CASHLESS ECONOMY TECHNOLOGIES, TRANSACTION VALUE AND FRAUD OCCURRENCE: THE CASE OF VENDORS IN NAIROBI

NKINI, DEBORAH GILLIARD

A RESEARCH THESIS TO BE SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF COMMERCE OF STRATHMORE UNIVERSITY

JUNE, 2025

Declaration

I hereby declare that this thesis has not been previously submitted for the award of a degree at this or any other university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person, except where proper citation is made within the thesis itself.

Name of Candidate: Nkini, Deborah Gilliard

Student No: 171739

Signature:  Date: 23/04/2025

Approval

The thesis of Nkini Deborah Gilliard was reviewed and approved by

Name of Supervisor: James Ndegwa

Signature:  Date: 25/04/2025

Acknowledgment

I am deeply grateful to God Almighty for the courage and determination that saw me through the completion of this thesis. I would also like to extend special thanks to my supervisor for their invaluable guidance. Additionally, I am profoundly thankful to my family for their unwavering support and care.

Abstract

Fraud remains a significant concern for Kenyan businesses, with small and medium-sized vendors frequently reporting incidents. While the adoption of cashless payment systems has improved convenience and efficiency, it has also introduced vulnerabilities that expose businesses to fraud. The economic sustainability of vendors and trust in cashless systems are critical; however, the factors driving fraud within this context remain insufficiently explored. This study examined the effect of cashless payment technologies on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, with transaction value as a moderating factor. The objectives were to assess the effects of mobile money, credit cards, cheques, and bank transfers on fraud diamond fraud occurrence and to analyse the moderating role of transaction value. Guided by the Fraud Triangle Theory and Routine Activity Theory, the study adopted a positivist research philosophy and employed a descriptive research design. The target population comprised vendors operating fuel stations, grocery shops, supermarkets, and restaurants. Data was collected using structured questionnaires featuring Likert-scale questions aligned with the study objectives. Analysis was performed using SPSS Version 27, with descriptive statistics summarising key data characteristics and binary logistic regression applied to infer relationships. The results indicated that all four cashless payment methods, mobile money, credit cards, cheques, and bank transfers significantly increased the likelihood of fraud. Furthermore, transaction value significantly moderated this relationship, with higher-value transactions more susceptible to fraud across all cashless payment methods. The study concluded that a strong, positive relationship exists between cashless payment technologies, fraud occurrence, and transaction value. The study recommended that policymakers implement stringent regulations for cashless platforms to mitigate fraud risks. Future research should explore advanced technologies such as blockchain, AI, and machine learning to enhance fraud prevention. Additionally, further investigation is needed into the relationship between transaction value and fraud across various industries and vendor types.

List of Figures

List of Tables

Table of Contents

VT OMNES
VNVM SINT

Definitions of Terms

Cashless Economy: A cashless economy refers to a financial system in which transactions are conducted electronically rather than using physical currency. This is facilitated by methods such as mobile money, credit cards, and electronic transfers, offering benefits like convenience, security, and cost-effectiveness (Rochemont, 2020; Schachter, 2019).

Mobile Money Payments: Mobile money payments involve the use of mobile phones to transfer money or pay for goods and services electronically. In Kenya, mobile money platforms like M-Pesa have become significant due to their accessibility and role in financial inclusion (Jumba & Wepukhulu, 2019; Kimani & Sirera, 2019).

Credit Card Payments: Credit card payments refer to transactions conducted using a credit card issued by financial institutions, enabling users to purchase goods and services on credit. While convenient, credit cards are susceptible to fraud risks, such as skimming and phishing, which necessitate robust security measures (Solat, 2017; Tade & Adeniyi, 2020).

Fraud Occurrence: Fraud occurrence refers to incidents of deceit or criminal activity intended to gain unauthorized financial benefits. Common fraud methods include identity theft, phishing, and payment-related scams, which have increased with the adoption of cashless payment systems (Ali, 2019; Transparency International Kenya, 2022).

Transaction Value: Transaction value refers to the monetary amount involved in a payment. It is a critical factor in understanding fraud dynamics, as larger transactions often attract more sophisticated fraud attempts, while smaller ones might be targeted more frequently (Ezeanolue, 2022; Katela, 2017).

VT OMNES
VNVM SINT

List of Acronyms and Abbreviations

CBK - Central Bank of Kenya

C2C - Consumer-to-Consumer

ICT - Information and Communication Technology

KYC - Know Your Customer

M-Pesa - Mobile-Pesa (Kenyan mobile money transfer service)

NACOSTI - National Commission for Science, Technology and Innovation

SMEs - Small and Medium-sized Enterprises

SPSS - Statistical Package for Social Sciences

SU-ISERC - Strathmore University Institutional Scientific and Ethical Review Committee

CHAPTER ONE: INTRODUCTION

1.1 Background to the Study

1.1.1 Fraud Occurrence

However, the rise of cashless economies worldwide has been accompanied by a surge in fraud attempts (Ali, 2019). Globally, highly developed payment market in Sweden, United States and India consists of cards including mobile phones which directly competes with cash. The losses from cash related frauds are higher than those from card related ones. Also, expensing solutions and serving electronic payments cost cheaper than fifty percent of that of cash operations. Therfore, the electronic payment methods are not as secure as the cash payment it is not private or independent in a way that the cash payment is (Iyer, 2017).

In Asia, cashless transactions is discovered to have a great and negative effect on in-store fraud in Indonesia. Factors such as police and security, and technology, boost the efficiency of the non-money exchange transactions. In addition, it found that the use of non-monetary transactions also moderates the relationship between the presence of law enforcement and protective measures, on the one hand, and the decrease in fraud in local government expenditure on the other, although the technological variable in this study did not (Dewi & Abdullah, 2021).

In Africa, one major challenge of the growing cashless society, especially in Nigeria, is the constantly emerging problem of electronic payment fraud or e-fraud. The fact that fraud is present in any financial framework means that there are existing issues and weaknesses that are being utilized by fraudsters. This underscores the importance of trust governance in electronic payment and the pivotal position of trust governance in the Nigeria's journey to a cash-less society (Tade & Adeniyi, 2020).

In Kenya, Transparency International Report of 2022 report estimated fraud prevalence in Kenyan businesses was 46.7% in the public sector, 20% in the private(large) businesses and 33.3% in the private(small/medium) businesses. This report shows that vendors in Nairobi who fall under the private(small/medium) businesses are at a high risk of experiencing fraud when conducting business transactions, especially with the advent of a cashless economy (Kithembe, 2023).This is shown in Figure 1 below.

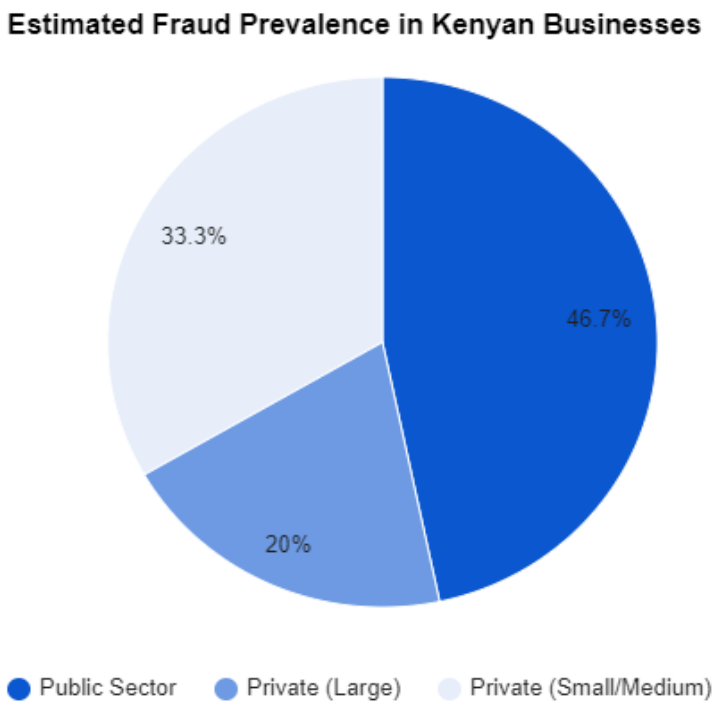

Figure 1.1: Estimated Fraud Prevalence in Kenyan Businesses
Source: (Transparency International Kenya,2022)

While recent years witness a burgeoning interest regarding fraud in C2C cashless sectors, the literature remains relatively scarce to the best of the researcher's knowledge with notable conceptual, contextual and empirical gaps. Conceptually, while articles like Iyer (2017) and Dewi and Abdullah (2021) have explored some facets of fraud like technology and mechanism of governance no research has made efforts to understand how much such characteristics influence the acceptance of the various forms of cashless payment. This fragmented approach lacks integration, which this study redresses by analyzing the broad technologically supported, security enhanced, government advanced, and collectively coordinated effects on fraud reduction in cashless economies.

Contextually, many of the research on effect of cashless transactions on fraud were carried out in developed countries with well-developed technological and legal systems such as Sweden and United States of America (Ibid, Ali, 2019; Iyer, 2017). These results may not be indicative of the Kenya scenario where the level of technology is not so advanced, and the general economic and legal environment is different. More so, despite Tade and Adeniyi (2020)

examining electronic payment fraud in Nigeria, little is known about the vendor sector in Kenya. This research aimed to fill this contextual void by exploring fraud within the Kenyan environment and among vendors that operate in Nairobi.

Empirically, literature points out ambiguity about cashless payment work on increasing or manipulating the rates of fraud. For example, Dewi and Abdullah (2021) argue that risk-free is attained through Swedish integrations for cashless transactions and Tade and Adeniyi (2020) argue that constant susceptibility is realized. These disparities suggest the need for more recent and perhaps more relevant data, which this research thesis sought to offer by determining the effect of cashless economy technologies on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya.

1.1.2 Cashless Economy Technologies

The evolution of payment methods has been a significant driver of economic development, tracing back to ancient times when commodities like grains or livestock were used as mediums of exchange (Schachter, 2019). Over time, these were replaced by metal coins, which offered greater convenience and standardization. The introduction of paper money marked another leap forward, providing a more portable and divisible form of currency (Rochemont, 2020).In the modern era, cashless payment technologies have emerged as the latest development in this long history, propelled by advances in information technology and global connectivity (Schachter, 2019).

Cashless payment technologies refer to systems, tools, and methods that facilitate financial transactions without the use of physical cash (coins or banknotes) (Stavins, 2020). Several factors, including the capabilities of information technology, regulatory environments, and the participation of key financial institutions influence the shift toward a cashless economy (Rochemont, 2020). On a global scale, In the United States, credit cards have become the dominant cashless payment method, supported by widespread infrastructure and consumer adoption. The market for cashless transactions now includes credit cards, checks, debit cards, mobile money, and electronic transfers, all of which offer benefits such as convenience, security, speed, and cost-effectiveness (Balaji & Balaji, 2017).

In Africa, for instance, mobile money has revolutionized the way financial transactions are conducted, particularly in regions with limited access to traditional banking services. In Ghana, the adoption of various cashless payment methods has fostered competition and consumer

choice, enhancing the overall payment experience (Otibo-Addo, 2021). In Kenya, mobile money services like M-Pesa have gained widespread acceptance, with 71% of businesses accepting digital payments and 56% of the population using mobile wallets. This trend contrasts with countries like South Africa and Nigeria, where cash still dominates, accounting for 91% and 94% of transactions, respectively (Kivuva, 2021).

Similarly, in Kenya, the Central Bank has actively promoted mobile money, which has become more prevalent than card payments (Jumba & Wepukhulu, 2019). This trend reflects a broader regional shift toward digital financial services, which are increasingly seen as essential for economic growth and financial inclusion. Businesses globally and locally are realizing the benefits of cashless payments, including increased customer satisfaction, enhanced cash flow, reduced operational costs, and improved customer relationship management (Kimani & Sirera, 2019). These advantages are driving businesses to integrate more cashless options into their operations, contributing to the broader digital transformation of the economy. The role of information and communication technology (ICT) in this transformation is undeniable, as it continues to shape the way societies transition from traditional to digital economies (Salehan, Kim, & Lee, 2018).

The rise of cashless payments is particularly evident in sectors such as food and accommodation, media and entertainment, travel and hospitality, farming and agriculture, transport and logistics, and professional services, where digital payments have become increasingly common (Kivuva, 2021). As businesses and consumers continue to embrace these technologies, the cashless economy is likely to expand further, driving innovation and competitiveness in the global market (Katela, 2019).

Though cashless payment technologies are on the rise both globally and regionally, there are existing research gaps in the areas of concept, context and methodology. On a conceptual level, whereas research by Kanyaru & Kyalo (2018), Kimani & Sirera (2019), and Kivuva (2021), have focused on individual effects of mobile money, credit card, cheque and bank transfer payments, their combined effects on the economy have not been analyzed. This lack of integration is problematic because the simultaneous use of these payment methods may introduce economies of scale or scope, which are unknown and ignored by this fragmented approach, and to fill this research gap, this study examined the combined effectiveness of these payment methods.

Contextually, prior studies including Balaji & Balaji (2017), Evans and Schmalensee (2017), and Chavdarova (2021), have been achieved in developed nations with dissimilar technological, economic, and rules of regulatory legibility than the Kenyan context. These studies fail to consider conditions specific to the Kenyan environment, including lower technological development and contrasting legal environment. Although Mbiti and Weil (2016) provided empirical data on mobile money in Kenya, they failed to examine how and to what extent vendors adopt as well as derive benefits from multiple forms of electronic payment.

This study, however, seeks to address this contextual research gap by availing information unique to Kenya in terms of regulation on financial services and the main economic indicators. On a methodological level, prior research by Maake, Oino, & Awuor (2018) states that a high positive impact of mobile money on fraud, while Schachter (2019) reveals low effects. The same methodological shortcomings can be observed in credit card use research, including Stavins (2020), which highlights increased consumer expenditure at the same time, overlooking accessibility barriers in the development setting. Over such issues, this research used a descriptive research design supported by questionnaires to repair all these inconsistencies and offers consistent and contextual data.

1.1.3 Transaction Value as a Moderating Variable

Globally, the adoption of cashless payment technologies has brought about significant advancements in convenience and efficiency but has also raised concerns about fraud. Governments and financial institutions have responded with measures like enhanced Know Your Customer (KYC) norms, improved data encryption, and multi-factor authentication to mitigate fraud risks (Ali, 2019). Despite these efforts, the effectiveness of these measures often depends on transaction characteristics, such as the value of payments being processed.

In developing economies, the role of transaction value as a determinant of fraud risks remains underexplored. For instance, in India, research has linked awareness of digital payments among financially excluded groups, like street vendors, to reduced fraud risks, with business performance playing a moderating role (Panda & Sahoo, 2022). However, this leaves a conceptual gap regarding whether transaction value might serve as an equally influential moderating factor.

Africa presents a unique context for studying cashless payment systems, particularly in Nigeria and Kenya. A study in Nigeria highlighted that while larger transactions attract sophisticated fraud attempts, smaller transactions, though frequent, are less lucrative targets (Ezeanolue, 2022). However, this research largely focused on payment methods like internet banking and point-of-sale services, overlooking broader systems like mobile money transfers, which are widely used in regions like Kenya.

Kenya offers further insights into these dynamics. Research indicates that transaction value significantly influences the likelihood of fraud in cashless transactions (Katela, 2017). Larger transactions tend to attract advanced fraud schemes, while smaller transactions pose lower risks (Ali, 2019). However, existing studies often fail to address the distinct challenges faced by small-scale vendors in Kenya, whose economic and technological environments differ significantly from those in more developed countries.

This study aims to bridge this contextual gap by focusing on small and medium-sized vendors in Embakasi East Constituency, Nairobi. These vendors operate in an environment characterized by unique economic conditions, varying levels of technology adoption, and distinct legal protections. Moreover, this research addresses methodological gaps in prior studies, which often relied on secondary data, by collecting primary data to capture vendors' real-time experiences with cashless transactions and fraud.

1.1.4 Vendors in Nairobi

The advent of cashless payment systems has revolutionized the way financial transactions are conducted globally (Nurhasanah, 2020). Nairobi, Kenya's capital and largest city, serves as a microcosm of these dynamics. As the epicenter of economic activity and technological innovation in Kenya. Nairobi hosts a dense network of fintech, banks and mobile money services catering to diverse communities and businesses, including vendors from every sector of the economy (Wanjau, 2020).

With the increasing use of cashless transactions among vending businesses in Nairobi, there has been a significant shift away from traditional cash-based economies (Kimani & Sirera, 2019). This transition promises numerous benefits, including enhanced convenience, financial inclusion, and improved efficiency in financial transactions (Maake, Oino, & Awuor, 2018). However, alongside these benefits, there are also emerging challenges, particularly concerning

fraud and security vulnerabilities inherent in cashless payment systems (Otibo-Addo, 2021). The study was carried out in Embakasi East Constituency in Nairobi, as the uptake of cashless payment platforms by local vendors has increased, resulting in a significant shift away from the use of traditional cash payments. Nairobi is Kenya's capital city and hub of economic and technological action, and it offers a fascinating situation to study the contours of cashless payments (Wanjau, 2020). Due to the rise in the utilization of cashless payments among vendors in Nairobi, particularly in Embakasi East, there is more interest in acquiring knowledge of both the merits and demerits these vendors enjoy.

The transition to electronic payments promises advantages such as increased convenience, financial inclusion, and enhanced efficiency in transactions (Maake, Oino, & Awuor, 2018). These are, however, accompanied by emerging risks, the key among them being those related to fraud and security vulnerabilities inherent in electronic payment systems (Otibo-Addo, 2021). Given the massive growth in cashless payment transactions in the area, Embakasi East has been the focus of this study because it is a representative sample of the opportunities and challenges vendors in the area are likely to encounter when adopting digital financial systems. The study population is 30,000 vendors that work within the constituency (KNBS, 2024), which puts it in an optimal position to explore the effect of cashless payment systems on fraud incidents.

1.2 Statement of the Problem

Fraud remains a global challenge that significantly affects financial systems, with Kenya being no exception. Reports suggest that businesses in Kenya lose billions of shillings annually to fraud linked to cashless payment systems (Wanjau, 2020). According to Transparency International (2022), 33.3% of small and medium-sized businesses in Kenya, including vendors, report incidences of fraud. This high prevalence not only threatens the economic stability of vendors but also erodes public trust in cashless payment technologies a critical pillar of Kenya’s rapidly evolving cashless economy.

Prior studies conducted in India and Nigeria both examine how transaction size can moderate fraud risks (Panda & Sahoo, 2022; Ezeanolue, 2022), but disregard how fraud risks vary when mobile money, credit cards, cheque payments, and bank transfers are used simultaneously. Such examination of these aspects concurrently could provide new perspectives different from studying them one by one and relating to one technology only, thus overcoming another

theoretical limitation.

Furthermore, most past studies have focused on developed countries like the United States and Sweden (Ali, 2019; Iyer, 2017) whose technological and legal systems are way more advanced than the Kenyan context. This is because most developed countries have weak technological systems unlike the Kenyan market, which has relatively weak legal systems than their counterparts in developed countries, and their economic pressures may differ from those of developed countries. Still, within Kenya, several studies have addressed cashless payments, but few have targeted vendors or intermediate players, which are the backbone of economies, with complicated formal structures, ambiguous regulatory policies, and the highest turnover (Jumba & Wepukhulu, 2019; Katela, 2019; Kimani & Sirera, 2019) therefore this research addressed this knowledge gap by determining the effect of cashless economy technologies on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya, with transaction value as the moderating factor.

Additionally, previous studies on cashless payment fraud have predominantly relied on secondary data (Ezeanolue, 2022; Solat, 2017). Such approaches may fail to capture real-time and context-specific dynamics experienced by vendors, especially in Nairobi's diverse economic landscape. This study addresses this methodological gap by collecting primary data directly from vendors to provide a more nuanced understanding of the relationship between cashless payment technologies and fraud occurrences. Given these research gaps, this study sought to provide a comprehensive analysis of how various cashless payment technologies influence fraud occurrence among vendors in Nairobi.

1.3 Objective of the Study

1.3.1 General Objective

To determine the effect of cashless economy technologies on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya, with transaction value as the moderating factor.

1.3.2 Specific Objectives

The study had the following specific objectives:

1. To assess the effect of mobile money payments on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya.
2. To examine the effect of credit card payments on fraud occurrence among vendors in Nairobi, Kenya.
3. To investigate the effect of cheque payments on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya.
4. To assess the effect of bank transfer payments on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya.
5. To assess the moderating effect of transaction value on the relationship between the cashless economy technologies and fraud occurrence among vendors.

1.4 Research Questions

The study sought to address the following research questions:

1. What is the effect of mobile money payments on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya?
2. What is the effect of credit card payments on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya?
3. What is the effect of cheque payments on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya?
4. What is the effect of bank transfer payments on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya?
5. How does the transaction value moderate the relationship between a cashless economy and fraud occurrence among vendors?

1.5 Scope of the Study

This study was geographically focused on the Embakasi East Constituency, Nairobi, specifically targeting vendors within this region. The study was conducted within a specific time frame, from February 2025 to March 2025. The total sample size was 379, with 95 vendors sampled from each of the four business categories using stratified sampling. The respondents included business owners, managers, and other relevant personnel responsible for handling

transactions and managing fraud risks within these businesses.

1.6 Significance of the Study

The significance of the study was discussed in contributions to theory, policy, and academia. This study therefore seeks to contribute to the theoretical understanding of the connection between the cashless economy and fraud occurrence. Decoding various forms of cashless transactions including mobile money, credit cards, cheques, and bank transfers, and the effects of the same on fraud occurrence, this research offers a framework that identifies how various modes of cashless transaction influence the occurrence of fraud among vendors. Further, it brings in the moderating variable transaction value as a new dynamic that defines the probability and characteristics of fraud based on transaction sizes. Thus, this theoretical contribution can complement the currently available theories on fraud deterrence and the adoption of new technology.

The implications of this research can be used in policymaking to come up with better policies that are effective in placing stricter deterrence mechanisms on fraud. Knowing how the cashless payment system affects fraud can assist the policymaker in formulating policies and measures to address or mitigate these effects. Moreover, findings on how payment quantity moderates cashless transactions and fraud helped to understand how to apply different tiers of security where transactions involving higher amounts are more likely to be exposed to fraud.

This study contributes academically by filling a gap in the existing literature on cashless economies and fraud. As highlighted in past literature, numerous studies have investigated specific dimensions of cashless transactions, though none of the studies have extensively assessed the effect of a cashless economy on fraud occurrence among vendors in Embakasi East Constituency, Nairobi County. Due to this study's focus on Embakasi East Constituency, Nairobi County, the findings can be generalized and related to current general trends in cashless economies, complementing the extant literature in the field. In addition, adding transaction value as a moderating variable provides a direction for future research, which makes it diverse and unique. Therefore, the findings of this study were useful for researchers and academia.

Lastly, the study contributed to business practice by offering practical implications for the business, especially to SMEs acting as vendors in Embakasi East Constituency, Nairobi. The vendors were able to identify the security threats that are inherent in the various electronic

cashless payment techniques and how transaction amounts impact the fraud strength. With this knowledge in check, vendors can afford to apply appropriate fraud-fighting measures such as implementing payment techniques that are much more secure or even increasing supervision on transactions that are considered to be riskier. Further, these findings can be useful to vendors in influencing consumer trust and assured payments for the reasons of firm reputation and business outcomes.

1.7 Chapter Summary

This chapter provided an overview of the study, including the background, problem statement, objectives, research questions, scope, and significance. The following chapters delved deeper into the literature review, research methodology, data analysis, and findings.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter presented the literature on which this study is built, it contains the theoretical foundation, empirical literature review, summary of knowledge gaps, conceptual framework, operationalization of study variables, and chapter summary.

2.2 Theoretical Framework

This study was anchored on the fraud diamond theory, the fraud triangle theory and the routine activity theory. Theories used in this study are selected according to their applicability in the study. The selected theories Fraud Diamond Theory, Fraud Triangle Theory, and Routine Activity Theory are all provide alternative yet complementary perspectives on fraud, and thus they are appropriate for a deeper exploration of the phenomenon. By combining these three theories, this research is offering a multi-dimensional method for studying fraud. Utilized in conjunction with each other, these theories offer a complete means of examining fraud and are therefore highly relevant to this research (Chukwuekwu, 2024).

2.2.1 Fraud Diamond Theory

The Fraud Diamond Theory, developed by David T. Wolfe and Dana R. Hermanson in 2004, expands on the earlier Fraud Triangle Theory by introducing a fourth element: capability. Taking the place of pressure, opportunity and rationalization, the Fraud Diamond puts forward a notion that to commit fraud, a perpetrator must also have the capacity and ability to implement the fraud and cover it up (Hermanson & Wolfe, 2024). Capability is regarded as another variable that defines the difference between those who could potentially embezzle, and those who carried it out and got away with it, which draws attention to aspects like high IQ, conning, programming aptitude and authorization to infiltrate the loopholes (Hermanson & Wolfe, 2024).

The theory's addition of capability also provides a more extensive view, especially in comprehending various kinds of comprehensive and intricate frauds. For instance, in cashless payment tools like mobile money, credit cards, or even transfers via banks, fraudsters may need expertise in the technology used to perform the fraud appropriately. This makes the theory particularly relevant to modern-day fraud types like cyber fraud because criminals take

advantage of existing technology and systems (Hermanson & Wolfe, 2024).

An advantage of using the Fraud Diamond is that it can be used in practical fraud prevention. Finding out the right people who possess the risk for fraud can help organizations to apply certain controls to reduce risks. Additionally, the theory gives a broader view by recognizing the relations between all of the four factors of fraud. However, their emphasis is directed to individual actors thus sometimes it may fail to consider broader systematic or organizational structures that make fraud possible. Furthermore, concerning capability as one of the key factors the theory suggests, there is a danger of focusing on capability obscuring the other factors, for example, poor internal controls, or failure to adhere to regulation (Mansor & Abdullahi, 2019).

Fraud Diamond Theory can be applied when explaining some of the variables in this study. It focuses on what is possible regarding opportunity-related factors like weaknesses in cashless transaction systems and how the abilities, or possession of specific tools such as technical skills or privileged access, make fraud possible. It also explains pressure-based attitudes, including financial incentives that could be pressed to prompt the fraudster, and rationalization that can be pressed to justify fraud. The capability dimension, in particular, enriches the understanding of how the offenders take advantage of the vulnerabilities in the processes of digital payments that constitute a common characteristic of the cashless economy, which is of particular relevance to fraud (Mansor & Abdullahi, 2019).

Several studies have applied the Fraud Diamond Theory to real-world contexts. For instance, Okoye and Gbegi (2013) used the theory to evaluate fraud prevention strategies in Nigerian banks, emphasizing capability as a significant factor in occupational fraud. Similarly, Chong and Liu (2019) applied the theory to analyze cyber-related financial fraud, focusing on skilled hackers who exploit digital payment systems. In Kenya, Ndede-Amadi (2021) examined employee fraud using the Fraud Diamond, highlighting how capability allowed insiders to bypass even robust systems.

While the Fraud Diamond Theory has been widely applied, several gaps remain. One issue is the lack of focus on organizational culture, which influences employees' propensity to commit fraud (Okoye and Gbegi, 2013; Chong and Liu, 2019; Ndede-Amadi, 2021). Many studies focus on individual elements without considering how cultural factors, like weak controls or

tolerance for minor ethical breaches, contribute to fraudulent behavior.

Additionally, external socioeconomic pressures, such as poverty and economic instability, are often overlooked, despite being significant drivers of fraud, especially in developing countries (Okoye and Gbegi, 2013; Ndede-Amadi, 2021). The theory also struggles to adapt to digital and cyber fraud, which involves different dynamics, such as anonymity and technological capability (Chong and Liu, 2019). In the context of this study, the Fraud Diamond Theory provides a comprehensive framework for assessing fraud occurrence among vendors in Embakasi East Constituency, Nairobi's cashless economy.

By examining how capability interacts with pressure, opportunity, and rationalization, the study aims to uncover how skilled fraudsters exploit cashless systems, such as mobile money and credit cards. Additionally, the moderating variable of transaction value can provide insights into how transaction sizes influence the likelihood and nature of fraud. The theory's focus on capability makes it especially relevant for understanding modern fraud dynamics in cashless economies, where technological expertise plays a crucial role.

2.2.2 The Fraud Triangle Theory

The Fraud Triangle Theory, developed by Donald R. Cressey in 1953, explains that for fraud to occur, three conditions must be met: pressure, opportunity, and rationalization. This theory offers a good platform to explain how the technologies in the cashless economy can affect the incidence of fraud amongst the Embakasi East Constituency, Nairobi vendors. Pressure is realised when business incomes reduce and impose financial constraints on vendors. For instance, personal debts or financial recuperation may impose some pressure on the vendors, who subsequently regard fraud as a way of releasing the burden (Katela, 2019). Such pressures, thus, may be magnified where there are increased competitive pressures and organizations' operational openness: pressures that may force vendors into embracing fraud to boost their residual income (Hedman & Henningsson, 2019).

An opportunity arises when people use cashless technologies, which entail some risks, such as hacking or exploiting cashless payment systems (Levi, 2019). For instance, computer hackers might trespass into computer systems, performing unlawful activities such as unauthorized transactions (Otibo-Addo, 2021). Suppliers may also alter details of the transactions, for

example, where the use of digital money transfers does not have secure means to prevent altering transaction records. On the other hand, in a cash-basis method, a vendor may record low sales because when giving change, there is no record trail, which can be used to assess taxes (Mtonga, 2023). Another example is the employees of the cash transport firms in Kenya who have been implicated in the theft of cash in transit (Ali, 2019).

The application of the Fraud Triangle Theory in cashless economies reveals several research gaps and their theoretical implications. One gap is the theory's limited focus on cybercrime, which often involves complex networks exploiting digital vulnerabilities. Studies by Ategeka (2021) and Mansor & Abdullahi (2019) suggest that the theory should be expanded to incorporate networked fraud, reflecting the collective nature of cybercriminal activity. Another gap is the oversimplification of opportunity, as fraud in cashless systems often exploits technological flaws, such as weak encryption or insider threats, as noted by Kassem (2022). This indicates the need to refine the theory's understanding of opportunity, considering technical and operational vulnerabilities.

Additionally, the theory overlooks the impact of transaction value on fraud, as larger transactions may increase the temptation for fraud, a factor highlighted by Mtonga (2023). Integrating transaction value as a moderating factor would provide deeper insights into how transaction size influences fraud risks. The theory also fails to account for organizational factors such as management practices and internal controls, which play a critical role in fraud. Studies by Katela (2019) and Otibo-Addo (2021) suggest that broader institutional influences should be integrated into the framework.

Moreover, the theory neglects psychological and sociocultural factors, which affect rationalization and decision-making. Kassem (2022) and Katela (2019) show that societal norms and peer influences can normalize fraudulent behavior, highlighting the need to integrate psychological and cultural insights into the theory. Lastly, as advanced fraud detection technologies evolve, the role of oversight in creating opportunities for fraud needs reassessment. Research by Ali (2019) and Otibo-Addo (2021) suggests that fraud detection systems could also present new opportunities for fraud, indicating the need to expand the theory to include digital oversight. Addressing these gaps would refine the Fraud Triangle and make it more relevant to modern cashless economies.

Despite its limitations, the Fraud Triangle Theory offers a useful framework for understanding how cashless economy technologies may create opportunities for fraud, particularly in environments where financial pressures are high and oversight is inadequate. This study applies the theory to explore the influence of cashless payment systems such as mobile money, credit cards, cheques, and bank transfers on fraud occurrence among vendors in Embakasi East Constituency, Nairobi. Furthermore, it incorporates transaction value as a moderating variable to understand how transaction sizes interact with these fraud-enabling conditions.

2.2.3 Routine Activity Theory

Routine Activity Theory, developed by Lawrence Cohen and Marcus Felson in 1979, postulates that crime occurs when three elements converge: a motivated offender, a suitable target, and a lack of capable guardians. This theory can be useful in analyzing fraud in the light of a cashless society since digital transactions offer ready grounds for the would-be offenders. According to Mohammad & Nooraini (2021), socio-technical incentives for motivated offenders in a cashless society include cybercriminals, hackers, and other fraudulent entities. These offenders are attracted to the growing cash-based flows across online platforms since the high risks of scams characterize them. Digital platforms may not have adequate protective measures compared to other platforms. Therefore, such platforms might attract persons intending to perpetrate cyber-related crimes like phishing or even identity theft, as noted by Payne et al. (2020).

According to Jumba & Wepukhulu (2019), many cashless payment systems lack adequate digital security measures. Therefore, vendors might be good acquisition candidates as they embrace cashless payment methods without realizing the potential dangers. The shift to using electronic cash increases their vulnerability to fraud in various forms, such as unauthorized electronic transactions and electronic theft (Levi, 2019). Factors such as insufficient training and guidance to identify cases of fraud and prevent them make vendors vulnerable (Schreck, 2017).

Prior studies have applied the Routine Activity Theory to study fraud in different contexts and, in the process, found different gaps in its application. Payne et al. (2020) examined cyber-based fraud in a cashless society, identifying the lack of guardianship, such as encryption, as a vulnerability. However, routine activity theory focuses on individual-level interactions, fails to

capture the global, multi-agent nature of cybercrimes, suggesting the need for a broader framework that includes institutional and global responses to complex fraud schemes.

Similarly, Mohammad & Nooraini (2021) explored the socio-technical incentives of criminals in a cashless society, focusing on individual motivations. The study overlooks emerging technologies like artificial intelligence, which influence criminal strategies. This reveals a gap in routine activity theory, as it does not fully account for technological advancements, highlighting the need for the theory to integrate technological factors into its framework to better explain modern fraud. Jumba & Wepukhulu (2019) studied vendor vulnerabilities in Kenya's cashless economy, noting a lack of training, but failing to address structural issues like regulation and institutional support. This highlights the routine activity theory's limitation in neglecting organisational and institutional roles in fraud prevention, suggesting the theory needs to incorporate these elements for a more comprehensive understanding of fraud.

Levi (2019) analysed unauthorised transactions in cashless economies, focusing on vulnerabilities in digital payment systems. However, routine activity theory focuses on individual interactions and overlooks the complexity of coordinated, cross-jurisdictional cybercrimes, pointing to the need for a more systemic approach that includes organisational and international cooperation. Taherdoost (2021) criticised routine activity theory for lacking a systemic perspective, particularly in cybercrime prevention, as it overemphasises individual-level interactions and ignores the role of regulatory and organizational measures. This suggests that RAT would benefit from incorporating institutional and collective action to address modern fraud effectively.

Generally, these studies suggest that, routine activity theory needs to go beyond the level of individual interaction to include technological, institutional, and systemic factors so that it is in a better position to explain fraud complexities of the digital age. Nevertheless, the given theory helped elucidate to what extent motivated offenders, vulnerable vendors, and the lack of security measures can contribute to fraud in a cashless economy. Using Routine Activity Theory, this paper sought to determine the effect of cashless economy technologies on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya, with transaction value as the moderating factor. This analysis aims to understand the weaknesses within current

security measures and the opportunities available to improve the protection against fraud.

2.3 Empirical Review

2.3.1 Mobile Money Payment and Fraud Occurrence

Matthew and Mike (2019) discuss the impacts of a cashless economy on Nigeria's banking industry. While they did not pay specific attention to the hazard of mobile money, they identified that in all forms of digital transaction fraud risks, among them e-fraud, were more pronounced. The study focused on improving protection against fraud incidents based on Nigeria's analyzed mobile payment services.

On the other hand, Otibo-Addo (2021), employing both quantitative and qualitative cross-sectional surveys in Ghana, revealed that the strengths of the mobile money systems were ease of access and convenience, but the systems suffered from cyber threats and technology-related hitches. While Matthew and Mike found common ground on the potential weaknesses in mobile money systems, they, on the other hand, have different approaches Matthew and Mike pinpointed the financial system's structural flaws, whereas Otibo-Addo discussed the technical problems.

In contrast, Kivuva (2021) undertook an online survey of 350 participants in Nigeria, South Africa, and Kenya and found that mobile money was the most popular mode of payment, especially among transport and professional service providers. Nonetheless, mobile money was not without fraud risks, and merchants had to address the risk of fraud to reap the benefits of the cashless system. This contrasts Esperance (2024), who sampled Kigali's cashless society and proposed that mobile money still has flaws like privacy infringement and hacking. The mobile money technology in Kigali differs from that in Nigeria, Ghana, and Kenya, where mobile money is relatively mature but faces similar fraud challenges.

Similarly, Kimani and Sirera (2019) explored online banking fraud in Kenya and observed that mobile money is the most vulnerable area to fraud. The authors acknowledged that businesses must create better fraud prevention methods, including customer awareness and improved security measures. These conclusions echo the findings of Matthew and Mike (2019), who emphasized that regulatory measures are necessary to protect digital payment platforms.

2.3.2 Credit Card Payment and Fraud Occurrence

Multiple studies investigating the incidence of credit card fraud and the factors that contribute to it find that credit card fraud is still rife in the payment industry across the world. The study done by Kanyaru and Kyalo (2018) worked from the perspective of Kenya though its scope was majorly targeted towards internet fraud with more emphasis on credit card fraud. Their findings highlighted two primary factors enabling fraud: the systems that have relatively low-security arrangements and customers who are easy targets for phishing scams or fraud-related transactions. The researchers stated that e-commerce merchants simply could not afford to be as lax as they currently are with the security issues and that they need to use far more sophistication, such as increased encryption technologies, and increased customer awareness campaigns.

In the same way, when comparing credit card usage in Sweden, the United States, and India, Iyer (2017) found that the high rate of fraud correlates always with a country's cybersecurity systems. Iyer also established that there were lower levels of card-related fraud in countries that safeguarded their figures well, including Sweden which has a well-formulated security system. For instance, emerging markets such as India are sorely acquitting themselves poorly when it comes to cyber security and therefore fraud is relatively high, especially for online and card-present transactions. The study highlighted the importance of International Integration in security to reduce international risk factors in credit card fraud.

Similarly, Solat (2017) examined the security of traditional e-payment systems in the United Kingdom focusing on the security risks presented by credit card transactions. Solat's study showed that the failure the authenticate the credit card via a secure offline mode such as biometric verification or dynamic PIN makes users of credit cards vulnerable to fraud through swipe-based payment methods. To its credit, the research stressed that credit cards, being convenience products, pose considerable risks and security must be equally convenient to counteract the convenience that credit card companies offer. The following findings are in line with Iyer, for he also established a convenient-secure ratio in credit card payment systems.

Tade and Adeniyi (2020) have analyzed e-banking fraud mainly concerning the role of credit cards within the context of the cashless policies in Nigeria. They named poor governance structures which they attributed to fraud management as one of the major challenges to the current e-banking services. The research pointed out that most EU member states fail to

establish proper supervisory structures and information security standards to guarantee people's confidence and extend the use of credit card facilities across the country. The authors stressed the need to improve the existing regulation policies and escalate the fraud management to fill such loopholes.

On the other hand, Kimani and Sirera (2019) focused on the advantages and disadvantages of using credit card payment systems in Kenya. They went further to show that companies that implement credit card payment systems benefited from improved customer outreach and competitiveness in the market. Nevertheless, it also revealed that the achievement of these benefits poses high risks; this is, Internet fraud is still prevalent. As part of the study, it was pointed out that although credit card payments give businesses an edge, there is a need to incorporate modern techniques of fraud control and pursue the implementation of international standards on payment security.

2.3.3 Cheque Payments and Fraud Occurrence

Despite the declining popularity of cheques in cashless economies, research highlights that they remain a significant source of fraud in specific contexts. Jumba and Wepukhulu (2019) examined the financial performance of supermarkets in Nairobi and found that while cheque usage has decreased over time, it still plays a notable role in transactional fraud. Among the common types of cheque-related fraud identified were check-kiting, a practice involving the deliberate misuse of floating cheque funds, and forgeries, where counterfeit or unauthorized cheques are used to withdraw funds fraudulently. These findings align with those of Matthew and Mike (2019), who observed that even in economies transitioning to cashless systems, cheques must not be overlooked due to their persistent susceptibility to fraud.

Similarly, Esperance (2024) extended this discourse by investigating cheque fraud in Kigali's increasingly cashless economy. The study noted that although cheque usage has become infrequent in modern payment systems, it remains a viable medium for fraudulent activities. Esperance highlighted that businesses transitioning toward fully cashless modes of operation often experience a proportional decline in cheque-related fraud. However, the threat has not been entirely eliminated, especially in regions where cheques are still occasionally used for specific transactions or as a backup payment method. This insight demonstrates the need for vigilance, even in economies where cheques are seemingly on the verge of obsolescence.

Similarly, Kanyaru and Kyalo (2018) explored how cheque fraud impacts internet merchants and emphasized that businesses using traditional payment modes, including cheques, are particularly vulnerable to fraudulent schemes. They pointed out that while many firms have moved to digital payment systems, some sectors continue to rely on cheques for certain transactions, leaving them exposed to security risks. This study underscores the importance of maintaining fraud prevention mechanisms for cheques, even in the context of digital transformations.

In contrast, Mwabu (2018) offered a nuanced perspective by comparing cheque fraud with other forms of digital payment fraud in the Kenyan banking sector. The research found that while cheques are less prone to fraud than mobile money or credit card payments, they are not entirely immune. Mwabu noted that cheque fraud typically involves more traditional schemes, such as counterfeit cheques or unauthorized endorsements, which, though less prevalent, still pose a significant risk in certain sectors and regions.

2.3.4 Bank Transfer Payments and Fraud Occurrence

In a study by Otibo-Addo (2021) found that the hacking of banking transfer platforms was the most prevalent and damaging in their quest towards the adoption of a cashless economy in Ghana. It also revealed that hackers attack vulnerable banking transfer services, erode people's confidence in electronic payment technology, and delay the shift to a cashless society. Similarly, Misango et al., (2020) revealed mobile money Payments in Nairobi, Kenya were prevalent despite consumers using bank transfers for large transactions. However, these transactions were increasingly vulnerable to crime-related criminal activities because of a lack of decent measures. Examples cited as having contributed to this included weak encryption, lack of adequacy IT security and increased complexity by cyber criminals as a major challenge to both financial institutions and users.

The findings of this study are in consonant with the research conducted by Matthew and Mike (2019) in Nigeria where a questionnaire survey revealed extensive infrastructural and security drawbacks in the banking industry contributing to fraud in cashless bank transfer. In their studies, they found that although a bank transfer is comfortable and quick, weak security systems enable customers to deal with other tricks such as phishing, hacking, and fraud.

Consequently, the study called for the implementation of strong security controls that would help fill the identified systemic vulnerabilities and make customers trust digital financial services.

On the other hand, Kimani and Sirera (2019) have provided a different perspective on this in Kenya having established that businesses that were using bank transfers had relatively lesser rates of fraud as relapsed to mobile money or credit cards as the case was with the businesses in this study. In their study, they found that more stringent regulations and increased use of security technology in the banking systems may lead to decreased cases of fraud in bank transfers. Nevertheless, this conclusion is quite different from the findings of Otibo-Addo (2021) and Misango et al., (2020) who established a difference in the effectiveness of these controls in preventing fraud within the banking transfer systems of other nations. This discrepancy shows that many other factors play a crucial role in the fight against fraud including the role and functioning of the regulatory environment, technological resources, and users' conduct.

Moreover, working with data collected from the United Kingdom, Solat (2017) concluded that, although bank transfer is considered secure, the identified payment method is still exposed to fraudsters using sophisticated techniques like social engineering and phishing. These methods target human vulnerabilities and not computer flaws; they strongly indicate that while there should be a focus on the technological aspect of fraud control, much more effort should be channelled towards the other part of the control triangle, which is the user controls.

This research concurs with Kivuva (2021) who studied the role of digital payment systems in Kenya and observed in this technological advancement that bank transfers contribute significantly to the improvement of business with streamlined operations and cost savings, though they are not beyond the reach of fraudsters. Kivuva's study focused on the two-fold task of encouraging the use of digital payments while at the same time overseeing the change in methods adopted by hackers.

VT OMNES
VNVM SINT

2.4 Summary of Research Gaps

The literature review highlights several key research gaps in the field of cashless economies, digital payments, and fraud prevention. Empirical gaps include the lack of detailed analysis on the effectiveness of measures addressing infrastructural and cybersecurity challenges in Nigeria (Matthew & Mike, 2019) and the need for comprehensive data on the long-term economic impacts of cashless payments in various sectors (Kivuva, 2021). Theoretical gaps are found in studies like Otibo-Addo (2021), which calls for exploration of the technological and regulatory frameworks needed to mitigate cyber-attacks in Ghana, and Iyer (2017), which lacks examination of how cash-based economies can integrate emerging digital payment technologies.

Methodological gaps are noted in Esperance (2024) and Kanyaru & Kyalo (2018), where further research is needed to balance economic growth with privacy and security concerns in Kigali, and provide practical recommendations for enhancing security and customer education in Kenya. Contextual gaps, identified in Jumba & Wepukhulu (2019) and Misango et al. (2020), emphasize the need for research into how different payment technologies impact consumer behavior and the barriers to smart card adoption despite awareness. These gaps present valuable opportunities for future studies to deepen the understanding of cashless systems and improve their effectiveness and security. Table 2.1 below presents the summary of knowledge gaps identified from the literature reviewed.

Table 2.1: Summary of Research Gap

Study	Key Findings	Knowledge Gaps	Type of Gap
Matthew & Mike (2019)	Cashless policy in Nigeria provides benefits like increased convenience and reduced crime, but faces challenges like infrastructural deficits and e-fraud.	Lack of detailed analysis on the effectiveness of specific measures to overcome infrastructural and cybersecurity challenges.	Empirical
Otibo-Addo (2021)	Ghana is ready for a cashless economy but faces issues like high costs and cyber-attacks.	Limited exploration of the specific technological and regulatory frameworks needed to mitigate cyber-attacks and reduce costs.	Theoretical
Kivuva (2021)	High usage of digital payments in Nigeria, South Africa, and Kenya, with 69% of businesses reporting positive impacts.	Need for comprehensive data on the long-term economic impacts of cashless payments on various sectors.	Empirical
Esperance (2024)	Cashless financial services in Kigali contribute to economic growth but also increase privacy concerns and technological dependency.	Further research is needed on strategies to balance economic growth with privacy and security concerns.	Methodological
Jumba & Wepukhulu (2019)	Financial access and innovation influence the financial performance of supermarkets in Nairobi.	Additional research is needed on customer perceptions and the impact of different payment technologies on consumer behavior.	Contextual
Misango et al. (2020)	Industry pressure influences cashless payment adoption, with mobile phone payments being more popular than smart cards.	Need for a deeper understanding of the factors deterring the adoption of	Contextual

		smart card systems despite awareness.	
Iyer (2017)	Cash has lower losses than card instruments, providing more privacy and financial freedom.	Examination of how cash-based economies can be integrated with emerging digital payment technologies.	Theoretical
Tade & Adeniyi (2020)	E-banking fraud in Nigeria affects adoption, with banks implementing security features like SCAM alerts.	Investigation into the long-term effectiveness of these security features and the role of customer trust in e-banking adoption.	Empirical
Kanyaru & Kyalo (2018)	Internet fraud in Kenya is linked to poor security measures and a lack of customer awareness.	Need for more practical recommendations for online merchants to enhance security and customer education.	Methodological
Mwabu (2018)	Customer awareness and security controls significantly influence electronic fraud in Kenyan banks.	Further analysis is required on the impact of employee training and remuneration on fraud prevention.	Empirical

Source: Researcher (2025)

2.5 Conceptual Framework

The conceptual framework explores the relationships between independent variables and dependent variables and the moderating role of the moderating variable.

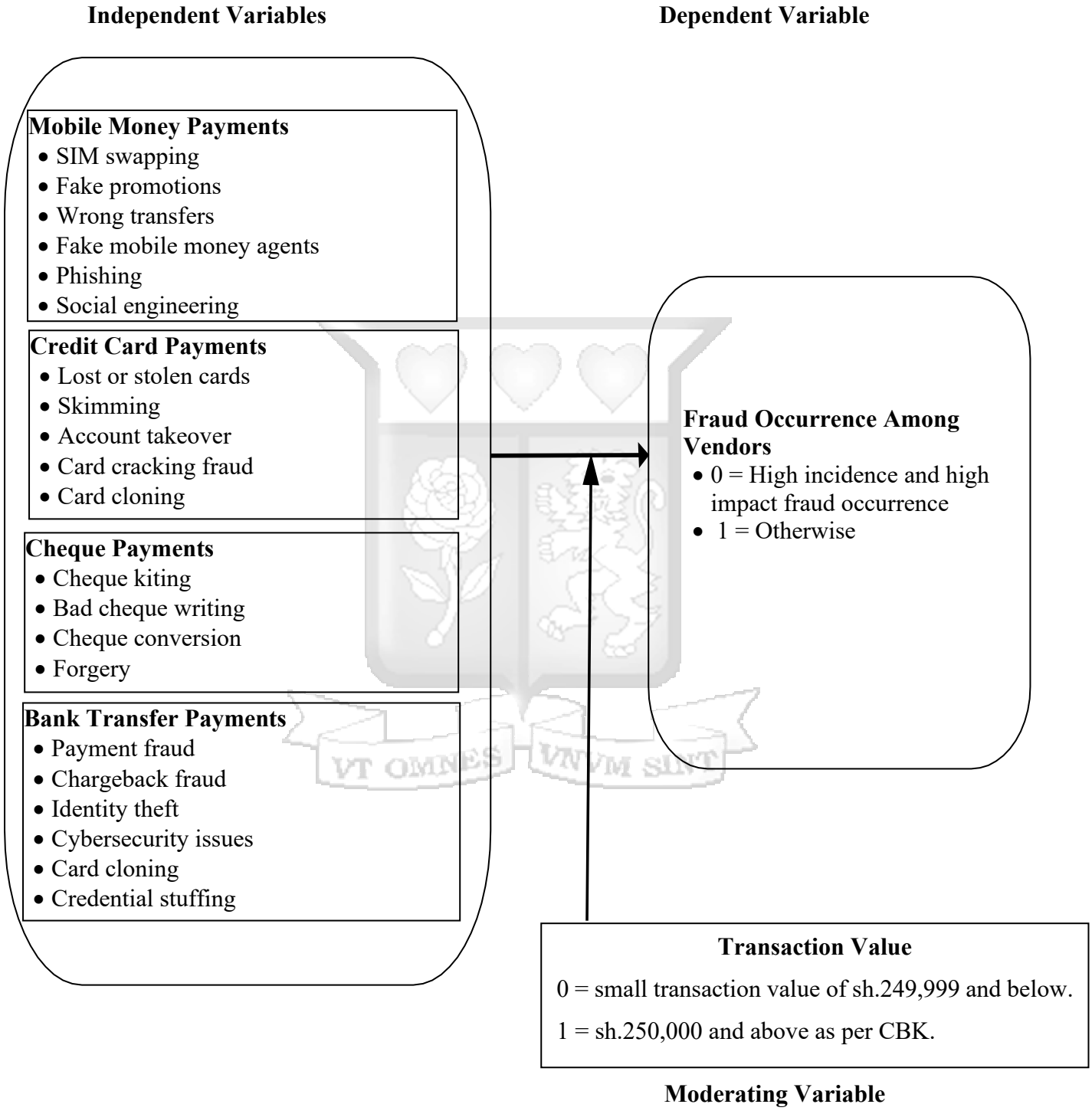

Figure 2.2:Conceptual Framework

2.6 Operationalization of Study Variables

Table 2.2: Operationalization of Study Variable

Variable and Indicator	Methodology	Measurement	Measurement Scale	Source
Independent Variable **1. Mobile Money Payments** • SIM swapping • Fake promotions • Wrong transfers • Fake mobile money agents • Phishing • Social engineering **2. Credit Card Payments** • Lost or stolen cards • Skimming • Account takeover • Card cracking fraud • Card cloning **3. Cheque Payments** • Cheque kiting • Bad cheque writing • Cheque conversion • Forgery **4. Bank Transfer Payments** • Payment fraud • Chargeback fraud • Identity theft • Cybersecurity issues • Card cloning • Credential stuffing	Quantitative, Close-ended questionnaires	Survey items rated (Frequency of use, amount transacted, user satisfaction) on a Likert scale (1-5).	Ordinal Scale	(Matthew & Mike, 2019) (Misangu,et al., 2020) (Jumba & Wepukhulu, 2019)
Dependent Variables Fraud Occurrence Among Vendors	Quantitative, Close-ended questionnaires	Survey items rated On a Binary scale. • 0 = High incidence and high impact fraud occurrence • 1 = Otherwise	Binary Scale	(Mwabu, 2018) (Tade & Adeniyi, 2020)
Moderating Variable **Transaction value**	Quantitative, Close-ended questionnaire.	Survey items are rated on a Binary scale. 0 = small transaction value of sh.249,999 and below. 1 = sh.250,000 and above as per CBK.	Binary Scale	(Otibo-Addo, 2021), (Kivuva, 2021)

VT OMNES
VNVM SINT

2.7 Chapter Summary

This chapter delved into the theoretical foundations and empirical studies related to the effect of a cashless economy on fraud occurrence among vendors in Embakasi East Constituency, Nairobi Kenya with transaction value as the moderating factor. It explores key theories such as the Fraud Triangle Theory and the Routine Occurrence Theory. Empirical evidence underscores the effect of a cashless economy on fraud occurrence among vendors in Embakasi East Constituency, Nairobi Kenya. The conceptual framework contained the relationship between variables and operationalizes them. The chapter concluded with a summary of these knowledge gaps, emphasizing the need for further research in diverse economic contexts.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter presented the methodology of the study. It contains the research philosophy, research design, population of the study, sampling design and technique, data collection methods, data quality, data analysis, and ethical considerations.

3.2 Research Philosophy

When selecting a research philosophy, four main approaches are typically considered: pragmatism, interpretivism, post-positivism, and positivism. This study adopted a pragmatist philosophy, which is flexible in combining both quantitative and qualitative methods to best answer research questions. Pragmatists are not committed to a single reality and select diverse techniques for data collection and analysis based on research objectives (Creswell, 2013; Christensen, 2022).

Interpretivism focuses on understanding subjective realities and the meanings individuals attach to their experiences, particularly in social settings (Pervin & Mokhtar, 2022). Post-positivism blends positivism and interpretivism, acknowledging an objective reality but recognizing that knowledge is always fallible. It encourages the use of both quantitative and qualitative approaches for a more comprehensive understanding of phenomena (Alharahsheh & Pius, 2020). Positivism, on the other hand, is rooted in the belief of an objective reality, relying heavily on quantitative data to establish patterns and generalizable findings.

This study adopts a positivist philosophy, which is well-suited for its focus on objective data and quantitative analysis. Positivism emphasises measurable and testable phenomena, enabling the study to explore relationships between variables systematically. The use of structured questionnaires with predominantly closed-ended questions aligns with this approach, ensuring consistency in data collection and facilitating numerical analysis to evaluate the effects of cashless payment technologies on fraud occurrence (Maksimovic & Evtimov, 2023).

The adoption of this philosophy is further justified by the study's focus on addressing specific gaps in understanding fraud dynamics within Kenya’s cashless economy (Alem, 2020). By employing a quantitative approach, the study objectively measures how different payment technologies (mobile money, credit cards, cheques, and bank transfers) influence fraud among

vendors (Munir, 2023). This methodology also allows for the testing of the moderating effect of transaction value, a critical factor often overlooked in prior research.

3.3 Research Design

Research design refers to the overall strategy or blueprint that a researcher uses to integrate the different components of the study coherently and logically, ensuring that the research problem is addressed effectively (Creswell et al., 2018). It outlines the methods, procedures, and techniques for collecting, analyzing, and interpreting data. The choice of research design depends on the research objectives, the nature of the problem, and the types of variables being investigated. Different designs include experimental, correlational, descriptive, mixed methods, and cross-sectional, each serving distinct purposes in the research process.

Experimental design is used to establish causality by manipulating independent variables and observing their effects on dependent variables, keeping other factors constant (Huntington-Klein, 2021). Correlational design, on the other hand, examines the relationships between variables without manipulation, focusing on identifying associations rather than causality (Huntington-Klein, 2021). Mixed research design combines quantitative and qualitative methods, offering a comprehensive approach to exploring a phenomenon in-depth while also measuring relationships between variables (Silver, 2016). Cross-sectional design provides a snapshot of a population or phenomenon at a specific point in time, useful for analysing correlations but not causality, as it doesn't track changes over time (Sheehan, 2010).

This study employed a descriptive research design, which is well-suited for understanding the characteristics and current status of phenomena without manipulating variables. Descriptive designs often utilize surveys, observations, or case studies to gather data, making them ideal for the use of questionnaires in this study (Creswell et al., 2018). This design aligns with the study's objectives of examining the effects of mobile money, credit cards, cheques, and bank transfers on fraud occurrence among vendors (Alharahsheh & Pius, 2020). By focusing on describing existing relationships and the moderating role of transaction value, the descriptive approach ensures a systematic and accurate representation of the phenomena under investigation. This methodology provides reliable insights essential for addressing gaps in fraud mitigation and advancing the understanding of cashless payment systems in Kenya (Pandey & Pandey, 2021).

3.4 Population of Study

The population of the study comprised 30,000 vendors operating in Embakasi East Constituency, Nairobi (KNBS, 2024).

3.5 Sampling Design and Technique

3.5.1 Sample Size

To determine the sample size, the study employed Mugenda and Mugenda (2013) formula since the population of the study is above 10,000.

$$n = \frac{Z^2 \cdot p \cdot q}{d^2}$$

Where:

- **n** = the desired sample size (if the population is greater than 10,000)
- **Z** = standard normal deviate (usually set at 1.96 for a 95% confidence level)
- **p** = proportion of the population assumed to have the characteristic being measured (typically 0.5 is used if unknown)
- **q** = 1 - p (which is also 0.5 in this case)
- **d** = the level of precision (the margin of error, often set at 0.05)

$$n = \frac{(1.96)^2 \cdot (0.5) \cdot (0.5)}{(0.05)^2}$$

$$n = \frac{3.8416 \cdot 0.25}{0.0025} = 384.16$$

So, the initial sample size was approximately 384.

Apply the finite population correction since the population is less than 10,000. The population in the study is 30,000 the researcher used the following formula for the adjusted sample size:

$$n_f = \frac{n}{1 + \frac{n-1}{N}}$$

Where:

- **n** = sample size from Step 1 = 384
- **N** = population size = 30,000

$$n_f = \frac{384}{1 + \frac{384 - 1}{30,000}}$$

$$n_f = \frac{384}{1 + \frac{383}{30,000}} = \frac{384}{1 + 0.01277} = \frac{384}{1.01277} \approx 379.16$$

Thus, the final sample size was approximately 379 respondents. The respondents included business owners, managers, and other relevant personnel responsible for handling transactions and managing fraud risks within these businesses.

3.5.2 Sampling Technique

The study used stratified sampling with a focus on those engaged in businesses such as fuel stations, grocery shops, supermarkets, and restaurants (Solat, 2017). These vendors were selected because they are heavily reliant on cashless payment methods, making them pertinent subjects for studying the relationship between cashless transactions and fraud (Bosibori, 2023). Table 3.3 shows the distribution of the sample size.

Table 3.3: Distribution of the Sample Size.

Strata's	**Sample Size**
Fuel Stations	95
Grocery Shops	95
Supermarkets	95
Restaurants	95

Thus, the total sample size was 379, with 95 vendors sampled from each of the four business categories using stratified sampling. The respondents included business owners, managers, and other relevant personnel responsible for handling transactions and managing fraud risks within these businesses.

3.6 Instruments of Data Collection

In this study, primary data was used. The primary data for this study were collected through questionnaires (Longwe, 2010). This study gathered in-depth information through questionnaires designed with closed-ended questions. The questionnaire was predominantly designed with closed-ended questions in a Likert scale format to collect quantitative data (Batterton & Hale, 2017). The questionnaires were subdivided into six sections. Section 1 of the questionnaire captures the demographic details of the respondents, Section 2 covers mobile money payments and fraud occurrence among vendors, Section 3 covers the credit card payments and fraud occurrence among vendors, Section 4 covers cheque payments and fraud occurrence among vendors, Section 5 covers bank transfer payments and fraud occurrence among vendors, and Section 6 covers the moderating effect of transaction value on the relationship between the cashless economy technologies and fraud occurrence among vendors (Batterton & Hale, 2017).

3.7 Data Collection Procedure

Data collection took two weeks. The researcher recruited two research assistants to help with data collection. Questionnaires were distributed to the respondents and collected using a drop-and-pick method.

3.8 Data Quality

3.8.1 Reliability

On reliability, Cronbach's alpha, a statistical measure for the reliability of a set of items, especially with multiple Likert-scale questions, was used to ensure reliability. This measures how closely the questions asked are related. According to Cooper and Chindelr (2016) a Cronbach's alpha coefficient ranging between 0.7 and 0.9 is regarded as good. For this study, a coefficient of 0.7 shall be regarded as acceptable. The Cronbach Alpha Test was calculated and analyzed using SPSS v28.

3.8.2 Internal Validity

Internal validity is the confidence that we have of whether or not the results of the research study reflect the connection between variables (Mohajan, 2020). To obtain internal validity, the researcher made sure that all the research questions effectively cover what is intended in the study. The research supervisor went through the research questions to ascertain whether they adequately respond to the research topic of study.

3.8.3 External Validity

To ensure external validity, the researcher ensured participants possess relevant experience and knowledge about the research.

3.9 Data Analysis

Different approaches to data analysis include qualitative methods (such as thematic analysis) and quantitative methods (such as statistical tests). Qualitative analysis is useful for interpreting rich, non-numeric data, while quantitative methods offer a more precise understanding of relationships between variables (Alem, 2020). This study employed a quantitative approach to analyse the collected data. This method ensures a comprehensive understanding of the variables under study (Mulisa, 2022). The data first underwent thorough cleaning and organisation using MS Excel, followed by detailed analysis using Statistical

Package for Social Sciences (SPSS) Version 28. Descriptive statistics, specifically mean and standard deviation, were used to summarize the characteristics of the data.

For each specific objective, inferential statistics were applied. The results were presented in tables, charts, and graphs for easier interpretation and visualisation of trends, relationships, and key findings. This study adopted a binary logit regression model. One without moderation and another with moderation as follows:

LN (P / 1-P) = B0 + B1MMP + B2CCP + B3CP + B4BTP + e .....(i) Before moderation

LN (P / 1-P) = B0 + B1MMP + B2CCP + B3CQP + B4BTP + B5TV + B6MMP*TV + B7CCP*TV + B8CP*TV + B9BTP*TV + e .....(ii) After moderation

where:

P = probability of high incidence and high impact fraud occurrence and 1-P = otherwise

MMP = mobile money payments

CCP = credit card payment

CQP = cheque payment

BTP = bank transfer payment

TV = transaction value

NB: moderating variable in the regression model is 1st presented as an independent variable (for direct effect) and then multiplied with each independent variable to create interactive terms for indirect effect Barron and Kenny (1986)

3.10 Diagnostic Tests

Diagnostic tests were applied to review the methods used to analyze data collected in the study. The heteroskedasticity test and the multicollinearity test were used.

3.10.1 Heteroscedasticity Test

Heteroscedasticity occurs when the standard deviation is non-constant for different values of independent variables (Munir, 2023). This can occur in a conditional or non-conditional form. Conditional heteroscedasticity occurs when volatility is related to previous periods, while

unconditional heteroscedasticity occurs when volatility is related to structural changes not related to prior periods (Munir, 2023). To detect heteroscedasticity, this study used the Modified Wald test.

3.10.2 Multicollinearity Test

Multicollinearity is a sectional problem that arises whereby the independent variables are correlated (Lindner et al.,2022). A robust method for detecting multicollinearity is the Variance Inflation Factor (VIF), which measures how much the variance of a regression coefficient is increased due to collinearity between predictors (Pandey & Pandey, 2021). A VIF value exceeding 10 indicates serious multicollinearity, while values between 5 and 10 suggest moderate multicollinearity that might require further investigation. A VIF below 5 is typically considered acceptable (Pandey & Pandey, 2021). In this study, multicollinearity was assessed by calculating the VIF using SPSS V28 software.

3.11 Ethical Considerations

The researcher sought approval from the Strathmore University Institutional Scientific and Ethical Review Committee (SU-ISERC). The researcher also applied for a National Commission for Science, Technology and Innovation (NACOSTI) research permit before the commencement of the study. The researcher remained keen on ethical considerations such as confidentiality, anonymity, privacy, and informed consent in carrying out this study. Further, the conduct of the study was guided by Strathmore University's code of ethics.

CHAPTER FOUR: PRESENTATION OF RESULTS/FINDINGS

4.1 Introduction

This study sought to determine the effect of cashless economy technologies on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, Kenya, with transaction value as the moderating factor. This chapter presents the findings of the study.

4.2 Response Rate

The study respondents returned 348 out of 379 distributed questionnaires, leading to a response rate of 91.8%. This high return rate exceeds the minimum threshold of 50% recommended by Mugenda and Mugenda (2003) for meaningful statistical analysis.

Table 4.4 : Response Rate

Distributed Questionnaire	*Returned Questionnaire*	*Response Rate*
379	*348*	*91.8%*

and the results were that all the coefficients were reliable as presented in Table 3.4; therefore, no adjustments were made to the data collection tool.

4.3 Reliability Results

Table 4.4 presents reliability tests for the instruments used to collect data on the different methods of payment, using Cronbach's Alpha.

Table 4.5: Reliability Results

Variable	Cronbach's Alpha Coefficient	Interpretation for the study
Mobile Money Payments	0.811	Reliable
Bank Transfer Payments	0.712	Reliable
Credit Card Payments	0.720	Reliable
Cheque Payments	0.823	Reliable

Source: Researcher (2025)

All four variables recorded coefficients above the acceptable level of 0.7, indicating high internal consistency and reliability of the measurement instruments. Mobile Money Payments recorded a Cronbach's Alpha of 0.811, an indication of high reliability. Bank Transfer Payments and Credit Card Payments had coefficients of 0.712 and 0.720, respectively, both of which are acceptable in terms of reliability. Cheque Payments had the highest reliability score of 0.823, which is very good internal consistency. These results confirm that the data collection tools used to gauge the payment methods were reliable and sufficient for further analysis in the study.

4.4 Demographic Information

Table 4.6 presents demographic information about the respondents.

Table 4.6: Demographic Information

Category	Details	Percentage (%)
Type of Business	Supermarket	31%
	Restaurant	29%
	Grocery	23%
	Fuel	17%
Duration in Business	Less than 1 year	33%
	1-3 years	26%
	3-5 years	24%
	More than 5 years	17%
Use of Cashless Payment Systems	Yes	88%
	No	12%

Source: Researcher (2025)

On the type of business of the respondents in the study, the findings indicate that a majority, 31%, of the respondents were in the supermarket business, 29% of the respondents were in the restaurant business, 23% of the respondents were in the grocery business, while the remaining 17% were in the fuel business. This distribution suggests a relatively balanced representation of all types of businesses, though with a slightly higher participation rate among the supermarket and restaurant businesses. The variation in representation could be influenced by factors such as industry demographics, workplace composition, or accessibility to the study (Crane et al., 2022)

On how long the respondents have been in business, majority of the respondents, 33% had been in business for less than 1 year, 26% of the respondents had been in business for 1- 3 years, 24% of the respondents had been in business for 3- 5 years while 17% of the respondents had been in business for more than 5years. This distribution highlights the varying length of

stay in the business, indicating a mix of both relatively long and short stays in the business. Such diversity in experience may influence decision-making approaches and policy implementation of cashless economy technologies on fraud occurrence among vendors (Guillaume et al. 2017).

On the use of cashless payment systems, the majority of the respondents, 88%, confirmed that they use cashless payment systems, while 12% of the respondents did not use cashless payment systems. This finding is consistent with Kirui (2022) who established that in Kenya use of cashless payment systems has increased over the last decade and that consumers grow more familiar with the different payment systems available, and encourage more transactions.

4.5 Descriptive Statistics

4.5.1 Effect of Mobile Money Payments on Fraud Occurrence Among Vendors.

Table 4.7 presents the findings on the effect of mobile money payments on fraud occurrence among vendors . Each statement was evaluated across a Likert scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree with a mean Likert score indicating the distribution of responses for the statement.

Table 4.7: Effect of mobile money payments on fraud occurrence among vendors

Statement	***Number of Respondents***	***Mean Likert Score (1-5)***	***Standard Deviation***
My business has experienced SIMswapping fraud in mobile moneypayments.	*348*	*1.67*	*0.28*
Fake mobile money promotions have led to fraud in my business.	*348*	*2.14*	*0.42*
Wrong mobile money transfers have increased fraud risks in mybusiness.	*348*	*4.91*	*0.82*
Fraudulent mobile money agentshave targeted my business.	*348*	*4.58*	*0.73*
Phishing attacks related to mobilemoney payments have occurred inmy business.	*348*	*4.72*	*0.80*
My business has experienced socialengineering fraud through mobile money transactions.	*348*	*4.12*	*0.58*

Source: Researcher (2025)

Findings in Table 4.7 depict varied effects of mobile money payments on fraud occurrence among vendors. For SIM swapping fraud, the average of 1.67 and standard deviation of 0.28 indicate that it is not prevalent with vendors. The small standard deviation is indicative of homogeneity in response, suggesting that it is not a problem with a majority of vendors. On the question of fake mobile money promotions, the mean of 2.14 and the standard deviation of 0.42 indicate that fake promotions affect businesses.

Vendors somewhat concur that fake mobile money promotions occasions fraud in their businesses, though it is not as critical as other forms of fraud. The comparatively higher standard deviation indicates a little variability in how much vendors feel the effects of fake promotions. Prevalence of wrong mobile money transfers is also a main concern, with a mean value of 4.91 and standard deviation of 0.82. That such a high mean exists indicates that the vendors are almost all in agreement that incorrect transfers increase the risk of fraud within their businesses. The standard deviation does indicate that there is some variation in the degree to which the vendors perceive this risk, with some businesses perceiving it more than others.

In addition, the impact of fraudulent mobile money agents is significant with a mean of 4.58 and standard deviation of 0.73. Most vendors concur that fraudulent agents target their businesses but there is a bit of spread in the responses as evidenced in the higher standard deviation. This indicates that even though fraudulent agents are a concern to most, the degree to which they target businesses differs between businesses. Mobile money payment phishing attacks are also a major issue, with a mean value of 4.72 and a standard deviation of 0.80. Vendors are in general agreement that phishing attacks are a key concern, but the higher standard deviation shows that there is some deviation from the level of exposure to these types of attacks by enterprises.

Finally, social engineering fraud through mobile money transactions is also of major concern, with a mean score of 4.12 and a standard deviation of 0.58. Even though the sellers are prone to agree that it does occur, it is comparatively less serious than other types of fraud, as suggested by the lower mean score. Standard deviation indicates that the responses are more consistent than in other forms of fraud and indicate that most vendors have comparable levels of concern for social engineering fraud.

The findings suggest that wrong mobile money transfers, impostor agents, phishing, and social engineering fraud are top concerns for vendors. However, SIM swap fraud and imitation promotions are less frequent and less pertinent. The findings identify areas in which vendors must be particularly vigilant regarding types of mobile money fraud where respondents were highly agreed upon.

4.5.2 Effect of Credit Card Payments on Fraud Occurrence Among Vendors.

Table 4.8 presents the findings on the effect of credit card payments on fraud occurrence among vendors. Each statement was evaluated across a Likert scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree with a mean Likert score indicating the distribution of responses for the statement.

Table 4.8: Effect of credit card payments on fraud occurrence among vendors

Statement	***Number of Respondents***	***Mean Likert Score (1-5)***	***Standard Deviation***
Lost or stolen credit cards have resulted in fraud in my business.	*348*	*4.15*	*0.63*
Skimming fraud has affected creditcard transactions in my business.	*348*	*4.06*	*0.67*
My business has experienced account takeover fraud throughcredit card payments.	*348*	*3.87*	*0.59*
Card-cracking fraud cases havebeen common in my business.	*348*	*3.02*	*0.49*
Card cloning fraud has occurred inmy business's credit card payments.	*348*	*4.69*	*0.72*

Source: Researcher (2025)

Table 4.8 results indicate various types of credit card fraud experienced by vendors. To begin with, the lost or stolen credit cards that lead to fraud in businesses have a mean score of 4.15 and a standard deviation of 0.63. This means that vendors generally agree that lost or stolen credit cards are a good cause of fraud in their businesses. The existence of the relatively low standard deviation means that respondents agree on this type of fraud, and most vendors have experienced it to some degree.

The impact of skimming fraud on business credit card transactions has a mean of 4.06 and standard deviation of 0.67, indicating that skimming fraud is also a significant issue to most vendors. Skimming fraud where the card information is skimmed with unauthorized card

readers is viewed as a persistent issue, though not quite as glaring as lost or stolen cards. The standard deviation points to some variation in the degree to which vendors are impacted by skimming fraud, ranging from business to business. With respect to account takeover fraud, where fraudsters steal card details to take over a vendor's account, the average rating of 3.87 and a standard deviation of 0.59 point to a moderate degree of impact on businesses. While the vendors do generally agree that account takeover fraud is a problem, it is not nearly as highly rated as lost or stolen cards fraud or skimming fraud. The standard deviation here is relatively low and so the answers are more consistent than those for skimming fraud.

In card-cracking fraud, where card accounts are cracked with various mechanisms, the mean score of 3.02 and standard deviation of 0.49 indicate that this type of fraud is less common with vendors. That the mean score is lower indicates towards the fact that card-cracking fraud is less of a relevant issue to most firms, and the fact that the standard deviation is low also indicates conformity in the response, with very few vendors reporting incidence of this type of fraud. Finally, card cloning fraud, which involves replicating information on a credit card and transferring it to an imitation card, has a mean value of 4.69 and a standard deviation of 0.72, showing that this is one of the most critical types of fraud that occurs to sellers. The fairly high mean score informs us that a significant number of the vendors are affected by card cloning fraud, but the higher standard deviation informs us that although the majority of the businesses are affected, the level of impact varies across businesses.

Finally, the results indicate that stolen or lost credit cards, card cloning fraud, and skimming fraud are of most concern to vendors. Account takeover fraud is also a concern but to a lesser degree, while card-cracking fraud seems less common. The findings emphasize the importance for vendors to be very aware of fraud types that were recorded as of great concern by many respondents.

4.5.2 Effect of Cheque Payments on Fraud Occurrence Among Vendors.

Table 4.9 presents the findings on the effect of cheque payments on fraud occurrence among vendors. Each statement was evaluated across a Likert scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree with a mean Likert score indicating the distribution of responses for the statement.

Table 4.9: Effect of cheque payments on fraud occurrence among vendors.

Statement	***Number of Respondents***	***Mean Likert Score (1-5)***	***Standard Deviation***
Cheque kiting fraud has occurred in my business.	*348*	*5.12*	*0.51*
Bad cheque writing has increased fraud risks in my business.	*348*	*5.26*	*0.43*
Cheque conversion fraud has impacted my business.	*348*	*2.27*	*0.43*
My business has experienced cheque forgery fraud.	*348*	*4.01*	*0.82*

Source: Researcher (2025)

The findings in Table 4.9 show some of the types of cheque fraud that Embakasi East Constituency, vendors have encountered. The lowest mean score is associated with bad cheque writing, whose mean score is 5.26 with a standard deviation of 0.43. This means that bad cheque writing is a source of concern to vendors, whose respondents overwhelmingly held the opinion that it increases fraud risk in business. The low standard deviation indicates that the majority of the respondents share similar views regarding how prevalent and risky this type of fraud is.

The same is true of cheque kiting fraud, in which a cheque is drawn on an insufficient account. This also has a high mean score of 5.12 and a standard deviation of 0.51. This suggests that cheque kiting is a significant issue among vendors, with most reporting that they have seen it occur in their business. The slightly greater standard deviation would suggest some variation in the degree of concern, with some vendors seeing it occur more frequently than others. On the other hand, cheque conversion fraud, which is an alteration or unauthorized processing of cheques, has a much lower mean score of 2.27 and standard deviation of 0.43. This indicates that cheque conversion fraud is not as prevalent among vendors, with respondents largely

disagreeing that it has been a major issue in their companies. The low standard deviation also means consistency in these responses, which means that this form of fraud is not as large a problem for most vendors.

Finally, cheque forgery fraud, with a mean of 4.01 and a standard deviation of 0.82, indicates that while it is an important problem, it is not as significant as bad cheque writing or cheque kiting. The greater standard deviation here indicates more variation in the responses, i.e., some vendors are affected by cheque forgery more frequently than others. In short, the findings show that bad cheque writing and cheque kiting fraud are the most common forms of fraud that affect vendors. Cheque forgery is a problem but to a lesser extent, while cheque conversion fraud is a less serious issue for most vendors. The findings show the importance of prioritizing some of the types of cheque fraud that are most dominant and with largest impact on businesses.

4.4.3 Effect of Bank Transfer Payments on Fraud Occurrence Among Vendors.

Table 4.10 presents the findings on the effect of bank transfer payments on fraud occurrence among vendors. Each statement was evaluated across a Likert scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree with a mean Likert score indicating the distribution of responses for the statement.

Table 4.10: Effect of Bank Transfer Payments on Fraud Occurrence Among Vendors.

Statement	***Number of Respondents***	***Mean Likert Score (1-5)***	***Standard Deviation***
My business has experienced payment fraud through bank transfers.	*348*	5.21	0.44
Chargeback fraud has been an issue with bank transfer payments in my business.	*348*	5.90	0.54
Identity theft has occurred during bank transfer transactions in my business.	*348*	5.23	0.59
Cybersecurity issues related to bank transfers have caused fraud in my business.	*348*	3.87	0.64
Card cloning fraud has been linked to bank transfers in my business.	*348*	2.83	0.82
Credential stuffing has led to fraud in my business's bank transfers.	*348*	3.35	0.83

Source: Researcher (2025)

The results in Table 4.10 present the different categories of bank transfer payment-related fraud experienced by vendors. The highest mean score is chargeback fraud, with a mean score of 5.90 and a standard deviation of 0.54. This indicates that chargeback fraud is a serious issue for merchants, with most respondents agreeing that it has been a persistent problem in their organizations. The low standard deviation suggests that there is consensus among the respondents that this form of fraud is a serious issue.

Second, payment fraud through bank transfers has a mean of 5.21 and a standard deviation of 0.44, implying that payment fraud through bank transfers is also a serious concern. The

implication that most vendors are experiencing payment fraud is suggested by the mean score, while the low standard deviation implies that vendors have high and uniform agreement regarding this problem. Identity theft in bank transfer transactions has a mean of 5.23 and a standard deviation of 0.59, meaning that identity theft is indeed a problem for vendors. Like chargeback fraud, vendors agree that identity theft is a significant problem in their businesses, with the slight difference in standard deviation meaning that a few vendors were faced with this problem more frequently than others.

However, cybersecurity issues related to bank transfers show a lower mean of 3.87 with a standard deviation of 0.64, showing that while the issue of the threat of cybersecurity is there, it is less serious than with other forms of fraud like chargeback fraud and identity theft. The moderate variability standard deviation shows that the extent of cybersecurity issues varies from company to company. Card cloning fraud related to bank transfers has a mean score of 2.83 and a standard deviation of 0.82, which means that this type of fraud is not prevalent among the vendors. The low mean score means that most vendors do not consider card cloning as a prevalent issue related to bank transfers, but the higher standard deviation indicates some variation in responses with few vendors having it more frequently.

Lastly, credential stuffing in bank transfer also has a mean of 3.35 and standard deviation of 0.83, meaning that fraud via this type is an average-level issue to sellers. Lower than identity theft or chargeback fraud but also a moderate issue, the greater standard deviation signifies that this is a less uniform issue by business type.

4.6 Diagnostic Tests

This section contains the results of the heteroskedasticity test and multicollinearity test.

4.6.1 Heteroscedasticity Test

In the research model, the Modified Wald test produced a chi-square value of 22000.31 with a p-value of 0.0000. This chi-square value was statistically significant at the 1% level, assuming constant variance. In response to the detected heteroscedasticity, robust standard errors were employed in the study to account for this issue.

4.6.2 Multicollinearity Test

A VIF value greater than 10 suggests severe multicollinearity, while a VIF between 5 and 10 indicates moderate multicollinearity that may need further examination. A VIF below 5 was generally considered acceptable. Table 4.11 shows the VIF results

Table 4.11: Variance Inflation Factor (VIF) Results

Predictor Variable	***VIF***	***Interpretation***
Mobile Money Payment	*1.90*	*No Multicollinearity*
Credit Card Payment	*1.73*	*No Multicollinearity*
Cheque Payment	*2.24*	*No Multicollinearity*
Bank Transfer Payment	*1.89*	*No Multicollinearity*
Transaction Value	*1.55*	*No Multicollinearity*

Source: Researcher (2024)

Since all VIF values are below 5, the results confirm that multicollinearity was not a concern in the dataset. Consequently, the assumption of non-multicollinearity in regression analysis was upheld, ensuring the reliability of coefficient estimates in the model.

4.7 Binary Logit Regression (Before Moderation)

4.7.1 Model Fitness Test Findings

The R square findings, as per Table 4.12, indicated that the regression model Nagelkerke R Square goodness test result of 51.3 %, which meant that the regression model was able to influence up to 51.3 % of the variance in fraud occurrence among vendors in Embakasi East Constituency, Nairobi (Hair et al., 2014).

Table 4.12: Findings on R Square Test

-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
439.812a	0.158	0.513

The Hosmer and Lemeshow test was carried out as an additional test of model fitness, as presented in Table 4.13.

Table 4.13: Findings on Hosmer & Lemeshow Test

Chi-square	Df	Sig.
8.167	8	.780

Table 4.13 indicated that the p-value Hosmer & Lemeshow test was 0.780, which was higher than the 0.05 level, and hence, the model fit was acceptable (Hair et al., 2014).

4.6.2 Regression

The goodness-of-fit tests were used to confirm the model's goodness of fit. The researcher applied the Pearson and Deviance Chi-square tests presented in Table 4.14.

Table 4.14: Pearson and Deviance Chi-square tests of Independence

Factor	Pearsons χ2 Value	df	P Value
Mobile Money Payment * Fraud Occurrence	217.812	96	0.000
Credit Card Payment* Fraud Occurrence	117.651	89	0.000
Cheque Payments* Fraud Occurrence	112.142	93	0.000
Bank Transfer Payment* Fraud Occurrence	117.312	70	0.000

Source: Researcher (2025)

The findings show that fraud occurrence was dependent on all four factors of mobile payment, credit card payment, cheque payments and bank transfer payment, tested at 5% significance

levels. The proportionate odds assumptions made by the data were put to the test using the parallel lines test shown in Table 4.14. This was done to ensure that the model didn't go against the proportional odds assumption.

Table 4.15: Test of Paralleled lines

Factor	Model	-2 Log Likelihood	Chi-Square	df	sig
Mobile Money Payment * Fraud Occurrence	Null Hypothesis	130.360			
	General	125.181	5.213	2	0.169
Credit Card Payment* Fraud Occurrence	Null Hypothesis	101.411			
	General	71.611	4.120	4	0.139
Cheque Payments* Fraud Occurrence	Null Hypothesis	72.167			
	General	55.180	2.172	2	0.172
Bank Transfer Payment* Fraud Occurrence	Null Hypothesis	67.621			
	General	58.814	1.920	3	0.153

Link Function: Logit
Source: Researcher (2025)

The analysis in Table 4.15 shows that the variables did not go against the proportional odds assumption since they were not statistically significant (all were above 0.05), which allowed the interpretation of the parameter estimates. Further, the determination measures were established using the NagelKerke Pseudo-R Square, presented in Table 4.16.

Table 4.16: Measures of Determination

Model	NagelKerke R^2	Cox and Snell R^2	McFadden R^2
Mobile Money Payment * Fraud Occurrence	0.192	0.130	0.093
Credit Card Payment* Fraud Occurrence	0.094	0.126	0.119
Cheque Payments* Fraud Occurrence	0.103	0.095	0.064
Bank Transfer Payment* Fraud Occurrence	0.098	0.062	0.036

Link Function: Logit
Source: Researcher (2025)

The pseudo-R square findings show that 19.2% of fraud occurrence among vendors in Nairobi is determined by mobile payment, 9.4% by credit card payments, 10.3% by cheques payment, and 9.8% by bank transfer payment.

Table 4.17: Ordinal Regression using Parameter Estimates

Step 1[a]	Estimate	Std. Error	Wald	df	Sig	95%CI Lower	Upper
Constant	0.244	0.042	26.180	1	0.630	0.431	0.914
Mobile Money Payment	0.693	0.092	21.523	1	0.000	0.695	1.472
Credit Card Payment	0.330	0.094	37.011	1	0.000	0.110	1.421
Cheque Payments	0.362	0.216	4.590	1	0.000	0.412	1.374
Bank Transfer Payment	0.353	0.201	3.820	1	0.000	0.290	1.326

Link Function: Logit
Source: Researcher (2025)

Substituted coefficient estimates in the equation:

LN (P / 1-P) = 0.244 + 0.693MMP + 0.330CCP + 0.362CP + 0.353BTP + e .....(i) Before moderation

As per the findings in Table 4.17, mobile money payment had a coefficient of 0.693 which lies within the lower bound 0.695 and upper bound of 1.472. This implied that mobile money payment had a significant positive effect on fraud occurrence among vendors in Embakasi East Constituency, Nairobi (p-value = 0.000). Further, for every unit increase in mobile money

payment, there was a predicted increase of 0.693 in the log odds of fraud occurrence among vendors in Embakasi East Constituency, Nairobi.

Credit card payment had a coefficient of 0.330 which lies within the lower bound 0.110 and upper bound 1.421. This implied that credit card payment had a significant positive effect on fraud occurrence among vendors in Embakasi East Constituency, Nairobi (p-value = 0.000). Further, for every unit increase in credit card payment, there was a predicted increase of 0.330 in the log odds of fraud occurrence among vendors in Embakasi East Constituency, Nairobi.

Cheque payment had a coefficient of 0.362 which lies within the lower bound 0.412 and upper bound of 1.374. This implied that market timing had a significant positive effect on fraud occurrence among vendors in Nairobi(p-value = 0.000). Further, for every unit increase in market timing, there was a predicted increase of 0.362 in the log odds of fraud occurrence among vendors in Embakasi East Constituency, Nairobi.

Bank transfer payment had a coefficient of 0.353 which lies within the lower bound 0.290 and upper bound of 1.326. This implied that bank transfer payment had a significant positive effect on fraud occurrence among vendors in Nairobi. (p-value = 0.000). Further, for every unit increase in bank transfer payment, there was a predicted increase of 0.353 in the log odds of fraud occurrence among vendors in Embakasi East Constituency, Nairobi.

The constant term had a coefficient of 0.244, which lies within the lower bound 0.431 and upper bound of 0.914. The constant term was not statistically significant (p = 0.630), indicating that fraud occurrence among vendors in Embakasi East Constituency, Nairobi cannot be explained without incorporating the independent variables. Further, for every unit increase in the constant term, there was a predicted increase of 0.244 in the log odds of fraud occurrence among vendors in Embakasi East Constituency, Nairobi. All independent variables; mobile money payment, credit card payments, cheque payments and bank transfer payments significantly increased the odds of fraud occurrence among vendors in Embakasi East Constituency, Nairobi. The constant term, however, was not significant, reinforcing the importance of these payment methods in predicting fraud occurrence.

VT OMNES
VNVM SINT

4.7 Binary Logistic Regression (After Moderation)

The binary logistic regression model was used to evaluate the moderating effect of Transaction Value (TV) on the relationship between cashless economy technologies and fraud occurrence among vendors in Nairobi, Kenya.

Table 4.18: Ordinal Regression using Parameter Estimates

Step 1[a]	Estimate	Std. Error	Wald	Df	Sig	95%CI Lower	Upper
Constant	0.244	0.042	26.180	1	0.630	0.431	0.914
Mobile Money Payment	0.693	0.092	21.523	1	0.000	0.695	1.472
Credit Card Payment	0.330	0.094	37.011	1	0.000	0.110	1.421
Cheque Payments	0.362	0.216	4.590	1	0.000	0.412	1.374
Bank Transfer Payment	0.353	0.201	3.820	1	0.000	0.290	1.326
Transaction Value	0.151	0.031	2.914	1	0.006	0.382	1.482
Mobile Money Payment_ Transaction Value	0.105	0.029	19.423	1	0.005	0.249	1.303
Credit Card Payment _ Transaction Value	0.050	0.032	23.092	1	0.013	0.319	1.425
Cheque Payment _ Transaction Value	0.055	0.022	11.089	1	0.001	0.206	1.259
Bank Transfer Payment _ Transaction Value	0.053	0.062	7.093	1	0.009	0.283	1.382

Link Function: Logit
Source: Researcher (2025)

LN (P / 1-P) = B0 + B1MMP + B2CCP + B3CQP + B4BTP + B5TV + B6MMP*TV + B7CCP*TV + B8CP*TV + B9BTP*TV + e .....(ii) After moderation

LN (P / 1-P) = 0.244 + 0.693MMP + 0.330CCP + 0.362CP + 0.353BTP + 0.151TV + 0.105 MMP*TV + 0.050CCP*TV + 0.055CP*TV + 0.053BTP*TV + e .....(ii) After moderation

Table 4.18 represents the moderating effect of Transaction Value on the relationship between each payment method and fraud occurrence. The MMP*TV coefficient for this interaction term was 0.105 (p-value = 0.005), which lies within the lower bound of 0.249 and upper bound of 1.303, suggesting that the significant and positive relationship between mobile money payments and fraud occurrence strengthens as transaction value increases.

CCP*TV coefficient for this interaction term was 0.050 (p-value = 0.013), which lies within the lower bound 0.319 and upper bound of 1.425, showing that as transaction value increases, the link between credit card payments and fraud occurrence becomes stronger. CP*TV

coefficient for this interaction term was 0.055 (p-value = 0.001), which lies within the lower bound 0.206 and upper bound of 1.259, indicating that higher transaction values increase the association between cheque payments and fraud.

BTP*TV coefficient for this interaction term was 0.053 (p-value = 0.009),which lies within the lower bound 0.283 and upper bound of 1.382 implying that larger transaction values exacerbate the relationship between bank transfer payments and fraud occurrence. The results indicate that Transaction Value (TV) significantly moderates the relationship between cashless payment methods and fraud occurrence. As transaction value increases, the likelihood of fraud in mobile money, credit card, cheque, and bank transfer payments also increases. This suggests that higher-value transactions may carry greater fraud risks, and the impact of payment methods on fraud occurrence is amplified when transaction values are larger.

The findings between the descriptive and regression results were consistent. Both highlighted significant concerns regarding fraud types associated with different payment methods, such as mobile money, credit cards, cheques, and bank transfers. The descriptive findings identified fraud types like wrong mobile money transfers, skimming, and chargeback fraud as major issues, which the regression analysis confirmed, showing that all payment methods significantly increased fraud risk. Additionally, the regression results introduced the moderating effect of transaction value, which had a positive and significant effect on fraud occurrence among vendors in Embakasi East Constituency, Nairobi, thus showing how larger transactions amplify fraud risks.

4.8 Chapter Summary

This chapter presents the study's findings on response reliability, demographics, and fraud risks associated with cashless payment methods. The data collection tools were confirmed as reliable for analysis, and businesses represented included supermarkets, restaurants, groceries, and fuel stations. The majority of respondents used cashless payment systems, reflecting growing adoption in the area. Key fraud risks were identified for each payment method, including phishing, card cloning, cheque kiting, and chargeback fraud. Higher transaction values were linked to increased fraud risks, emphasizing the importance of enhanced security measures in cashless transactions.

CHAPTER FIVE: DISCUSSIONS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter contains the summary of findings, the study's discussion, conclusion, and recommendations, presented according to the study objectives, limitations and areas of further study.

5.2 Summary of Findings

The descriptive findings highlighted the various fraud types vendors in Embakasi East Constituency face with different payment methods. Mobile money fraud, such as wrong transfers, fraudulent agents, phishing, and social engineering, were major concerns, while SIM swapping and fake promotions were less common. Credit card fraud, including lost or stolen cards, skimming, and card cloning, was significant, but account takeover and card-cracking were less prevalent. Cheque fraud, particularly bad cheque writing and cheque kiting, was a major issue, while cheque conversion fraud was less concerning. For bank transfers, chargeback fraud and identity theft were primary concerns, while card cloning and credential stuffing were less prominent. The regression findings provided a deeper understanding of the relationship between payment methods and fraud occurrence. All four payment; mobile money, credit card, cheque, and bank transfer, were found to significantly increase the odds of fraud occurrence. The moderating effect of transaction value was also significant: as transaction value increases, the likelihood of fraud in all payment methods also rises, indicating that higher-value transactions are more susceptible to fraud.

5.3 Discussions

5.3.1 Effect of Mobile Money Payments on Fraud Occurrence Among Vendors.

Mobile money payment had a significant positive effect on fraud occurrence among vendors in Embakasi East Constituency. Further, for every unit increase in mobile money payment, there was a predicted increase of 0.693 in the log odds of fraud occurrence among vendors in the Embakasi East Constituency.

This aligns with the empirical findings of Kivuva (2021) who found that mobile money was the most popular mode of payment and had a positive and significant relationship with fraud occurrence. He recommended that merchants had to address the risk of fraud to reap the benefits of the cashless system. The study corroborates findings of Esperance (2024), who

found that mobile money payment has a positive and significant relationship with fraud. Further established that mobile money still has flaws like privacy infringement and hacking. Similarly, the findings of the study are consistent with the findings of Kimani and Sirera (2019), they established a positive and significant relationship between mobile payment and fraud. They further acknowledged that businesses must create better fraud prevention methods, including customer awareness and improved security measures.

Additionally, the positive and significant effect of mobile money payments on fraud upholds the opportunity aspect of the fraud diamond theory in which the vulnerabilities in the system provide an opportunity for fraud (Hermanson & Wolfe, 2024). The capability of fraudsters to exploit such vulnerabilities (e.g., phishing, SIM swapping) is one of the contributing factors to fraud. Pressure arises due to simple transactions within the fraud triangle, and rationalization results from fraudsters' rationalization of exploiting an open system. Further, Routine activity theory establishes that mobile money is an opportunistic target for fraud due to high usage and lack of proper guardianship, with larger-value transactions carrying higher risks to fraud (Mohammad & Nooraini, 2021).

5.3.2 Effect of Credit Card Payments on Fraud Occurrence Among Vendors.

Credit card payment had a significant positive effect on fraud occurrence among vendors in Embakasi East Constituency. Further, for every unit increase in credit card payment, there was a predicted increase in the log odds of fraud occurrence among vendors in the Embakasi East Constituency.

These findings are consistent with the findings of Kanyaru and Kyalo (2018). Their findings highlighted the positive and significant effect of credit card payment on fraud. They identified two primary factors enabling fraud: the systems that have relatively low-security arrangements and customers who are easy targets for phishing scams or fraud-related transactions. Similarly, these findings are also consistent with the findings of Solat (2017), which established the positive and significant effect of credit card payment on fraud. The research stressed that credit cards, being convenience products, pose considerable risks and security must be equally convenient to counteract the convenience that credit card companies offer.

Further, the positive and significant effect of credit card payments on fraud occurrence is

supported by the opportunity factor in the fraud diamond when low security is the foundation for weaknesses (Hermanson & Wolfe, 2024). The capability of fraudsters, for instance, by phishing and skimming, leads to higher fraud activities. The fraud triangle suggests more pressure with convenient credit card payments, and rationalization may occur on grounds of felt insecurity (Mansor & Abdullahi, 2019). Additionally, Routine activity theory highlights that credit card payments are being targeted since they are available and have low surveillance, with larger transactions making them more vulnerable (Mohammad & Nooraini, 2021).

5.3.3 Effect of Cheque Payments on Fraud Occurrence Among Vendors.

Cheque payment had a significant positive effect on fraud occurrence among vendors in Nairobi. Further, for every unit increase in cheque payments , there was a predicted increase in the log odds of fraud occurrence among vendors in the Embakasi East Constituency.

This result aligns with studies such as Jumba and Wepukhulu (2019). Their findings showed that a positive and significant relationship existed between cheque payment and fraud. The further identified the common types of cheque-related fraud, including check-kiting and forgeries, where counterfeit or unauthorized cheques are used to withdraw funds fraudulently. Similarly, the findings concur with Esperance (2024) who noted that although cheque usage has become infrequent in modern payment systems, it remains a viable medium for fraudulent activities. Esperance highlighted that businesses transitioning toward fully cashless modes of operation often experience a proportional decline in cheque-related fraud.

In contrast, Mwabu (2018) findings differ from the findings of this study. His research found that while cheques are less prone to fraud than mobile money or credit card payments. Mwabu (2018) noted that cheque fraud typically involves more traditional schemes, such as counterfeit cheques or unauthorized endorsements, which are less prevalent. The findings align with the fraud triangle theory (Mansor & Abdullahi, 2019). Cheques are prone to fraud due to opportunity (e.g., cheque kiting and cheque forgeries), as fraudsters exploit loopholes within the system. The facility to modify or fake cheques increases fraud risk. Pressure is delivered by large cheque transactions within the fraud triangle, and rationalization is delivered if fraudsters believe cheques are insecure. Additionally, Routine activity theory explains why cheques are an ideal target due to low surveillance, and high-value transactions increase fraud vulnerability (Mohammad & Nooraini, 2021).

VT OMNES
VNVM SINT

5.3.4 Effect of Bank Transfer Payments on Fraud Occurrence Among Vendors

Bank transfer payment had a significant positive effect on fraud occurrence among vendors in Nairobi. Further, for every unit increase in bank transfer payment, there was a predicted increase in the log odds of fraud occurrence among vendors in Nairobi.

The findings align with Otibo-Addo (2021), who found that bank payment had a significant positive effect on fraud. He further established that the hacking of banking transfer platforms was the most prevalent and damaging in their quest towards the adoption of a cashless economy. Also revealed that hackers attack vulnerable banking transfer services, erode people's confidence in electronic payment technology, and delay the shift to a cashless society.

The findings of this study agree with the research conducted by Matthew and Mike (2019) they found that bank transfer payments had a positive and significant effect on fraud occurrence. They further established that bank transfer systems are susceptible to phishing and hacking. Consequently, the study called for the implementation of strong security controls that would help fill the identified systemic vulnerabilities and make customers trust digital financial services.

This finding corroborates with the fraud triangle theory (Mansor & Abdullahi, 2019). The rationalization in the fraud triangle is argued based on weaknesses perceived within the bank transfer systems. Routine activity theory illustrates that bank transfers are victimized as a result of being unsupervised, and larger transactions are more appealing to fraudsters.

5.3.5 The Moderating Effect of Transaction Value on the Relationship Between the Cashless Economy Technologies and Fraud Occurrence among Vendors.

Mobile money payments had a significant and positive relationship with transaction value and fraud occurrence which strengthens as transaction value increases. Credit card payments had a significant and positive relationship with transaction value and fraud occurrence, showing that higher transaction values amplify the link to fraud. Similarly, cheque payments and bank transfers had a significant and positive relationship with transaction value and fraud occurrence which suggest that larger transaction values intensify the association with fraud occurrence.

These findings are consistent with the findings of Misango et al., (2020) revealed that transaction value influence the occurrence of fraud when using cashless technologies. They further noted that mobile money Payments in Nairobi, Kenya were prevalent despite consumers using bank transfers for large transactions values. However, these transactions were increasingly vulnerable to crime-related criminal activities as the value increased.

This finding corroborates with the routine activity theory. The routine activity theory argues that larger transactions have reduced security and are therefore more prone to fraud. The transaction value moderating effect heightens the pressure to commit fraud because bigger transactions are more rewarding. The fraud potential also increases with the size of the transaction, while fraudsters' potential to capitalize on such transactions is heightened (Mohammad & Nooraini, 2021).

Additionally, this finding corroborates with the fraud triangle theory. Being like other cashless payment modes, susceptible to opportunity and capability-based fraud. The pressure to defraud increases with larger transactions, as fraudsters are motivated by larger financial returns. Pressure is delivered by large cheque transactions within the fraud triangle (Mansor & Abdullahi, 2019).

5.4 Conclusion

The study concluded that the results indicate a significant and positive relationship between the independent variables, the dependent variable and the moderating variable. The R square findings showed that the regression model was able to influence fraud occurrence among vendors in Embakasi East Constituency. The pseudo-R square findings show that fraud occurrence among vendors in Nairobi is determined by mobile payment, credit card payment, cheque payment, and bank transfer payment. The study findings revealed consistency across descriptive statistics and regression analysis in identifying the effect of cashless economy technologies on fraud occurrence among vendors in Embakasi East Constituency, with transaction value as the moderating factor. Further, the study made the following conclusions regarding the study objectives:

The study concluded that mobile money payment had a significant positive effect on fraud occurrence among vendors in Embakasi East Constituency. Further, for every unit increase in

mobile money payment, there was a predicted increase in the log odds of fraud occurrence among vendors Embakasi East Constituency

The study concluded that credit card payment had a significant positive effect on fraud occurrence among vendors in Nairobi. Further, for every unit increase in credit card payment, there was a predicted increase in the log odds of fraud occurrence among vendors in Embakasi East Constituency.

The study concluded that cheque payments had a significant positive effect on fraud occurrence among vendors in Nairobi. Further, for every unit increase in cheque payments, there was a predicted increase in the log odds of fraud occurrence among vendors in Embakasi East Constituency.

The study concluded that bank transfer payment had a significant positive effect on fraud occurrence among vendors in Nairobi. Further, for every unit increase in bank transfer payment, there was a predicted increase in the log odds of fraud occurrence among vendors in Embakasi East Constituency.

The study concluded that transaction value has a positive and significant moderating effect on the relationship between the cashless economy technologies and fraud occurrence among vendors in Embakasi East Constituency.

5.5 Recommendation

5.5.1 Policy Recommendations

The study recommended that policymakers should establish and enforce stringent regulations for mobile money, credit card, cheque, and bank transfer platforms to enhance fraud prevention mechanisms. These regulations should mandate the implementation of advanced encryption and authentication technologies, such as two-factor authentication and biometric verification, to secure transactions.

The study recommended that the government should collaborate with financial institutions to run nationwide awareness campaigns that educate consumers and vendors on identifying and preventing fraud. These campaigns should focus on the most prevalent fraud types, such as phishing, SIM swapping, and card skimming, and provide practical advice on secure

transaction practices.

The study recommended that given that transaction value significantly influences fraud risk, policies should require additional verification steps or security measures for large-value transactions, especially on mobile money platforms and bank transfers. These could include additional checks or alerts for high-value transactions to prevent unauthorized activities.

The study recommended that a central body should be established for reporting fraud-related incidents across all payment methods. This system should offer real-time tracking of fraud cases, provide support for affected vendors, and ensure quick resolution. Moreover, regular audits and fraud detection should be conducted on cashless payment systems to identify vulnerabilities.

5.5.2 Recommendation for Theory

The study recommended that the fraud diamond and triangle theories could be further refined to account for the specific challenges and vulnerabilities associated with cashless payment systems. Researchers should investigate how emerging technologies, such as blockchain or artificial intelligence, could reduce the opportunity and capability factors that contribute to fraud.

The study recommended that routine activity theory could be expanded to better explain how technological advances in payment systems alter the dynamics of fraud risk. Future studies should focus on how increased digitalization, mobile payment platforms, and online transactions create new opportunities for fraud, particularly about vendors' routines and operational contexts.

5.5.3 Recommendation for Practice

The study recommended that vendors should prioritize the adoption of robust security protocols, including regular updates to fraud detection systems, secure payment gateways, and encryption technologies. Training staff to identify potential fraudulent activities and implement security best practices can also reduce fraud risks.

The study recommended that vendors should adopt transaction monitoring systems that flag

unusual or high-value transactions, enabling early detection of fraudulent activities. These systems should be able to analyze patterns in real time and send alerts to vendors for immediate action.

The study recommended that it is crucial for vendors to invest in training their employees on the latest fraud tactics, security measures, and how to handle potential fraud incidents. Regular workshops or training sessions on preventing fraud will help ensure that staff remain vigilant and proactive in securing transactions.

The study recommended that vendors should implement multi-layered customer verification processes for both high-value transactions and new customers. Verification steps like two-factor authentication, biometric verification, or a one-time passcode can significantly reduce the risk of fraud.

The study recommended that vendors should collaborate with payment service providers to ensure that security features are built into the payment systems. Regularly reviewing and upgrading security protocols with the payment providers is crucial to stay ahead of emerging fraud risks.

5.6 Limitations of the Study

The study is geographically limited to vendors in Embakasi East Constituency, Nairobi, which may not represent the broader situation in other regions or countries. Additionally, the research employed a descriptive design, which may restrict the generalizability of the findings. The focus on only four specific payment methods (mobile money, credit cards, cheques, and bank transfers) may overlook other emerging cashless payment technologies, such as digital wallets or cryptocurrencies. The study also relied on self-reported data through questionnaires, which could introduce bias or inaccuracies, particularly on sensitive topics like fraud. Furthermore, while the study examined the moderating effect of transaction value, it did not explore other potential moderating factors, such as the type of fraud or the scale of the business.

5.7 Areas for Further Research

Future research could investigate the role of emerging technologies like blockchain, AI, and machine learning in preventing fraud and enhancing the security of cashless payment systems. A cross-industry comparison could provide insights into how different sectors experience fraud

with cashless payments, particularly regarding varying transaction values. Expanding the study to other regions or countries would offer a broader understanding of how geographic and economic factors influence fraud dynamics. Moreover, research into effective fraud prevention measures and regulatory frameworks could help mitigate the risks associated with cashless systems. Longitudinal studies tracking fraud patterns over time could also provide valuable insights as cashless technologies evolve and transaction values increase.

5.8 Chapter Summary

Chapter Five discusses the study's findings, concluding that mobile money, credit cards, cheques, and bank transfers significantly increase fraud among vendors in Embakasi East Constituency, with transaction value amplifying this effect. The findings align with theories such as the Fraud Triangle and Routine Activity theory, highlighting systemic vulnerabilities and higher risks for larger transactions. Recommendations include stricter regulations, enhanced security measures, and vendor training to mitigate fraud. The study's limitations, such as its geographic focus and reliance on self-reported data, are noted, and future research areas.

References

Alem, D. D. (2020). An overview of data analysis and interpretations in research. *International Journal of Academic Research in Education and Review, 8*(1), 1-27. Retrieved from https://www.academia.edu/download/78408562/Dawit.pdf

Alharahsheh , H. H., & Pius, A. (2020). A review of key paradigms: Positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences, 2*(3), 39-43.

Ali, M. A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, 408-427.

Ategeka, C. (2021). *The Unintended Consequences of Technology: Solutions, Breakthroughs, and the Restart We Need.* John Wiley & Sons. Retrieved from https://books.google.com/books

Batterton, K. A., & Hale, K. N. (2017). The Likert scale what it is and how to use it. *Phalanx, 50*(2), 32-39.

Bosibori, C. M. (2023). *Modeling Cross Sectional Data Of The Sale Price Of Residential Properties In Ames Using Fuzzy Regression Analysis.* Kirinyaga University.

Chukwuekwu, O. (2024). Fraud and performance of listed deposit money banks in Nigeria: Exploring the combined effects of fraud triangle and fraud diamond theories. *Journal of Business and Econometrics Studies, 1*(3), 1-8.

Crane, L. D., Decker, R. A., Flaaen, A., & Hamins-Pu. (2022). Business exit during the COVID-19 pandemic: Non-traditional measures in historical context. *Journal of macroeconomics*, 72.

Detzen, D., & Gold, A. (2021). The different shades of audit quality: A review of the academic literature. *Maandblad voor Accountancy en Bedrijfseconomie, 95*(1/2), 5-15. Retrieved from https://mab-online.nl/article_preview.php?id=60608

Dewi, C., & Abdullah, S. (2021). Cashless Transactions and Retail Fraud. *In 2nd International Conference on Science, Technology, and Modern Society (ICSTMS 2020)*, (pp. 217-222). Retrieved from https://www.atlantis-press.com/proceedings/icstms-20/125960656

Esperance, M. (2024). Effect of Cashless Financial Services on Economic Growth in Kigali, Rwanda. *Valley International Journal Digital Library*, 5743-5755. Retrieved from https://vipublisher.com/index.php/vij/article/view/154

Ezeanolue, E. T. (2022). The effect of cashless economy on the performance of small scale enterprises in Anambra State. *Anspoly Journal Of Innovative Development (AJID),*

1(2), 143-161. Retrieved from https://journal.anspolyjoid.org.ng/index.php/ajid/article/view/19

Hedman, J., & Henningsson, S. (2019). The new normal: Market cooperation in the mobile payments ecosystem. *Electronic Commerce Research and Applications, 14*(5), 305-318.

Hermanson, D., & Wolfe, D. (2024). The Fraud Diamond. *CPA Journal*, 94. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&profile

Huntington-Klein, N. (2021). *The effect: An introduction to research design and causality. Chapman and Hall/CRC.* Retrieved from https://www.taylorfrancis.com/books/mono/10.1201/9781003226055/effect-nick-huntington-klein

Iyer, S. M. (2017). *A Case Study on Monetary Fraud in a Cashless Economy.* Master's thesis, Purdue University. Retrieved from https://search.proquest.com/openview/c337417c7f55c91fd5759ce6b754f8a1/1?pq-origsite=gscholar&cbl=18750

Jumba, J., & Wepukhulu, J. M. (2019). Effect of cashless payments on the financial Performance of supermarkets in Nairobi County, Kenya. *International Journal of Academic Research Business and Social Sciences, 9*(3), 1372-1397. Retrieved from https://www.academia.edu/download/83326756/Effect_of_Cashless_Payments_on_the_Financial_Performance_of_Supermarkets_in_Nairobi_County2.pdf

Kanyaru, P. M., & Kyalo, J. K. (2018). Factors affecting the online transactions in the developing countries: a case of e-commerce businesses in Nairobi County, Kenya. *Journal of Educational Policy and Entrepreneurial Research, 2*(3), 1-7. Retrieved from http://ir-library.ku.ac.ke/bitstream/handle/123456789/13834

Kassem, R. (2022). How could external auditors assess the rationalization of fraud? *Journal of Financial Crime, 29*(4), 1458-1467.

Katela, M. M. (2019). *Challenges Facing Financial Services Agents: Case Study of Nairobi County.* United States International University-Africa.

Kimani, J. M., & Sirera, M. (2019). Strategies used by mpesa agents and their effectiveness in deterrence of counterfeit bank notes fraud in Nairobi City County. *International Academic Journal of Economics and Finance, 3*(4), 255-266.

Kirui, E. C. (2022). *Influence of regulatory framework on the relationship between factors influencing cashless transactions and growth of cashless transactions.* Doctoral dissertation, Strathmore University. Retrieved from https://su-

plus.strathmore.edu/bitstreams/04ad2ed6-5e6f-428e-9431-42d8fe3e7b60/download

Kithembe, C. M. (2023). *Information Technology and Performance of SMEs in Nairobi County, Kenya.* Doctoral dissertation, University of Nairobi. Retrieved from http://erepository.uonbi.ac.ke/handle/11295/164631

Kivuva, E. (2021, September Thursday). South Africa, Nigeria trail Kenya cashless payments. *The East African*. Retrieved from https://www.theeastafrican.co.ke/tea/business/south-africa-nigeria-trail-kenya-cashless-payments-3567936

KNBS. (2024). *Economic Survey Inequalities in wellbeing in Kenya Report Consumer Price Indices and Inflation.*

Kovarik, Q. (2023). *Essays on Audit Quality.* Aarhus Universitet. Retrieved from https://pure.au.dk/portal/files/319399276/Essays_on_Audit_Quality_PhD_dissertation_Qing_Kovarik.pdf

Levi, M. (2019). *Organized fraud and organizing frauds: Unpacking research on networks and organization in Transnational Financial Crime.* Routledge.

Longwe, F. (2010). *Friday Longwe.* Research proposal. Retrieved from https://core.ac.uk/download/301020064.pdf

Maake, B. M., Oino, N. N., & Awuor, F. M. (2018). M-Powering: How Mobile Money (M-PESA) Services Promote Realization of a Digital Society in the Kenyan Government. *IGI Global:In Emerging Issues and Prospects in African E-Government*, pp. 97-107.

Mansor, N., & Abdullahi, R. (2019). Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Science,*, 38-45.

Martin, C. J. (2023). *Population Census Estimates and Methods in British East Africa. In Essays on African Population.* Routledge. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9781003427643-3/population-census-estimates-methods-british-east-africa-martin

Matthew, O. M., & Mike, A. (2019). Cashless economic policy in Nigeria: A performance appraisal of the banking industry. *IOSR Journal of Business and Management, 18*(10), 01-17. Retrieved from https://www.researchgate.net/profile/Ordu-Matthew/publication/309275087

Misango, S., Njeru , P., & Kithae, P. (2020). *Analysis of industry pressure on the adoption of cashless payment system among passenger service vehicles in Nairobi city county, Kenya.* Retrieved from http://repository.seku.ac.ke/handle/123456789/3807

Mohammad, T., & Nooraini, I. (2021). Routine activity theory and juvenile delinquency: The roles of peers and family monitoring among Malaysian adolescents. *Children and Youth Services Review*, 121,. Retrieved from https://www.sciencedirect.com/science/article/pii/S0190740920322179

Msibi, N. N. (2021). *An Investigation of the Impact of Internal Quality Auditing Practices on ISO 9001 Quality Management System Performance: The Case of Company XYZ in South Africa.* University of Johannesburg (South Africa). Retrieved from https://search.proquest.com/openview

Mtonga, V. (2023). *Factors affecting tax administration in the informal sector: a case study of Lusaka district.* The University of Zambia.

Muhoro, P. G. (2023, September Wenesday). Boost informal food vendors to spur economy. *nation.africa*, p. 2. Retrieved from https://nation.africa/kenya/blogs-opinion/blogs/boost-informal-food-vendors-to-spur-economy-3965662

Mulisa, F. (2022). When Does a Researcher Choose a Quantitative, Qualitative, or Mixed Research Approach? *Interchange, 53*(1), 113-131. Retrieved from https://link.springer.com/article/10.1007/s10780-021-09447-z

Munikrishnan, U. T. (2024). Modelling the intention and adoption of cashless payment methods among the young adults in Malaysia. *Journal of Science and Technology Policy Management, 15*(2), 374-395.

Munir, M. D. (2023). Prediction of Heteroscedastic Data Using Linear Regression and Various Machine Learning Models. *Int. J. Sci. Res. in Mathematical and Statistical Sciences, 10*(1). Retrieved from https://www.researchgate.net/profile/Muhammad-Danish-Munir-3/publication/372744245

Mwabu, D. K. (2018). *Factors influencing electronic fraud in the banking industry in Kenya: a case of Kenya commercial bank central region.* Doctoral dissertation, University of Nairobi. Retrieved from http://erepository.uonbi.ac.ke/handle/11295/60487

Newman, G. R., & Clark, D. E. (2003). *Combating cybercrime: A survey of the legal issues.* London: Sweet & Maxwell.

Nurhasanah, I. S.-G. (2020). *Social Innovation in the Face of COVID-19 Pandemic.*

Otibo-Addo, E. P. (2021). *Investigating the prospects and challenges of a cashless economy in Ghana.* Doctoral dissertation. Retrieved from https://hdl.handle.net/20.500.11988/760

Otibo-Addo, E. P. (2021). *Investigating the prospects and challenges of a cashless economy in Ghana.* Doctoral dissertation.

Panda, S., & Sahoo, A. (2022). Impact of Digital Payment on Fraud: A Study of Street Vendors in Odisha. *SEDME (Small Enterprises Development, Management & Extension Journal), 49*(2), 181-191.

Pandey, P., & Pandey, M. M. (2021). Research methodology tools and techniques. *Bridge Center*.

RBA. (2023). *Annual Report 2023.* Retrieved from https://www.rba.go.ke/downloads/

Rieger, A. (2022). *Impact of COVID-19 on Security Policies of States in the Area of Cyber Security.*

Rochemont, S. (2020). *The payments revolution: Toward financial exclusion or inclusion?. In Discrimination, Vulnerable Consumers and Financial Inclusion.* Routledge. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9781003055075-7/payments-revolution-sabrina-rochemont

Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse researcher, 25*(4), 41-49.

Salehan, M., Kim, D. J., & Lee, J. N. (2018). Are there any relationships between technology and cultural values? A country-level trend study of the association between information communication technology and cultural values. *Information & Management*, 55. Retrieved from https://www.sciencedirect.com/science/article/pii/S0378720616302580

Schachter, K. (2019). The Digitalization of Development: Understanding the Role of Technology and Innovation in Development through a Case Study of Kenya and M-Pesa. *scholarship.claremont.edu*. Retrieved from https://scholarship.claremont.edu/cmc_theses/2062/

Schreck, C. J. (2017). Routine activity theory. *Preventing crime and violence*, 67-72. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-44124-5_7

Solat, S. (2017). *Security of electronic payment systems.* A comprehensive survey. Retrieved from https://arxiv.org/abs/1701.04556

Standard Media. (2023). Sunday Standard. *Kibandasky: City food vendors who feed two million Nairobians daily*. Retrieved from https://www.standardmedia.co.ke/entertainment/news/article/2001313286

Stavins, J. (2020). Credit card debt and consumer payment choice: what can we learn from credit bureau data? *Journal of Financial Services Research, 58*, 59-90. Retrieved from https://link.springer.com/article/10.1007/s10693-019-00330-8

Tade, O., & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in

Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology, 64*(16), 1717-1740. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/0306624X20928028

Taherdoost, H. (2021). A review on risk management in information systems: Risk policy, control and fraud detection. *Electronics, 10*(24), 3065. Retrieved from https://www.mdpi.com/2079-9292/10/24/3065

Transparency International . (2022). *Corruption Perception Index.* Nairobi. Retrieved from https://tikenya.org/2023/01/31/corruption-perceptions-index-2022/

Transparency International Report . (2022). *Action for Integrity.* Retrieved from https://tikenya.org/wp-content/uploads/2023/07/Action-for-Integrity_TI-Kenya-Strategic-Plan-2022-2028.pdf

Wanjau, M. S. (2020). *Illicit Financial Flows And Economic Growth In Kenya.*

Yiosese, M. O. (2020). *Auditors Independence and Quality of Financial Reporting of Listed Manufacturing Companies in Nigeria.* Master's thesis, Kwara State University (Nigeria). Retrieved from https://search.proquest.com/openview/2cb53b7f4faf1d2cca377197ae7c78d9/1?pq-origsite=gscholar&cbl=51922&diss=y

APPENDICES

APPENDIX I: QUESTIONNAIRE

Questionnaire

The purpose of this questionnaire is to gather data on the effect of various cashless economy technologies on fraud occurrence among vendors in Nairobi, Kenya. The questionnaire is subdivided into six sections. Section 1 of the questionnaire captures the demographic details of the respondents, Section 2 covers mobile money payments and fraud occurrence among vendors, Section 3 covers the credit card payments and fraud occurrence among vendors, Section 4 covers cheque payments and fraud occurrence among vendors, Section 5 covers bank transfer payments and fraud occurrence among vendors, and Section 6 covers the moderating effect of transaction value on the relationship between the cashless economy technologies and fraud occurrence among vendors. Please indicate the extent to which you agree or disagree with each of the following statements using the scale provided:

Scale:
1 = Strongly Disagree
2 = Disagree
3 = Neutral
4 = Agree
5 = Strongly Agree

SECTION A: DEMOGRAPHIC INFORMATION

1. Type of Business:

a. Fuel Station [ ]
b. Grocery Shop [ ]
c. Supermarket [ ]
d. Restaurant [ ]

2. How long have you been in business?

a. Less than 1 year [ ]
b. 1–3 years [ ]
c. 3–5 years [ ]
d. More than 5 years [ ]

3. Do you use cashless payment systems?

a. Yes [ ]
b. No [ ]

SECTION B: SPECIFIC INFORMATION

OBJECTIVE 1: MOBILE MONEY PAYMENTS AND FRAUD OCCURRENCE

N/B: Please answer the questions appropriately.

Statement	1	2	3	4	5
My business has experienced SIM swapping fraud in mobile money payments.	[ ]	[ ]	[ ]	[ ]	[ ]
Fake mobile money promotions have led to fraud in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Wrong mobile money transfers have increased fraud risks in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Fraudulent mobile money agents have targeted my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Phishing attacks related to mobile money payments have occurred in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
My business has experienced social engineering fraud through mobile money transactions.	[ ]	[ ]	[ ]	[ ]	[ ]

OBJECTIVE 2: CREDIT CARD PAYMENTS AND FRAUD OCCURRENCE

N/B: Please answer the questions appropriately.

Statement	**1**	**2**	**3**	**4**	**5**
Lost or stolen credit cards have resulted in fraud in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Skimming fraud has affected creditcard transactions in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
My business has experienced account takeover fraud throughcredit card payments.	[ ]	[ ]	[ ]	[ ]	[ ]
Card-cracking fraud cases havebeen common in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Card cloning fraud has occurred in my business's credit card payments.	[ ]	[ ]	[ ]	[ ]	[ ]

OBJECTIVE 3: CHEQUE PAYMENTS AND FRAUD OCCURRENCE

N/B: Please answer the questions appropriately.

Statement	**1**	**2**	**3**	**4**	**5**
Cheque kiting fraud hasoccurred in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Bad cheque writing has increased fraud risks in mybusiness.	[ ]	[ ]	[ ]	[ ]	[ ]
Cheque conversion fraud hasimpacted my business.	[ ]	[ ]	[ ]	[ ]	[ ]
My business has experienced cheque forgery fraud.	[ ]	[ ]	[ ]	[ ]	[ ]

OBJECTIVE 4: BANK TRANSFER PAYMENTS AND FRAUD OCCURRENCE

N/B: Please answer the questions appropriately.

Statement	**1**	**2**	**3**	**4**	**5**
My business has experienced payment fraud through bank transfers.	[ ]	[ ]	[ ]	[ ]	[ ]
Chargeback fraud has been an issue with bank transfer payments in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Identity theft has occurred during bank transfer transactions in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Cybersecurity issues related to bank transfers have caused fraud in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Card cloning fraud has been linked to bank transfers in my business.	[ ]	[ ]	[ ]	[ ]	[ ]
Credential stuffing has led to fraud in my business's bank transfers.	[ ]	[ ]	[ ]	[ ]	[ ]

OBJECTIVE 5: MODERATING EFFECT OF TRANSACTION VALUE ON THE RELATIONSHIP BETWEEN CASHLESS ECONOMY TECHNOLOGIES AND FRAUD OCCURRENCE

Survey items are rated on a Binary scale:

a) 0 = small transaction value of sh.999,999 and below.

b) 1 = sh.1M and above**.**

STATEMENT	0	1
Fraud is more likely to occur with mobile money transactions involving payments of sh.1M and above.		
Fraud is more likely in credit card transactions when the transaction value exceeds sh.1M.		
Cheque payments of sh.1M and above increase the chances of fraud in my business.		
Bank transfer payments of sh.1M and above carry a higher risk of fraud.		

FRAUD OCCURRENCE AMONG VENDORS IN NAIROBI, KENYA

Survey items are rated on a Binary scale:

a) 0 = High incidence and high impact fraud occurrence
b) 1 = Otherwise

STATEMENT	0	1
Mobile money payments		
Credit card payments		
Cheque payments		
Bank payments		

APPENDIX II:NACOSTI RESEARCH PERMIT

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **267102**

Date of Issue: **14/March/2025**

RESEARCH LICENSE

This is to Certify that Ms.. Deborah Masilau Nkini of Strathmore University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: Effect of Cashless Economy Technologies on Fraud Occurrence among Vendors in Nairobi Kenya: Moderated by the Transaction Value for the period ending : 14/March/2026.

License No: **NACOSTI/P/25/416866**

267102

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

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.

See overleaf for conditions

APPENDIX III: ETHICS APPROVAL CERTIFICATE

Strathmore UNIVERSITY

3rd March 2025

Ms Nkini Deborah,
deborah.gilliard@strathmore.edu

Dear Ms Nkini,

RE: Effect of Cashless Economy Technologies on Fraud Occurrence among Vendors in Nairobi Kenya: Moderated by the Transaction Value

This is to inform you that SU-ISERC has reviewed and **approved** your above **SU-masters** proposal. Your application reference number is **SU-ISERC2589/25.** The approval period is from **3rd March 2025 to 2nd March 2026.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

Mr Ambrose Rachier,
Chairperson; SU-ISERC

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu