctorates. This shows that the managers of commercial banks were well educated and could understand the study questions.

Figure 4.7 Education Level of Respondents
4.3 Card Payments and Operational Risk Management of Commercial Banks

The first objective of the study was set to examine the effect of card payments on the operational risk management of Kenyan commercial banks. This section offers the descriptive, correlation and regression analyses for card payment factors and their influence on the operational risk management of Kenyan commercial banks.

4.3.1 Descriptive Analysis

Table 4.1 shows that the banks have a wide range of plastic money that their customers can make use of as indicated by 83.6% of the respondents, while 16.4% were neutral (mean 4.35, standard deviation=0.751). The banks rely on third-party service providers to conduct card payment processing as indicated by 83.6% of the respondents, while 16.4% were neutral (mean 4.27, standard deviation=0.732). The banks compete with nonbank entities to provide retail payment services as indicated by 78.2% of the respondents, while 21.8% were neutral (mean 4.11, standard deviation=0.737). Expanding card services significantly increases banks’ potential operational risk as indicated by 69.1% of the respondents, while 30.9% were neutral (mean 3.98, standard deviation=0.782).

Retail payment-related systems affect the reputation of the bank in terms of meeting regulatory and consumer protection obligations as indicated by 67.3% of the respondents, while 32.7% were neutral (mean 3.95, standard deviation=0.780). The bank is responsible for risks associated with the activities of the third-party service providers they contract as indicated by 78.2% of the respondents, while 21.8% were neutral (mean 4.25, standard deviation=0.799). When using a third-party service provider, the bank is responsible for the credit risk exposure of the services being performed as indicated by 83.6% of the respondents, while 16.4% were neutral (mean 4.27, standard deviation=0.732).

Deferred settlements present a risk for the bank that the paying institution or intermediate party may fail before the inter-institution settlement occurs as indicated by 87.3% of the respondents, while 12.7% were neutral (mean 4.22, standard deviation=0.658). Bankcards have specific procedures for amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account as indicated by 85.5% of the respondents, while 14.5% were neutral (mean 4.22, standard deviation=0.686). The banks allow corporate
customers to incur intraday or “daylight” overdrafts as indicated by 90.9% of the respondents, while 9.1% were neutral (mean 4.11, standard deviation=0.737).

Table 4.1 Descriptive Analysis for Card Payments & Operational Risk Management

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
<th>Std.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our bank has a wide range of plastic money that our customers can make use of</td>
<td>0</td>
<td>0</td>
<td>16.4</td>
<td>32.7</td>
<td>50.9</td>
<td>4.35</td>
</tr>
<tr>
<td>Our bank relies on third-party service providers to conduct card payment processing</td>
<td>0</td>
<td>0</td>
<td>16.4</td>
<td>40</td>
<td>43.6</td>
<td>4.27</td>
</tr>
<tr>
<td>Our bank competes with nonbank entities to provide retail payment services</td>
<td>0</td>
<td>0</td>
<td>21.8</td>
<td>45.5</td>
<td>32.7</td>
<td>4.11</td>
</tr>
<tr>
<td>Expanding card services significantly increases our potential operational risk</td>
<td>0</td>
<td>0</td>
<td>30.9</td>
<td>40</td>
<td>29.1</td>
<td>3.98</td>
</tr>
<tr>
<td>Retail payment-related systems affect the reputation of the bank in terms of meeting regulatory and consumer protection obligations</td>
<td>0</td>
<td>0</td>
<td>32.7</td>
<td>40</td>
<td>27.3</td>
<td>3.95</td>
</tr>
<tr>
<td>Our bank is responsible for risks associated with the activities of the third-party service providers we contract</td>
<td>0</td>
<td>0</td>
<td>21.8</td>
<td>30.9</td>
<td>47.3</td>
<td>4.25</td>
</tr>
<tr>
<td>When using a third-party service provider, the bank is responsible for the credit risk exposure of the services being performed</td>
<td>0</td>
<td>0</td>
<td>16.4</td>
<td>40</td>
<td>43.6</td>
<td>4.27</td>
</tr>
<tr>
<td>Deferred settlements present a risk for the bank that the paying institution or intermediate party may fail before the inter-institution settlement occurs</td>
<td>0</td>
<td>0</td>
<td>12.7</td>
<td>52.7</td>
<td>34.5</td>
<td>4.22</td>
</tr>
<tr>
<td>Our bankcards have specific procedures for amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account</td>
<td>0</td>
<td>0</td>
<td>14.5</td>
<td>49.1</td>
<td>36.4</td>
<td>4.22</td>
</tr>
<tr>
<td>Our bank allows corporate customers to incur intraday or “daylight” overdrafts</td>
<td>0</td>
<td>0</td>
<td>9.1</td>
<td>47.3</td>
<td>43.6</td>
<td>4.35</td>
</tr>
</tbody>
</table>
4.3.2 Correlation Analysis for Card Payments and Operational Risk Management

Table 4.2 presents the correlations between card payment factors and operational risk management of commercial banks. The table shows that card payments were significant to the operational risk management of commercial banks \( (r=0.340, \ p<0.05) \). The strategic risk was insignificant to the operational risk management of commercial banks \( (r=0.175, \ p<0.05) \). Reputation risk was insignificant to the operational risk management of commercial banks \( (r=0.045, \ p<0.05) \). Credit risk was insignificant to the operational risk management of commercial banks \( (r=-0.091, \ p<0.05) \).

<table>
<thead>
<tr>
<th></th>
<th>Operational Management Risk</th>
<th>Card Payments</th>
<th>Strategic Risk</th>
<th>Reputation Risk</th>
<th>Credit Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Risk</td>
<td></td>
<td>.340*</td>
<td>.011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Payments</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic Risk</td>
<td>.175</td>
<td>.289*</td>
<td>.202</td>
<td>.032</td>
<td></td>
</tr>
<tr>
<td>Reputation Risk</td>
<td>.045</td>
<td>.249</td>
<td>.078</td>
<td>.570</td>
<td></td>
</tr>
<tr>
<td>Credit Risk</td>
<td>-.091</td>
<td>-.052</td>
<td>.018</td>
<td>.332*</td>
<td>.507</td>
</tr>
<tr>
<td></td>
<td>.507</td>
<td>.507</td>
<td>.897</td>
<td>.013</td>
<td></td>
</tr>
</tbody>
</table>

* Correlation is significant at the 0.05 level (2-tailed)

4.3.3 Regression Analysis for Card Payments and Operational Risk Management

The following part presents the regression analysis between card payments and operational risk management of commercial banks. This was conducted to examine the nature of the relationship between the two study variables (card payments and operational risk management), specifically, to determine how the independent variable influences the dependent variable, and the course of their relationship when one of the variables change. This is presented using the model summary, ANOVA, and linear regression coefficient.
4.3.3.1 Model Summary for Card Payments and Operational Risk Management

Table 4.3 shows the existing relationship between card payments and operational risk management of commercial banks, and the R square value of 0.116 shows that card payments influence operational risk management of commercial banks by 11.6%.

<table>
<thead>
<tr>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.340</td>
<td>.116</td>
<td>.099</td>
<td>.27879</td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), Card Payments

4.3.3.2 ANOVA for Card Payments and Operational Risk Management

Table 4.4 presents the ANOVA for card payments and operational risk management. The linear regression of the F statistics shown signifies that there was a statistical and significant linear relationship between card payments and operational risk management of commercial banks (F (1, 53) = 6.939, p<.05). This means that the regression analysis was fit for the study.

<table>
<thead>
<tr>
<th>Model</th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regression</td>
<td>.539</td>
<td>1</td>
<td>.539</td>
<td>6.939</td>
</tr>
<tr>
<td></td>
<td>Residual</td>
<td>4.119</td>
<td>53</td>
<td>.078</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>4.659</td>
<td>54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), Card Payments

b. Dependent Variable: Operational Risk Management

4.3.3.3 Coefficients for Card Payments and Operational Risk Management

Table 4.5 provides the regression coefficient that indicates the existing relationship between card payments and operational risk management of commercial banks. The table produces a linear regression of the relationship in the form:

\[
\text{Operational Risk Management} = 3.506 + 0.182 \text{ Card Payments} + e
\]

From the table, it can be inferred that card payments were significant to the operational risk management of commercial banks because its p-value was < 0.05. From the equation, it can also be inferred that a single unit increase in card payments results in an 18.2% increase in operational risk management of commercial banks.
Table 4.5 Coefficient for Card Payments and Operational Risk Management

<table>
<thead>
<tr>
<th>Model</th>
<th>Unstandardized Coefficients</th>
<th>Standardized Coefficients</th>
<th>t</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>Std. Error</td>
<td>Beta</td>
<td></td>
</tr>
<tr>
<td>1 (Constant)</td>
<td>3.506</td>
<td>.182</td>
<td>.283</td>
<td>12.370</td>
</tr>
<tr>
<td>Card Payments</td>
<td>.182</td>
<td>.069</td>
<td>.340</td>
<td>2.634</td>
</tr>
</tbody>
</table>

a. Dependent Variable: Operational Risk Management

4.4 Electronic Cash and Operational Risk Management of Commercial Banks

The second objective of the study was set to determine the effect of electronic cash on the operational risk management of Kenyan commercial banks. This section offers the descriptive, correlation and regression analyses for electronic cash factors and their influence on the operational risk management of Kenyan commercial banks.

4.4.1 Descriptive Analysis

Table 4.6 shows that the bank has developed electronic cash payment instruments as indicated by 90.9% of the respondents, while 9.1% were neutral (mean 4.42, standard deviation=0.658). The bank provides options for pre-funded accounts that facilitate the ability to use online auction payments as indicated by 87.3% of the respondents, while 12.7% were neutral (mean 4.44, standard deviation=0.714). Electronic money represents liabilities on the balance sheet of the bank as indicated by 85.5% of the respondents, while 14.5% were neutral (mean 4.31, standard deviation=0.717). The value of electronic money can diminish if the liabilities of the issuer are higher than the value of the assets as indicated by 96.4% of the respondents, while 3.6% were neutral (mean 4.35, standard deviation=0.552). Liquidity risk in payment system may arise from the bank’s inability to meet their obligations when they are due as indicated by 92.7% of the respondents, while 7.3% were neutral (mean 4.36, standard deviation=0.620).

Liquidity problems result in opportunity costs for the bank as indicated by 85.5% of the respondents, while 14.5% were neutral (mean 4.24, standard deviation=0.693). The banking scheme has the ability to detect counterfeits and fraud in the system as indicated by 92.7% of the respondents, while 7.3% were neutral (mean 4.51, standard deviation=0.635). The banks’ electronic money units are transferable from customer to customer without the transactions being subsequently recorded by the issuer or a clearing
system as indicated by 96.4% of the respondents, while 3.6% were neutral (mean 4.44, standard deviation=0.570). Legal disputes that occur, cause systemic risk to the payment systems as indicated by 92.7% of the respondents, while 7.3% were neutral (mean 4.38, standard deviation=0.623). The bank has a legal measure that ensures they have complied with laws and regulations pertinent to e-payment systems as indicated by 94.5% of the respondents, while 5.5% were neutral (mean 4.42, standard deviation=0.599).

Table 4.6 Descriptive Analysis for Electronic Cash & Operational Risk Management

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
<th>M</th>
<th>Dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our bank has developed electronic cash payment instruments</td>
<td>0</td>
<td>0</td>
<td>9.1</td>
<td>40</td>
<td>50.9</td>
<td>4.42</td>
<td>.658</td>
</tr>
<tr>
<td>The bank provides options for pre-funded accounts that facilitate the ability to use online auction payments</td>
<td>0</td>
<td>0</td>
<td>12.7</td>
<td>30.9</td>
<td>56.4</td>
<td>4.44</td>
<td>.714</td>
</tr>
<tr>
<td>Electronic money represents liabilities on the balance sheet of the bank</td>
<td>0</td>
<td>0</td>
<td>14.5</td>
<td>40</td>
<td>45.5</td>
<td>4.31</td>
<td>.717</td>
</tr>
<tr>
<td>The value of electronic money can diminish if the liabilities of the issuer are higher than the value of the assets</td>
<td>0</td>
<td>0</td>
<td>3.6</td>
<td>58.2</td>
<td>38.2</td>
<td>4.35</td>
<td>.552</td>
</tr>
<tr>
<td>Liquidity risk in the payment system may arise from our inability to meet our obligations when they are due</td>
<td>0</td>
<td>0</td>
<td>7.3</td>
<td>49.1</td>
<td>43.6</td>
<td>4.36</td>
<td>.620</td>
</tr>
<tr>
<td>Liquidity problems results in opportunity costs for the bank</td>
<td>0</td>
<td>0</td>
<td>14.5</td>
<td>47.3</td>
<td>38.2</td>
<td>4.24</td>
<td>.693</td>
</tr>
<tr>
<td>Our banking scheme has the ability to detect counterfeits and fraud in the system</td>
<td>0</td>
<td>0</td>
<td>7.3</td>
<td>34.5</td>
<td>58.2</td>
<td>4.51</td>
<td>.635</td>
</tr>
<tr>
<td>Our banks’ electronic money units are transferable from customer to customer without the transactions being subsequently recorded by the issuer or a clearing system</td>
<td>0</td>
<td>0</td>
<td>3.6</td>
<td>49.1</td>
<td>47.3</td>
<td>4.44</td>
<td>.570</td>
</tr>
<tr>
<td>Legal disputes that occur, cause systemic risk to our payment systems</td>
<td>0</td>
<td>0</td>
<td>7.3</td>
<td>47.3</td>
<td>45.5</td>
<td>4.38</td>
<td>.623</td>
</tr>
<tr>
<td>The bank has a legal measure that ensures we have complied with laws and regulations pertinent to e-payment systems</td>
<td>0</td>
<td>0</td>
<td>5.5</td>
<td>47.3</td>
<td>47.3</td>
<td>4.42</td>
<td>.599</td>
</tr>
</tbody>
</table>
4.4.2 Correlation Analysis

Table 4.7 presents the correlations between electronic cash factors and operational risk management of commercial banks. The table shows that electronic cash was significant to the operational risk management of commercial banks ($r=0.376$, $p<0.05$). Consumer and merchant risk was insignificant to the operational risk management of commercial banks ($r=0.140$, $p>0.05$). Liquidity risk was significant to the operational risk management of commercial banks ($r=0.304$, $p<0.05$). Counterfeit and fraud risk was insignificant to the operational risk management of commercial banks ($r=0.155$, $p>0.05$). The legal risk was insignificant to the operational risk management of commercial banks ($r=0.165$, $p>0.05$).

Table 4.7 Correlation Analysis for Electronic Cash and Operational Risk Management

<table>
<thead>
<tr>
<th>Operational Risk Management</th>
<th>Electronic Cash</th>
<th>Consumer Risk</th>
<th>Liquidity Risk</th>
<th>Counterfeit &amp; Fraud Risk</th>
<th>Legal Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Risk Management</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Cash</td>
<td>.376**</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash</td>
<td>.005</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer Risk</td>
<td>.140</td>
<td>-.102</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>.309</td>
<td>.458</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liquidity Risk</td>
<td>.304*</td>
<td>.168</td>
<td>.788**</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>.024</td>
<td>.219</td>
<td>.000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counterfeit &amp; Fraud Risk</td>
<td>.155</td>
<td>.410**</td>
<td>.028</td>
<td>.464**</td>
<td>1</td>
</tr>
<tr>
<td>Legal Risk</td>
<td>.258</td>
<td>.002</td>
<td>.837</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td>Legal Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

** Correlation is significant at the 0.01 level (2-tailed)
* Correlation is significant at the 0.05 level (2-tailed)

4.4.3 Regression Analysis

The following part presents the regression analysis between electronic cash and operational risk management of commercial banks. This was conducted to examine the nature of the relationship between the two study variables (electronic cash and operational risk management), specifically, to determine how the independent variable influences the dependent variable, and the course of their relationship when one of the variables change. This is presented using the model summary, ANOVA, and linear regression coefficient.
4.4.3.1 Model Summary for Electronic Cash and Operational Risk Management
Table 4.8 shows the existing relationship between electronic cash and operational risk management of commercial banks, and the R square value of 0.142 shows that electronic cash influence operational risk management of commercial banks by 14.2%.

<table>
<thead>
<tr>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.376</td>
<td>.142</td>
<td>.125</td>
<td>.27469</td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), Electronic Cash

4.4.3.2 ANOVA for Electronic Cash and Operational Risk Management
Table 4.9 presents the ANOVA for electronic cash and operational risk management. The linear regression of the F statistic shown signifies that there was a statistical and significant linear relationship between electronic cash and operational risk management of commercial banks (F (1, 53) = 8.740, p<.05). This is indicative of the regression being the best fit for this study.

<table>
<thead>
<tr>
<th>Model</th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regression</td>
<td>.660</td>
<td>1</td>
<td>.660</td>
<td>8.740</td>
</tr>
<tr>
<td></td>
<td>Residual</td>
<td>3.999</td>
<td>53</td>
<td>.075</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>4.659</td>
<td>54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), Electronic Cash
b. Dependent Variable: Operational Risk Management

4.4.3.3 Coefficients for Electronic Cash and Operational Risk Management
Table 4.10 provides the regression coefficient that indicates the existing relationship between electronic cash and operational risk management of commercial banks. The table produces a linear regression of the relationship in the form:

\[ \text{Operational Risk Management} = 2.799 + 0.335 \text{Electronic Cash} + e \]

From the table, it can be inferred that electronic cash was significant to the operational risk management of commercial banks because its p-value was < 0.05. From the equation, it can also be inferred that a single unit increase in electronic cash results in a 33.5% increase in operational risk management of commercial banks.
Table 4.10 Coefficient for Electronic Cash and Operational Risk Management

<table>
<thead>
<tr>
<th>Model</th>
<th>Unstandardized Coefficients</th>
<th>Standardized Coefficients</th>
<th>t</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>Std. Error</td>
<td>Beta</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>(Constant)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Cash</td>
<td>2.799</td>
<td>.491</td>
<td>5.705</td>
<td>.000</td>
</tr>
<tr>
<td></td>
<td>.335</td>
<td>.113</td>
<td>.376</td>
<td>.005</td>
</tr>
</tbody>
</table>

a. Dependent Variable: Operational Risk Management

4.5 E-Wallets and Operational Risk Management of Commercial Banks

The third objective of the study was set to examine the effect of e-wallets on the operational risk management of Kenyan commercial banks. This section offers the descriptive, correlation and regression analyses for e-wallet factors and their influence on the operational risk management of Kenyan commercial banks.

4.5.1 Descriptive Analysis

Table 4.11 shows that the bank provides a digital wallet where customers make money transactions and payments as indicated by 83.6% of the respondents, while 16.4% were neutral (mean 4.16, standard deviation=0.688). The bank has outsourced retail payment-related services to third parties to enhance the services they perform in-house as indicated by 80% of the respondents, while 20% were neutral (mean 4.11, standard deviation=0.712). The bank has adequate due diligence processes that monitor their service providers for compliance as indicated by 96.4% of the respondents, while 3.6% were neutral (mean 4.45, standard deviation=0.571). The bank maintains effective control over customer and financial institution information accessed by their service providers as indicated by 90.9% of the respondents, while 9.1% were neutral (mean 4.42, standard deviation=0.658). The bank has a continuity plan in place that is capable of maintaining acceptable retail payment-related customer service levels as indicated by 94.5% of the respondents, while 5.5% were neutral (mean 4.40, standard deviation=0.596).

The bank has a business continuity plan in place that is based on their business impact analysis that is relative to their retail payment system products and services as indicated by 92.7% of the respondents, while 7.3% were neutral (mean 4.40, standard deviation=0.627). Privacy risk of e-wallets’ fund transfer has ensured that it is ranked high in the bank as indicated by 90.9% of the respondents, while 9.1% were neutral.
(mean 4.29, standard deviation=0.629). The bank has physical controls in place that limit access to the staff assigned the responsibility of supporting e-payment operations as indicated by 94.5% of the respondents, while 5.5% were neutral (mean 4.47, standard deviation=0.604). E-wallets expose banks to transaction risks from fraudulent activities as indicated by 96.4% of the respondents, while 3.6% were neutral (mean 4.44, standard deviation=0.570). The bank has system measures in place that verify the authenticity of the payer and transaction information integrity as indicated by 94.5% of the respondents, while 5.5% were neutral (mean 4.38, standard deviation=0.593).

### Table 4.11 Descriptive Analysis for E-Wallet and Operational Risk Management

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>D</th>
<th>N</th>
<th>A</th>
<th>SA</th>
<th>M</th>
<th>Std. Dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>The bank provides a digital wallet where customers make money transactions and payments</td>
<td>0</td>
<td>0</td>
<td>16.4</td>
<td>50.9</td>
<td>32.7</td>
<td>4.16</td>
<td>.688</td>
</tr>
<tr>
<td>We have outsourced retail payment-related services to third parties to enhance the services we perform in-house</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>49.1</td>
<td>30.9</td>
<td>4.11</td>
<td>.712</td>
</tr>
<tr>
<td>Our bank has adequate due diligence processes that monitor our service providers for compliance</td>
<td>0</td>
<td>0</td>
<td>3.6</td>
<td>47.3</td>
<td>49.1</td>
<td>4.45</td>
<td>.571</td>
</tr>
<tr>
<td>Our bank maintains effective control over customer and financial institution information accessed by our service providers</td>
<td>0</td>
<td>0</td>
<td>9.1</td>
<td>40</td>
<td>50.9</td>
<td>4.42</td>
<td>.658</td>
</tr>
<tr>
<td>The bank has a continuity plan in place that is capable of maintaining acceptable retail payment-related customer service levels</td>
<td>0</td>
<td>0</td>
<td>5.5</td>
<td>49.1</td>
<td>45.5</td>
<td>4.40</td>
<td>.596</td>
</tr>
<tr>
<td>The bank has a business continuity plan in place that is based on our business impact analysis that is relative to our retail payment system products and services</td>
<td>0</td>
<td>0</td>
<td>7.3</td>
<td>45.5</td>
<td>47.3</td>
<td>4.40</td>
<td>.627</td>
</tr>
<tr>
<td>Privacy risk of e-wallets’ fund transfer has ensured that it is ranked high in the bank</td>
<td>0</td>
<td>0</td>
<td>9.1</td>
<td>52.7</td>
<td>38.2</td>
<td>4.29</td>
<td>.629</td>
</tr>
<tr>
<td>The bank has physical controls in place that limit access to the staff assigned the responsibility of supporting e-payment operations</td>
<td>0</td>
<td>0</td>
<td>5.5</td>
<td>41.8</td>
<td>52.7</td>
<td>4.47</td>
<td>.604</td>
</tr>
<tr>
<td>E-wallets expose our bank to transaction risks from fraudulent activities</td>
<td>0</td>
<td>0</td>
<td>3.6</td>
<td>49.1</td>
<td>47.3</td>
<td>4.44</td>
<td>.570</td>
</tr>
<tr>
<td>Our bank has system measures in place that verify the authenticity of the payer and transaction information integrity</td>
<td>0</td>
<td>0</td>
<td>5.5</td>
<td>50.9</td>
<td>43.6</td>
<td>4.38</td>
<td>.593</td>
</tr>
</tbody>
</table>
4.5.2 Correlation Analysis

Table 4.12 presents the correlations between e-wallet factors and operational risk management of commercial banks. The table shows that e-wallet was significant to the operational risk management of commercial banks ($r=0.407$, $p<0.05$). Vendor and third-party management were significant to the operational risk management of commercial banks ($r=0.390$, $p<0.05$). Business continuity risk was insignificant to the operational risk management of commercial banks ($r=0.013$, $p>0.05$). Information security was significant to the operational risk management of commercial banks ($r=0.384$, $p<0.05$). Transaction risk was insignificant to the operational risk management of commercial banks ($r=0.070$, $p>0.05$).

Table 4.12 Correlation Analysis for E-Wallet and Operational Risk Management

<table>
<thead>
<tr>
<th></th>
<th>Operational Risk Management</th>
<th>E-Wallet</th>
<th>Vendor Mgt</th>
<th>Business Continuity Risk</th>
<th>Information Security</th>
<th>Transaction Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Risk</td>
<td>1</td>
<td>.407**</td>
<td>.002</td>
<td>.390**</td>
<td>.526**</td>
<td>.013</td>
</tr>
<tr>
<td>Vendor &amp; 3rd-Party</td>
<td></td>
<td>.003</td>
<td>.000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity</td>
<td></td>
<td>.016</td>
<td>.928</td>
<td>.570**</td>
<td>.016</td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td></td>
<td>.069</td>
<td>.906</td>
<td>.320*</td>
<td>.008</td>
<td></td>
</tr>
<tr>
<td>Transaction Risk</td>
<td></td>
<td>.017</td>
<td>.953</td>
<td>.386</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

** Correlation is significant at the 0.01 level (2-tailed)
* Correlation is significant at the 0.05 level (2-tailed)
4.5.3 Regression Analysis

The following part presents the regression analysis between e-wallet and operational risk management of commercial banks. This was conducted to examine the nature of the relationship between the two study variables (e-wallet and operational risk management), specifically, to determine how the independent variable influences the dependent variable, and the course of their relationship when one of the variables change. This is presented using the model summary, ANOVA, and linear regression coefficient.

4.5.3.1 Model Summary for E-Wallet and Operational Risk Management

Table 4.13 shows the existing relationship between e-wallet and operational risk management of commercial banks, and the R square value of 0.166 shows that e-wallet influences operational risk management of commercial banks by 16.6%.

<table>
<thead>
<tr>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.407</td>
<td>.166</td>
<td>.150</td>
<td>.27082</td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), E-Wallet

4.5.3.2 ANOVA for E-Wallet and Operational Risk Management

Table 4.14 presents the ANOVA for e-wallet and operational risk management. The linear regression of the F statistics shown signifies that there was a statistical and significant linear relationship between e-wallet and operational risk management of commercial banks (F (1, 53) = 10.515, p<.05). This was proof that the regression analysis was best suited for this study.

<table>
<thead>
<tr>
<th>Model</th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regression</td>
<td>.771</td>
<td>1</td>
<td>.771</td>
<td>10.515</td>
</tr>
<tr>
<td></td>
<td>Residual</td>
<td>3.887</td>
<td>53</td>
<td>.073</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>4.659</td>
<td>54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), E-Wallet

b. Dependent Variable: Operational Risk Management
4.5.3.3 Coefficients for E-Wallet and Operational Risk Management

Table 4.15 provides the regression coefficient that indicates the existing relationship between e-wallet and operational risk management of commercial banks. The table produces a linear regression of the relationship in the form:

\[
\text{Operational Risk Management} = 3.122 + 0.260 \times \text{E-Wallet} + e
\]

From the table, it can be inferred that e-wallet was significant to the operational risk management of commercial banks because its p-value was < 0.05. From the equation, it can also be inferred that a single unit increase in e-wallet results in a 26% increase in operational risk management of commercial banks.

Table 4.15 Coefficient for E-Wallet and Operational Risk Management

<table>
<thead>
<tr>
<th>Model</th>
<th>Unstandardized Coefficients</th>
<th>Standardized Coefficients</th>
<th>t</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>Std. Error</td>
<td>Beta</td>
<td></td>
</tr>
<tr>
<td>1 (Constant)</td>
<td>3.122</td>
<td>.348</td>
<td>8.962</td>
<td>.000</td>
</tr>
</tbody>
</table>

a. Dependent Variable: Operational Risk Management

4.6 Chapter Summary

This chapter has presented the results and findings of the collected and analyzed data. It was guided by the questionnaire structure. The chapter has provided descriptive, and inferential analysis for card payments and operational risk management of commercial banks, electronic cash and operational risk management of commercial banks, and e-wallets and operational risk management of commercial banks. The next chapter focuses on the discussions, conclusions, and recommendations of the study.
CHAPTER FIVE
5.0 DISCUSSIONS, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction
This section summarizes the study by providing a detailed summary, discussion, conclusion, and recommendation for the effect of e-payments on the operational risk management of Kenyan commercial banks. These deliberations have been guided by the study objectives.

5.2 Summary
The general objective of the study was to examine the effect of e-payments on the operational risk management of Kenyan commercial banks. The study was geared towards finding the following: to examine the effect of card payments on the operational risk management of Kenyan commercial banks, to determine the effect of electronic cash on the operational risk management of Kenyan commercial banks, and to examine the effect of e-wallets on the operational risk management of Kenyan commercial banks.

This study made use of a descriptive research design. The population for this study comprised of the senior management employees of the 45 commercial banks that operated in Nairobi - Kenya who were approximately 505. For this study, the sampling frame was the list of senior management employees of the 45 Kenyan commercial banks and was obtained from the respective banks. Stratified sampling technique was used in the study to divide the population into homogeneous groups, where simple random sampling was used to select respondents. Yamane (1967) formula was used to determine the sample size for the study to 83. The primary data was collected using structured questionnaires which were piloted using 10 respondents. Collected data were analyzed using SPSS. Measures of central tendencies including percentages, means, and standard deviation were used during analysis. Inferential analysis was also used in the study. Correlation analysis was used to investigate the relationship between the various causative factors of operational risks in commercial banks. Linear regressions analysis including model summary, ANOVA and regression coefficients were used to observe how each of the independent variables (card payments, electronic cash, and e-wallets) influenced operational risks in commercial banks. Final analyzed data was presented using figures and tables.
The study showed that the commercial banks had a wide range of plastic money that their customers made use of, and they relied on third-party service providers to conduct card payment processing. These banks competed with nonbank entities to provide retail payment services, and the expansion of card services significantly increases their potential operational risk. Retail payment-related systems affected the reputation of the banks in terms of meeting regulatory and consumer protection obligations since they were responsible for risks associated with the activities of the third-party service providers they had contracted, as well as being responsible for the credit risk exposure of the services being performed. Deferred settlements presented a risk for the banks that the paying institution or intermediate party may fail before the inter-institution settlement occurs, however, the bankcards had specific procedures for amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account. Commercial banks in Nairobi allowed corporate customers to incur intraday or “daylight” overdrafts, wherever possible.

The study revealed that the banks had developed electronic cash payment instruments which provided options for pre-funded accounts that facilitated the ability to use online auction payments. Electronic money represented liabilities on the balance sheet of the banks because the value of electronic money could diminish if the liabilities of the issuer were higher than the value of the assets. Liquidity risk in the payment system could arise from the inability of the banks to meet their obligations when they were due, and this would result in opportunity costs for the banks. The banking scheme had the ability to detect counterfeits and fraud within the system since the banks’ electronic money units were transferable from customer to customer without the transactions being subsequently recorded by the issuer or a clearing system. Legal disputes that occurred, caused systemic risk to the banks’ payment systems, and thus, the banks had legal measures that ensured they had complied with laws and regulations pertinent to e-payment systems.

The study showed that the banks provided a digital wallet where customers made money transactions and payments, although they had outsourced these retail payment-related services to third parties to enhance their in-house services. The banks had adequate due diligence processes that monitor their service providers for compliance, and they maintained effective control over customer and financial institution information accessed.
by these service providers. The banks had a continuity plan in place that was capable of maintaining acceptable retail payment-related customer service levels and were based on their business impact analysis that was relative to their retail payment system products and services. Privacy risk of e-wallets’ fund transfer had ensured that it was ranked high in the banks, and physical controls were in place that limited access to the staff assigned the responsibility of supporting e-payment operations. E-wallets exposed commercial banks to transaction risks from fraudulent activities, however, the banks had system measures in place that verified the authenticity of the payer and transaction information integrity.

5.3 Discussions
5.3.1 Card Payments and Operational Risk Management of Commercial Banks
The study showed that the banks have a wide range of plastic money that their customers make use of. This result is in agreement with Michael, Bodmer & LeMasters (2009) who state that, a contrast can be drawn between banks that have a wide range of plastic money to those that have limited or non-existent use of plastic money. Credit and debit card overdraft loans account for one of the highest rates of consumer debt growth.

The study revealed that the banks rely on third-party service providers to conduct card payment processing. This result agrees with ISACA (2015) who indicate that, financial institutions rely on third-party service providers to conduct card payment processing which may include card issuing services, merchant services, account maintenance, and authorization services, transaction routing and gateway services, off-line debit processing services, and clearing and settlement services.

The study indicated that the banks compete with nonbank entities to provide retail payment services. The study result is in agreement with Cheng et al. (2014) who stated that financial institutions also increasingly compete with nonbank entities to provide retail payment services. This competition benefits the consumer through enhanced product offerings at a lower cost.

The study showed that expanding card services significantly increases the banks’ potential operational risk. The study result agrees with Urban (2016) who states that,
expanding Internet banking services to include electronic bill presentment and payment services, expanding existing bankcard issuing programs, or entering the merchant bankcard processing business significantly increase the potential risk to the financial institution.

The study revealed that retail payment-related systems affect the reputation of the banks in terms of meeting regulatory and consumer protection obligations. This result concurs with Hohl (2016) who states that, for retail payment-related systems, reputation risk is linked with customer expectations regarding the delivery of retail payment services, and whether the institution is meeting its regulatory and consumer protection obligations relating to those services.

The study showed that the banks are responsible for risks associated with the activities of the third-party service providers they contract. This study agrees with ENISA (2016) who stated that, financial institutions are responsible for risks associated with the activities of third-party service providers with which they contract, for example, deficiencies in security and privacy policies that result in the release of customer information by a service provider may result in reputation damage.

The study indicated that when using a third-party service provider, the banks are responsible for the credit risk exposure of the services being performed. The study result agrees with Vos et al. (2014) who indicate that, if a financial institution uses a third-party service provider, it is responsible for the credit risk exposure for the services performed., and financial institutions should have procedures in place to manage the credit risk of third parties using their accounts to settle transactions.

The study revealed that deferred settlements present a risk for the bank that the paying institution or intermediate party may fail before the inter-institution settlement occurs. This study agrees with ENISA (2016) who stated that, with the deferred settlement, there is a risk that the paying institution or some intermediate party will fail before inter-institution settlement occurs. This deferred settlement, rather than real-time settlement, mitigates but does not eliminate the credit risk.
The study indicated that the bankcards have specific procedures for amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account. This study result is in agreement with Gupta (2013) who observed that, bankcards have specific procedures for chargebacks, which are amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account.

The study showed that the banks allows corporate customers to incur intraday or “daylight” overdrafts. This study result is in agreement with Tanai (2014) who indicates that, financial institutions often allow their corporate customers to incur intraday or “daylight” overdrafts. In principle, an institution engaging in this practice is extending credit to its customer.

5.3.2 Electronic Cash and Operational Risk Management of Commercial Banks

The study revealed that the banks have developed electronic cash payment instruments. The study result agrees with Dzemydiene et al. (2015) who noted that, financial institutions and retailers have also developed electronic cash payment instruments where individuals can transfer electronic cash value to other individuals or businesses.

The study indicated that the banks provide options for pre-funded accounts that facilitate the ability to use online auction payments. This study outcome is in agreement with Kim et al. (2014) who state that, consumers can use the cash payment instruments for purchases at retailers’ like pre-funded accounts, where consumers may use for online auction payments or with participating retailers are among the most recent applications.

The study showed that electronic money represents liabilities on the balance sheet of the banks. This study agrees with Elly (2012) who states that, electronic money represents liabilities on the balance sheet of the issuer, created against the provision by customers of cash or scriptural money, which are payable at par to the entities accepting electronic money as payment (the merchants).

The study revealed that the value of electronic money can diminish if the liabilities of the issuer are higher than the value of the assets. The result of the outcome concurs with Kasiyanto (2016) who observed that, as is the case with the value of bank deposits, the
value of electronic money could diminish, or even disappear, if the liabilities of the issuer are higher than the value of the assets.

The study showed that liquidity risk in the payment system may arise from the banks’ inability to meet their obligations when they are due. This result is in agreement with Parshotam & Gulati (2015) who state that, liquidity risk is the current and potential risk to earnings or capital arising from a financial institution’s inability to meet its obligations when they come due without incurring unacceptable losses.

The study revealed that liquidity problems result in opportunity costs for the banks. This result is in agreement with Parshotam & Gulati (2015) who state that, liquidity problems can result in opportunity costs, defaults on other obligations, or costs associated with obtaining the funds from another source for some period of time, and in addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period.

The study indicated that the banking scheme has the ability to detect counterfeits and fraud in the system. This study agrees with Elly (2012) who observed that, in the fast-developing technical world, the risk of counterfeit and fraud can hardly be excluded, and therefore, if a scheme lacks means detecting counterfeits and fraud, it will not be able to take appropriate counter-measures.

The study showed that the banks’ electronic money units are transferable from customer to customer without the transactions being subsequently recorded by the issuer or a clearing system. This agrees with Berentsen (2014) who observed that, by contrast, if electronic money units are transferable from customer to customer without these transactions being subsequently recorded by the issuer or a clearing system, the systems might entail a higher degree of operational risk.

The study revealed that legal disputes that occur, cause systemic risk to the banks’ payment systems. This study result agrees with Tak (2014) who observed that, though unlikely, legal disputes can also potentially cause systemic risk to the payments system.
and such legal problems are more likely to result from the failure of a financial institution than the default of an individual payer.

The study indicated that the banks have a legal measure that ensures they have complied with laws and regulations pertinent to e-payment systems. This result agrees with Goczek & Witkowski (2016) who opined that, legal measures should ensure compliance with specific laws and regulations pertinent to retail payment systems, as well as compliance with general consumer protection rules that allocate responsibility.

5.3.3 E-Wallets and Operational Risk Management of Commercial Banks
The study showed that the banks provided digital wallet where customers make money transactions and payments. The study result is supported by Yang et al. (2017) who state that, a digital wallet is a virtual wallet in a smartphone, in which money is stored in the form of virtual money, out of which one can make money transactions and payments.

The study revealed that the banks have outsourced retail payment-related services to third parties to enhance the services they perform in-house. This concurs with Berentsen (2014) who had observed that, some financial institutions rely on third-party service providers and other financial institutions to provide retail payment system products and services to their customers, which are directly related to core processing financial institution operations.

The study showed that the banks have adequate due diligence processes that monitors their service providers for compliance. The study result agrees with the opinion of Yaokumah, Kumah & Okai (2017) that, to ensure retail payment operations are conducted appropriately, financial institutions should have appropriate contract provisions and adequate due diligence processes. They should also monitor service providers for compliance.

The study revealed that the banks maintain effective control over customer and financial institution information accessed by their service providers. This outcome concurs with Goczek & Witkowski (2016) who state that, financial institution must maintain effective
control over service provider access to customer and financial institution information consistent with existing legal frameworks.

The study showed that the banks have a continuity plan in place that is capable of maintaining acceptable retail payment-related customer service levels. The result is in agreement with Francisco et al. (2015) who opined that, financial institutions and technology service providers should develop, implement, and test appropriate disaster recovery and business continuity plans capable of maintaining acceptable retail payment-related customer service levels.

The study revealed that the banks have a business continuity plan in place that is based on their business impact analysis that is relative to their retail payment system products and services. This study outcome is confirmed by Kasiyanto (2016) who states that, business continuity plans should be based on business impact analyses and the relative importance of retail payment system products and services to the financial institution.

The study indicated that the privacy risk of e-wallets’ fund transfer has ensured that it is ranked high in the banks. The result agrees with ISACA (2015) who state that, the privacy risk combined with the fund transfer capability should cause these systems to rank high in all institutions’ information security risk assessments, and these risk assessments should consider physical and logical security controls for the origination, approval, transmission, and storage of retail payment systems transactions.

The study showed that the banks have physical controls in place that limit access to the staff assigned the responsibility of supporting e-payment operations. This study outcome is in agreement with Junadi & Fenrianto (2015) who state that, physical controls should limit access to those staff assigned responsibility for supporting the operations and business line centers processing retail payment and accounting transactions.

The study indicated that e-wallets expose the banks to transaction risks from fraudulent activities. The result of the study is in agreement with Rachna & Singh (2016) who state that, a financial institution’s exposure to transaction risk from fraud is the risk that a wrongful or criminal deception will lead to a financial loss for one of the parties involved.
The study revealed that the banks have system measures in place that verify the authenticity of the payer and transaction information integrity. This result agrees with Hoofnagle et al. (2014) who state that, security controls include the use of certified tamper-resistant equipment, logical access controls to verify transactions, online verification of account balances, logging of all transactions and attempts to make a transaction, and the use of serial numbers and check digits.

5.4 Conclusions

5.4.1 Card Payments and Operational Risk Management of Commercial Banks
The study concludes that the commercial banks had a wide range of plastic money that their customers made use of, and they relied on third-party service providers to conduct card payment processing. These banks competed with nonbank entities to provide retail payment services, and the expansion of card services significantly increases their potential operational risk. Retail payment-related systems affected the reputation of the banks in terms of meeting regulatory and consumer protection obligations since they were responsible for risks associated with the activities of the third-party service providers they had contracted, as well as being responsible for the credit risk exposure of the services being performed. Deferred settlements presented a risk for the banks that the paying institution or intermediate party may fail before the inter-institution settlement occurs, however, the bankcards had specific procedures for amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account. Commercial banks in Nairobi allowed corporate customers to incur intraday or “daylight” overdrafts, wherever possible.

5.4.2 Electronic Cash and Operational Risk Management of Commercial Banks
The study concludes that the banks had developed electronic cash payment instruments which provided options for pre-funded accounts that facilitated the ability to use online auction payments. Electronic money represented liabilities on the balance sheet of the banks because the value of electronic money could diminish if the liabilities of the issuer were higher than the value of the assets. Liquidity risk in the payment system could arise from the inability of the banks to meet their obligations when they were due, and this would result in opportunity costs for the banks. The banking scheme had the ability to detect counterfeits and fraud within the system since the banks’ electronic money units
were transferable from customer to customer without the transactions being subsequently recorded by the issuer or a clearing system. Legal disputes that occurred, caused systemic risk to the banks’ payment systems, and thus, the banks had legal measures that ensured they had complied with laws and regulations pertinent to e-payment systems.

5.4.3 E-Wallets and Operational Risk Management of Commercial Banks
The study concludes that the banks provided a digital wallet where customers made money transactions and payments, although they had outsourced these retail payment-related services to third parties to enhance their in-house services. The banks had adequate due diligence processes that monitor their service providers for compliance, and they maintained effective control over customer and financial institution information accessed by these service providers. The banks had a continuity plan in place that was capable of maintaining acceptable retail payment-related customer service levels and were based on their business impact analysis that was relative to their retail payment system products and services. Privacy risk of e-wallets’ fund transfer had ensured that it was ranked high in the banks, and physical controls were in place that limited access to the staff assigned the responsibility of supporting e-payment operations. E-wallets exposed commercial banks to transaction risks from fraudulent activities, however, the banks had system measures in place that verified the authenticity of the payer and transaction information integrity.

5.5 Recommendations

5.5.1 Recommendations for Improvement

5.5.1.1 Card Payments and Operational Risk Management of Commercial Banks
The study recommends the commercial banks in Nairobi to ensure that they put in place strategies to manage the credit and liquidity risks that come from settlement of retail payments of these cards, by preparing themselves for issues that may arise from incomplete settlements, by setting aside funds to cater of these needs when they do arise.

5.5.1.2 Electronic Cash and Operational Risk Management of Commercial Banks
The study recommends the commercial banks in Nairobi to put in place a system that captures the complete audit trail of all electronic transactions at all times. This would allow the banks to pin point the source and exact quantity of any counterfeit and
fraudulent transaction that may take place within their networks, and thus avert dire consequences of these transactions.

5.5.1.3 E-Wallets and Operational Risk Management of Commercial Banks
The study recommends the commercial bank managers in Nairobi to ensure that they put in place appropriate logical controls over their internal staff, as well as contracted third-party service providers who responsible for retail payment-related services. This would ensure that they limit to a great extent their ability to encounter fraudulent activities, as well as shield themselves from legal ramifications that may occur from system breaches.

5.5.2 Recommendations for Further Studies
This study focused on the effect of e-payments on the operational risk management of commercial banks in Nairobi. The study therefore recommends that similar studies be conducted on other commercial banks within the country, this would provide a better overview of the effect of e-payments nationwide.
REFERENCES


APPENDICES
APPENDIX I: QUESTIONNAIRE

The aim of this questionnaire is to provide an answer to the effect of e-payments on operational risk management in the Kenyan banking industry. Please fill the questionnaire appropriately and do not that the information gathered is for academic purpose only.

Section 1: Demographics

1. Please indicate your gender.
   Male [ ] Female [ ]

2. Please indicate your age bracket.
   26-30 Years [ ] 31-35 Years [ ] 36-40 Years [ ] 41-45 Years [ ]
   46 Years and Above [ ]

3. Please indicate your position in the bank.
   Senior Manager [ ] Middle-Level Manager [ ] Low-Level Manager [ ]

4. Please indicate the section/department in the bank.
   Branch Manager [ ] Compliance [ ] Information & Technology [ ]
   Operations [ ] Finance [ ] Retail Banking [ ]
   Corporate Banking [ ] Risk [ ] Legal [ ]
   Other [ ] __________________________________________________________

5. For how many years have you worked in the bank?
   Less than 5 Years [ ] 6-10 Years [ ] 11-15 Years [ ]
   16-20 Years [ ] 21 Years and Above [ ]

6. Please indicate the highest level of education you have attained.
   College Diploma [ ] Bachelor’s Degree [ ] Master’s Degree [ ]
   Doctorate [ ] PhD [ ]
   Other [ ] __________________________________________________________

63
Section 2: Card Payments and Operational Risk Management of Commercial Banks

7. Using the scale 1-5 where 1 = strongly disagree and 5 equals strongly agree, please rate the following statements on card payments and how they affect operational risk management in your organization.

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our bank has a wide range of plastic money that our customers can make use of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bank relies on third-party service providers to conduct card payment processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bank competes with nonbank entities to provide retail payment services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expanding card services significantly increases our potential operational risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail payment-related systems affect the reputation of the bank in terms of meeting regulatory and consumer protection obligations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bank is responsible for risks associated with the activities of the third-party service providers we contract</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When using a third-party service provider, the bank is responsible for the credit risk exposure of the services being performed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deferred settlements present a risk for the bank that the paying institution or intermediate party may fail before the inter-institution settlement occurs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bankcards have specific procedures for amounts disputed by the cardholder and “charged back” or reversed out of the merchant’s account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bank allows corporate customers to incur intraday or “daylight” overdrafts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section 3: Electronic Cash and Operational Risk Management of Commercial Banks

8. Using the scale 1-5 where 1 = strongly disagree and 5 equals strongly agree, please rate the following statements about e-cash and how they affect operational risk management in your organization.

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our bank has developed electronic cash payment instruments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The bank provides options for pre-funded accounts that facilitate the ability to use online auction payments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic money represents liabilities on the balance sheet of the bank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The value of electronic money can diminish if the liabilities of the issuer are higher than the value of the assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liquidity risk in the payment system may arise from our inability to meet our obligations when they are due</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liquidity problems result in opportunity costs for the bank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our banking scheme has the ability to detect counterfeits and fraud in the system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our banks’ electronic money units are transferable from customer to customer without the transactions being subsequently recorded by the issuer or a clearing system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal disputes that occur, cause systemic risk to our payment systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The bank has a legal measure that ensures we have complied with laws and regulations pertinent to e-payment systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section 4: E-Wallets and Operational Risk Management of Commercial Banks

9. Using the scale 1-5 where 1 = strongly disagree and 5 equals strongly agree, please rate the following statements about e-wallets and how they affect operational risk management in your organization

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>The bank provides a digital wallet where customers make money transactions and payments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>We have outsourced retail payment-related services to third parties to enhance the services we perform in-house</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bank has adequate due diligence processes that monitor our service providers for compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bank maintains effective control over customer and financial institution information accessed by our service providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The bank has a continuity plan in place that is capable of maintaining acceptable retail payment-related customer service levels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The bank has a business continuity plan in place that is based on our business impact analysis that is relative to our retail payment system products and services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy risk of e-wallets’ fund transfer has ensured that it is ranked high in the bank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The bank has physical controls in place that limit access to the staff assigned the responsibility of supporting e-payment operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-wallets expose our bank to transaction risks from fraudulent activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our bank has system measures in place that verify the authenticity of the payer and transaction information integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

THE END
APPENDIX II: NACOSTI RESEARCH PERMIT

This is to certify that Mr. Simon Mwangi of United States International University Africa, has been licensed to conduct research in Nairobi on the topic: The Effect Of E-Payments On The Operational Risk Management In The Banking Industry: A Case Of Commercial Banks In Kenya for the period ending: 25/July/2020.

License No. NACOSTI/P/19/261

Applicant Identification Number

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.