THE EFFECT OF RISK MANAGEMENT PRACTICES ON FRAUD PREVENTION IN MOBILE MONEY BUSINESSES

HAZEL NINSIIMA KALINDWA

S23B33/024

A DISSERTATION SUBMITTED TO THE SCHOOL OF BUSINESS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN ACCOUNTING AND FINANCE OF UGANDA CHRISTIAN UNIVERSITY

April, 2026

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I, Kalindwa Hazel Ninsiima, declare that this research report is entirely my own original work, except were acknowledged and that this work was never submitted before to any University or Institution of higher learning for the award of a degree or certificate or for other academic purposes.

Signature: ..... Date: 01/04/2026.....

KALINDWA HAZEL NINSIIMA

APPROVAL

This research report was conducted under my supervision and has been submitted for examination with my approval

Signature: ..... Date: 01/04/2026

JENNIFER ABIYAR N. (MRS)

(Supervisor)

DEDICATION

I dedicate this dissertation to father, Mr. Isingoma Pius whose constant support and belief have given me the strength during my academic pursuit.

I would also like to dedicate this dissertation Mutebi Richard Miiro, for doing more for me than I could ever be able to thank him for.

ACKNOWLEDGEMENT

I express my gratitude to Jennifer Abiyar N. (Mrs) for her guidance during the writing of this dissertation. It’s been real.

My sincere appreciation goes to my supervisor, Jennifer Abiyar N (Mrs), whose guidance, patience and constructive feedback greatly shaped this study. Her commitment and continuous support provided direction and confidence throughout the research process. I am profoundly grateful to my family, whose encouragement and support kept me focused and determined. I thank God for the wisdom and strength and grace to finish the race.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Mobile money operations are essential for financial inclusion in Uganda; however, their sustainability is persistently jeopardized by elevated instances of fraud. This study evaluated the impact of risk management practices on fraud prevention in mobile money enterprises, utilizing Namagoma as a case study.

The research specifically investigated the impact of risk identification, risk analysis, risk mitigation strategies, and regulatory compliance. The research employed a descriptive design to examine the present circumstances. Primary data was gathered through structured questionnaires administered to a sample of 121 mobile money agents. The study achieved a response rate of 76.9%, resulting in 93 completed questionnaires. The data was subsequently analysed utilizing descriptive statistics within the Statistical Package for the Social Sciences.

The findings indicated that risk identification facilitates the early detection of suspicious behaviour; however, numerous agents depend on informal peer learning instead of formal training. Risk analysis predominantly depends on insights gained from historical incidents instead of utilizing sophisticated digital tools. Although mitigation controls such as transaction monitoring are considered effective, agents often circumvent security protocols to expedite service for trusted clients, thereby creating vulnerabilities that may elevate fraud risk and compromise the overall efficacy of the risk management framework. Regulatory compliance, including compulsory SIM registration and Know-Your-Customer (KYC) regulations, serves as the foremost safeguard against fraud by eliminating anonymity in transactions.

The study concluded that human behaviour and structural business challenges, such as low agent commissions, significantly undermine risk management practices. It is advised that service providers enforce compulsory formal training and reassess commission structures to alleviate the financial pressures that contribute to internal theft. Moreover, mobile money agents must rigorously comply with security protocols for all clients and prioritize fundamental physical security investments.

CHAPTER 1

INTRODUCTION

1.0 Introduction

This chapter is a presentation of the background of the study, statement of problem, general and specific objectives, research questions, scope, and significance of the study. It concludes with the conceptual framework which gives a picture of the relationship between risk management practices and fraud prevention.

1.2 Background of the Study

The effectiveness of fraud prevention in the 21st Century has been improved by its transformation from a reactive and strict process to a hands-on and technologically combined subject. (Mappanyukki et al., 2024). The origin of fraud prevention traces back to the Mail Fraud Statute of 1987 in the United States where fraudulent actors were prosecuted by authorities who were empowered by the statute.(USPIS, 2023). Fraud schemes in the early day like the Green Goods and Millionaires Clubs scams relied heavily on deception through goods which were counterfeit and fixed games respectively. This showed that the early approaches to fraud prevention where divided as they were largely based on these schemes

(USPIS, 2023). The early methods of fraud prevention often limited the possibility of recovery of losses in a timely manner because they relied heavily on manually reviewing the fraud crimes after they had occurred. (SAS, 2024). The early approaches to fraud prevention were a display of the early Risk management theory perspective. It suggested that risk was addressed only after the realization of it happening instead of systematic anticipation and prevention. (Ali et al., 2020).

In the late 1980's, technological improvements changed fraud prevention from an practical and analytical process. The technological improvements led to the adoption of new systems by financial institutions. These new systems were capable of processing large volumes of transaction data in order to identify any irregularities that came up in real time. (IBM, 2024). The capacity of fraud prevention systems has since improved due to the rise of machine learning and deep learning techniques. It has enabled the fraud prevention systems to detect complicated fraud patterns (Chen, 2025). The introduction of more strict auditing standard by the International

Auditing and Assurance Standards Board (IAASB) has reinforced the transformation of the fraud prevention process. These standards require auditors to assess fraud risk in their reviews. (IAASB, 2025). Organisations have now been able to anticipate fraudulent activity and respond to it more effectively due to the integration of predictive and adaptive analytics of fraud. (SAS, 2024; ACFE, 2020). However, the Agency theory puts emphasis on the fact that the persistence of fraud with in financial institutions is influenced by the weak supervision and irregular information between the principals and agents.

In the global perspective, both developed and developing economies have shown that fraud prevention has been strengthened by the combination of technology and regulatory frameworks. In the United Kingdom and France, technology-based fraud management systems and multi-factor authentication have reduced online transactional fraud and significantly improved institutional flexibility. (Ken Research, 2024; EPC AISBL, 2024). Across Asia, countries such as India, China, and Singapore have embraced the use of real time monitoring systems for fraud, biometric authentication, and national digital identity platforms. These systems reduce impersonation cases and identity-based fraud crimes. (Interpol, 2024; Edu. J et al., 2023). In Africa, nations such as Nigeria, Kenya and South Africa have implemented the use of advanced biometric verification and transaction monitoring frameworks. They safeguard financial transactions against fraud (Dojah, 2024;Sumsub, 2023). On the other hand, Uganda does not have a unified biometric verification for users of mobile money. It depend on manual identification processes which are that are not consistently enforced (Katamba & Namuli, 2024). This gap in fraud prevention weakens enforcement and the overall effectiveness of fraud prevention frameworks.

Despite this, Ugandan financial institutions like commercial banks and mobile money operators have adopted other fraud prevention measures like transaction limits, PIN controls, and real-time monitoring in order to control fraud. (Kyuspace, 2024). These initiatives by Uganda have been supported by public education campaigns and infrastructure investments. Despite these initiatives, limitations like weak enforcement and limited integration of technology have been faced. (CGAP, 2022). Uganda reported mobile money fraud losses amounting to UGX 19.2 billion in the year 2022 and in the following year the cybercrime report documented 245 cases valued at UGX 1.5 billion (Katamba & Namuli, 2024; EPRC, 2024). These statistics highlight

the difference between policy design and implementation. This situation is consistent with the Agency Theory which weak control or supervision of agents.

1.2 Statement of the Problem

Mobile money operations in Uganda should be able to provide secure, transparent, and reliable financial services to Ugandans. This would promote enhance financial inclusion and strengthen user confidence in mobile money services. Effective risk management practices like as proper customer verification, transaction monitoring, employee training, and compliance with regulatory standards should reduce fraud and protect service providers and users. In this ideal context, consistent application of these risk management measures would ensure operational honesty and promote viable growth in the mobile money sector. In practice, mobile money is essentially an element of financial inclusion in Uganda. Despite this but its viability is continuously threatened by high levels of fraud which often result in significant annual financial losses for users (Katamba & Namuli, 2024; EPRC, 2024). Various measures of risk management practices have been implemented by mobile money companies but their effect on fraud prevention remains underexplored. Regulators and service providers have introduced practices such as Know-Your-Customer (KYC) protocols, mandatory SIM card registration, and agent-level transaction limits. The weak implementation of risk identification, analysis, mitigation, and compliance practices continues to expose businesses and users to fraud. Additionally , limited technology adoption, inadequate employee training, and poor organizational culture may influence how these risk management practices transform into effective fraud prevention outcomes.

Consequently, there is limited empirical evidence on the effect of risk management practices on fraud prevention in mobile money operations. Therefore, this study sought to examine the effect of risk identification, analysis, mitigation, and regulatory compliance on fraud prevention in Namagoma.

1.3 General Objective

To assess the effect of risk management practices on fraud prevention in mobile money businesses, using Namagoma as a case study.

1.4 Specific Objectives

I. To determine the effect of risk identification practices on fraud prevention in mobile money businesses.

II. To examine the effect of risk analysis practices on fraud prevention in mobile money services.

III. To assess the effect of risk mitigation strategies on fraud prevention in mobile money transactions.

IV. To evaluate the effect of regulatory compliance on fraud prevention in mobile money operations.

1.5 Research Questions

I. What is the effect of risk identification practices on fraud prevention in mobile money businesses?

II. What is the effect of risk analysis practices on fraud prevention in mobile money services?

III. What is the effect of the strategies of risk mitigation on fraud prevention in mobile money businesses?

IV. What is the effect of regulatory compliance on fraud prevention in mobile money businesses?

1.6 Scope of Study

1.6.1 Geographical

The study was conducted in Namagoma village. It is a busy shopping center located along Masaka Road in Wakiso District. It was chosen because of its high number of active mobile money agents and local community who use mobile money services. They are the relevant population for the study

1.6.2 Content

The study aimed find out the relationship between risk management practices and fraud prevention in mobile money businesses. It specifically covered risk identification, analysis, mitigation and regulatory compliance.

1.6.3 Time

The study considered the period between 2020 and 2025. This was because it had information on recent technological advances and regulatory changes. This choice ensured that the findings of the study reflected the current risk management practices.

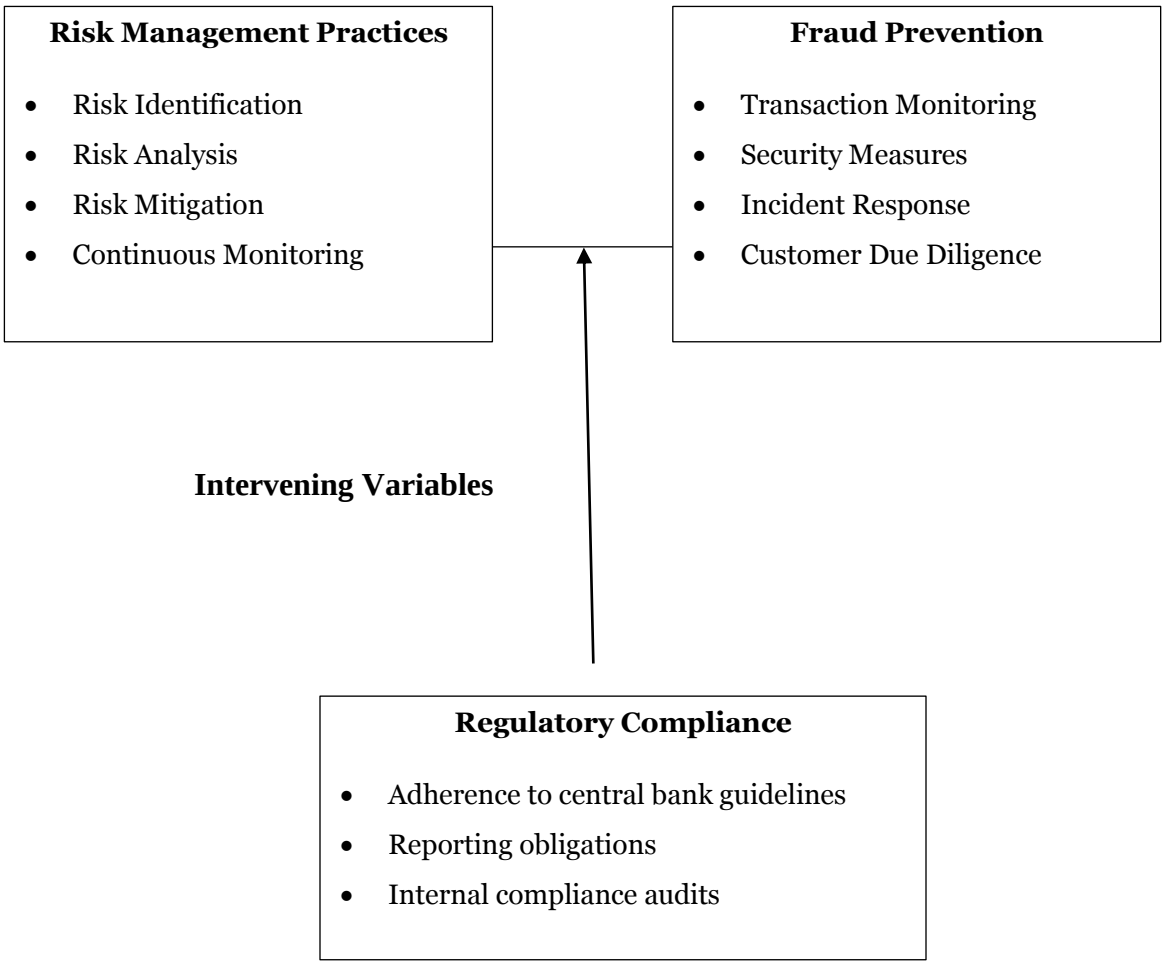
1.7 Significance of the Research

The findings showed that risk management practices can mitigate fraud risks, safeguard customer funds, and boost customer trust. This is important for the growth of the business. enhance the trust essential for sustainable growth among service providers. This information also enabled mobile money agents to improve their fraud prevention strategies through the application of real-world evidence leading to a decrease of fraud cases.

Regulatory bodies, such as the Bank of Uganda and the Uganda Communications Commission, used this study to evaluate the practical effects of the current policies and regulatory structures. This enabled them to formulate and enforce evidence-based policies that promote a secure and stable financial services environment. This in turn safeguards consumers and ensures the integrity of the national payment system.

1.8 Conceptual Framework

Independent Variable **Dependent Variable**



Source: Researcher's own creation

Figure 1.1: Conceptual framework showing the relationship between risk management practices and fraud prevention in Mobile Money Businesses.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This chapter present current literature on the effect of risk management practices on fraud prevention in mobile money businesses in Uganda. The literature focused of four main components. They are Risk identification, analysis, mitigation and regulatory compliance.

2.1 Definitions of Key Terms

According to the Institute of Internal Auditors (IIA), Risk Management is defined as the process of identifying, assessing, managing events to give a reasonable assurance to an organisation about achieving its goals. (Tsyhankov, 2023). This definition shows that risk management is a procedure which is focused on control. Purdy (2020) defines risk management an effort coordinated by stakeholders to guide and regulate an organisation to avoid risk. This effort is aimed at safeguarding and creating value for the stakeholders.

Research shows that fraud prevention can views a hands-on measures and strategies to prevent fraud from happening. It includes reviewing internet controls, employee training and security policies. (Button, 2022). This definition is based on the effective implementation of measures. Fraud prevention is also defined as the process of applying advanced analytics and machine learning methodologies to monitor transactions in real-time. This process aims to detect and prevent fraudulent activities before they happen. (Al-Thani et al., 2022).

Mobile money can be defined as an electronic wallet service which enabling users to store, transmit, and receive funds through their mobile devices (Otiwu et al., 2022). 2). This definition emphasizes the fundamental technological service. On the other hand, other scholars define mobile money as a transformative financial service that makes use of mobile technology to enhance financial inclusion for unbanked and underbanked populations. It thus facilitates access to savings, credit, and insurance (Alhassan et al., 2023).

Risk identification is seen as either a discrete first step in fraud prevention or a continuous process in risk management. A foundational view defines it as the process of finding, recognizing, and describing risks that might help or hinder the achievement of objectives

(International Organization for Standardization, as cited in Purdy (2020). This portrays it as the initial stage of risk management. Another definition is that it is a "continuous and iterative process that involves systematically identifying new and emerging risks arising from changes in the internal and external context," such as new technologies or fraud schemes (Tchankova, 2023). While the ISO definition presents it as a foundational step, Tchankova (2023) emphasizes that in a fast-changing environment like mobile money, risk identification cannot be a one-off activity but must be an ongoing surveillance process.

Risk Analysis is commonly defined states as the process to comprehend the nature of risk and to determine the level of risk (Purdy, 2020). Scholars usually approach risk analysis by emphasizing its different components which are understanding the risk and estimating its impact. Another scholar describes it as the process of evaluating the identified risks in terms of their likelihood of occurrence and the potential magnitude of their consequences (Button, 2022). Purdy's (2020) definition is holistic, focusing on the overall objective of understanding risk levels while Button's (2022) definition of risk analysis is more operational, specifying the two key variables which are likelihood and impact that must be assessed.

Risk mitigation is commonly defined as the actions taken to address risks, though definitions differ on the range of available actions. A focused definition describes it as the process of selecting and implementing options for addressing risk, with the goal of modifying it, often by reducing its likelihood or negative consequences Purdy (2020). A more comprehensive view, however, includes a wider set of strategies, defining mitigation as taking action to reduce the exposure to a risk, either by lessening its likelihood, its potential impact, or both. It can also involve risk avoidance, transfer (e.g., through insurance), or acceptance Tchankova (2023).

2.2 Conceptual review

2.2.1 The Impact of Risk Identification Practices on Fraud Prevention in Mobile Money Enterprises

Financial accessibility has been improved by the abundance if of mobile money services in Uganda. This abundance has left the mobile money sector exposed to a number of fraud risks. Early identification of risks has become important due to the rise in the number of mobile money transactions because it protects both the consumers and service providers. Efficient risk

identification enable transactions to understand the weak areas. These include identity theft, authentication failures, and agent-related fraud. These issues can result into big losses when they are not detect early. Risk identification establishes the basis of a comprehensive risk management framework by facilitating prompt responses and focused preventive measures.

. Guma Ali et al. (2020) and Medrine Kyomuhendo et al. (2025) agree that that identity theft, authentication attacks, and agent-driven fraud among the biggest risk that make risk identification important. Mackenzie et al. (2024) established a statistically significant positive correlation between the frequency of risk assessments in an organisational and a decrease in fraud threat incidents inside the organisation. This evidence emphasizes the fact that that regular risk identification improves the ability of the concerned parties to detect and prevent fraud. Arim et al. (2022) pointed out that technological deficiencies, inadequate talent management, and criminal activities are heavy risks that also necessitate proactive identification in Uganda's mobile money.

Despite the fact that the above literature agrees on the categories of risk, other studies show discrepancies emerging in the interpretation of the relationship between risk identification and fraud preventions. Guma Ali et al. (2020) emphasized the importance of technical measures like enhanced access controls, strict supervision of high value transactions and efficient legal frameworks. Bongomin et al. (2020) argued that consumer protection serves an important mediating function in fraud prevention. He suggests that merely identifying risks does not stop fraud from happening without sufficient user protection. Kyomuhendo et al. (2025) also emphasizes that technical identification should be complemented by educating users and using fraud detection systems to monitor fraud in real time. The findings of these scholars suggest that technology-driven measures are most effective when they integrated with human-centred interventions. Mackenzie et al. (2024) found out that that 88 percent of organizations utilized access control systems, while 80 percent instituted security awareness training in their study. This reflects, significant organizational focus on risk management practices.

Milly et al. (2021) noted that when there is a high risk perceived with caring out mobile money transactions, it diminishes the adoption of mobile money and banking. This suggests that suggesting that the identification of risks may discourage users despite improving security. Users despite enhancing security. Museba et al. (2021) argues that that effective communication

of transparency in risk management significantly improves user confidence. This shows that user perception and communication are essential in in determining the efficiency of risk identification initiatives. Arinze et al. (2024) aligns these conflicting perspectives by insisting that effective risk identification makes balance between enhanced security and a favourable user experience necessary. They also caution that cautioning that excessively strict identification protocols may drive users towards informal financial systems. This perspective aligns with Arim et al. (2022), who similarly emphasize the necessity of balancing IT security expenditure with customer satisfaction.

2.2.2 The Effect of Risk Analysis on Fraud Prevention In Mobile Money Businesses

Effective risk analysis is important due to the necessity for risk identification, as the swift expansion of mobile money services in Uganda has generated new opportunities for financial inclusion while simultaneously heightening exposure to fraud risks.

Mobile money businesses depend data-driven risk analysis to identify and mitigate potential threats of fraud Risk analysis allows mobile money operators to identify areas prone to fraud, analyse transaction patterns, and anticipate fraudulent activities before their occurrence. The efficiency of risk analysis is dependent upon the combination of technology, human discernment, and regulatory frameworks into daily mobile money operations. , as this integration can this combination significantly enhances the accuracy and responsiveness of fraud detection systems. Many scholars have investigated the usefulness of technological solutions in risk analysis. Botchey et al. (2020) presented convincing empirical evidence supporting the application of machine learning. The research indicated that gradient boosted decision trees attained remarkable detection rates of 99.90 percent accuracy, 99.99 percent precision, and 100 percent recall in the analysis of fraud in mobile money transactions. These finding also proposed the potential of artificial intelligence in detecting fraudulent activity. On the other hand, Guma Ali et al. (2020) argued that that technological weaknesses like authentication attacks and identity theft continue to exist despite improved access controls and monitoring systems. A study involving 1,240 participants in Uganda demonstrated technological interventions in fraud prevention. In order to build on this Arinze et al. (2024) noted that new technologies like as biometric identification, artificial intelligence, and blockchain have enhanced financial security.

Researchers also emphasize human-centred risk analysis practices beyond technical solutions to fraud. Guma Ali et al. (2020) reported support for human-focused strategies backed with statistics. 60.9 percent of respondents agreed that customer awareness campaigns are crucial for fraud prevention. The other 60.4 percent of respondents agreed on the importance of agent training. These findings emphasize that educating users and empowering agents are important parties in effective fraud prevention. Arim et al. (2022) pointed out persistent challenges in the execution. These challenges include poor communication, liquidity shortages, agent inactivity, and unsatisfactory customer experiences. These operational challenges limit the potential impact of human-centred practices even when their value is well recognized. Bongomin et al. (2020) also found that digital consumer protection is a good way to reduce fraud. It has both direct and indirect positive effects on the use of mobile money. Their evidence strengthens the case for integrating consumer protection into risk analysis frameworks.

2.2.3 The Effect of Risk Mitigation Strategies on Fraud Prevention in Mobile Money Businesses

The risk mitigation strategies include things like transaction monitoring, employee training, multi-factor authentication, and customer awareness initiatives. These risk mitigation measures aim to control the effects of fraud after potential risks have been identified and assessed. Effective risk mitigation in mobile money businesses improves consumer confidence by far. It also safeguards institutional assets, and maintains financial stability. Assessing the impact of these risk management strategies on fraud prevention helps in identifying which ones are most effective.

A study by Guma Ali et al. (2020) indicated that 53 percent of Ugandan mobile money agents experienced fraud at some point. Their study highlighted significant threats of fraud including identity theft, authentication breaches, and vishing attacks. Mackenzie et al. (2024) also provided convincing evidence of fraud prevention by identifying a positive correlation between routine risk assessments and diminished insider threats. Their findings demonstrate that organizations which implement security policies against fraud like access controls, and security awareness training encountered reduced instances of fraud.

Academics in many studies disagree regarding the effective of human-centred fraud prevention. Guma Ali et al. (2020) noted that customer awareness campaigns were supported as an effective

method of preventing fraud. These findings indicate perceived effectiveness and not actual effectiveness. Bongomin et al. (2020) explained that digital consumer protection substantially bridges the connection between mobile money adoption and financial inclusion. This outcome illustrates that consumer protection improves confidence and utilization and also mitigates fraud. Arim et al. (2022) disagreed with this perspective by noting that although banks invest in customer education, they often lack effective risk information systems to underpin these initiatives. This gap indicates that human-centred strategies make institutional and technological support necessary in order to be genuinely effective.

Botchey et al. (2020) strongly advocated for mitigation based on technology. The study references machine learning algorithms that attained detection accuracy of fraud in experimental settings. In contrast, Guma Ali et al. (2020) highlighted procedural strategies of fraud prevention which include access controls, agent training, and monitoring of high-value transactions. Arim et al. (2022) in his study, proposed a comprehensive model that actually combines these approaches of fraud prevention. The study suggests that a combination of strategies more effectively mitigate digital risks. Their qualitative findings indicated that traditional frameworks such as ISO 31000 frequently fail to address complicated fraud cases.

2.2.4 The Effect of Regulatory Compliance on Fraud Prevention in Mobile Money Business

The efficiency of technical, human, and procedural controls depends on the strength of regulatory compliance in mitigating fraud in mobile money businesses. The quick expansion of mobile money services throughout Uganda and East Africa has increased the focus on regulatory compliance. Despite the fact that digital financial services progress in promote financial inclusion, researchers emphasize the importance of effective regulatory compliance to mitigate security vulnerabilities and maintain system integrity.

Recent studies consistently agree that strong regulatory monitoring in important in fraud prevention. Guma Ali et al. (2020) listed a number of security challenges within Uganda's mobile money sector. The security challenges include identity theft, authentication breaches, and agent fraud. These challenges emphasized that implementing a comprehensive legal framework was essential in enhancing oversight and accountability. George Okello Candiya and Bongomin et al. (2020) pushed for more cooperative measures among regulators, mobile money businesses, and mobile operators in order to implement more strict legislations against people who commit

fraud. Jimmy Ebong et al. (2021) put forward that enhanced regulatory frameworks are important in the mitigation of digital risks.

In spite of this agreement, scholars differ in their perspectives on the implementation of regulations. Guma Ali et al. (2020) stressed that operational strategies including access controls, customer education, and agent training promote strict following of regulations. Bongomin et al. (2020) emphasized the digital consumer protection is also important in safeguarding user rights. E. Arinze et al. (2024) asserted that lessening cybersecurity threats, regulatory fragmentation, and consumer scepticism calls for collaboration among the various stakeholders in the mobile money sector.

The literature also shows the unintended consequences of regulatory compliance Lorna Katusiime et al. (2021) discovered that the mobile money tax negatively affected usage in both the short and long term. This suggests that specific interventions may hinder adoption of mobile money services. Bongomin et al. (2020) argues that consumer protection measures boost inclusion and trust.

2.3 Conclusion

The literature which was used indicates that fraud prevention in mobile money businesses relies on the effectiveness of implementing risk identification, analysis, mitigation, and adherence to regulations in their daily operations.

CHAPTER 3

METHODOLOGY

3.0 Introduction

This chapter is a presentation of the research design of the study, study population, sample size and the sampling method. It also includes the methods of data collection, data collection instruments, data sources, data analysis techniques and the data quality control measures. Finally, the chapter concludes with the ethical considerations, study limitations, and strategies for overcoming suggested limitations.

3.1 Research Design

The study used the descriptive research design. The research design facilitated a detailed assessment of the effect risk management practices on fraud prevention through observation and recording of variables in the mobile money businesses in Namagoma.

3.2 Study Population

The study population consisted of all the mobile money agents doing business within Namagoma Village. The study aimed at utilizing the population of 176 mobile money businesses in the area. This population was divided into two distinct categories which included 66 agents who pay full operating licenses for their mobile money businesses, and 110 agents who run mobile money business alongside other businesses.

3.3 Sample Size

The sample size was calculated as 121 (Krejcie and Morgan, 1970) mobile money agents from the study population of 176 agents in Namagoma Village.

3.4 Sampling Method

The stratified random sampling technique was used for the study. It ensured that every registered agent had an equal chance of being chosen for the study. Agents who had operated for at least one year in Namagoma Village were selected to ensure that the sample size possessed adequate experience with risk management and fraud prevention practices.

3.5 Data Sources

Both primary and secondary sources of data were used for the study

3.5.1 Primary Data

The primary data include the direct responses from mobile money agents in Namagoma Village. It was obtained through the questionnaires issued to them.

3.5.2 Secondary Data

The secondary data include published documents like including academic journals, reports and telecom industry records. The provided support for the primary findings of the study.

3.6 Methods of Data Collection

The questionnaire was the primary method of data collection for this study. This method was chosen to gather firsthand quantifiable data from mobile money agents. The questionnaire ensured a high level of consistency across all participants.

3.7 Data Collection Instruments

The questionnaire was the primary research instrument. It was designed to gather both quantitative and qualitative data from the agents.

3.8 Data Analysis

The questionnaires underwent a thorough review for completeness and accuracy. The data was then coded and entered into the Statistical Package for the Social Sciences (SPSS) to process the data.

3.9 Data Quality Control

A thorough set of procedures was implemented for the questionnaire to ensure the quality and credibility of the collected data.

3.9.1 Validity

The validity of the study was established using the Content Validity Index. This involved submitting the questionnaires to eligible experts who rated the relevance of each item. This

ensured that the questionnaire measured the variables of risk management and fraud prevention in Namagoma Village

3.9.2 Reliability

The reliability was established using a pilot test. It was conducted with 5 mobile money agents the area. They were excluded from the final study sample.

3.10 Ethical Considerations

The study strictly followed the established ethical standards for research. Informed consent was prioritized during data collection from the mobile money agents. I provided a clear explanation of the purpose and procedures of the study. I also ensuring that participants understood that their participation was entirely voluntary and that they had the right to withdraw at any stage without consequence.

3.11 Limitations and Delimitations of the Study

There were a number of limitations faced during the study but they were addressed through the employment of different strategies.

The study design limited the ability for the findings to be generalised. This was solved by focusing deep contextual insights that established a foundation for future research,

The heavy reliance on self-reported data was also a significant limitation in the study and it brought about bias. It was minimized by ensuring the mobile money agents of absolute confidentiality to encourage honest responses.

There was hesitation in disclosure by some mobile money agents due to the sensitive nature of fraud caused. This challenge was overcome by building strong rapport with them.

CHAPTER 4

PRESENTATIONS, ANALYSIS AND INTERPRETATION OF FINDINGS

4.0 Introduction

The chapter presents findings On "The Effect Of Risk Management Practices On Fraud Prevention In Mobile Money Businesses In Namagoma". This chapter starts by showing the response rate, followed the demographic findings of the study and finally descriptive presentation and analysis of the study findings in relation to specific objectives.

4.1 Findings of the study

4.1.1 Response rate

A total of 121 questionnaires were distributed to mobile money agents in Namagoma. The table below shows the distribution of responses.

Table 1: Table showing the response rate of respondents

Category	Frequency	Percent
Responses Received	**93**	**76.9%**
Non-responses	**28**	**23.1%**
Total	**121**	**100.0%**

Source: Primary Data

Out of the 121 questionnaires distributed, 93 were successfully filled and returned, yielding a response rate of 76.9%. While there was a non-response rate of 23.1%, the 93 participants represent a significant majority and provide a high level of engagement to ensure the data is representative of the target population.

4.2 Demographic findings of the study

The demographic characteristics are represented by gender, age bracket, highest level of education attained, time worked in mobile money business and number of mobile money transactions processed in a day.

4.2.1 Gender of respondents

The findings on the gender composition are represented in the table below;

Table 2: Table showing the gender of respondents

Gender (1=Male,2=Female)					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	30	32.3	32.3	32.3
	2	63	67.7	67.7	100.0
	Total	93	100.0	100.0	

Source: Primary Data

The findings in the table show that the majority of the respondents were females, representing 67.7% of the sample, while male respondents accounted for 32.3%. This means that majority of mobile money business in Namagoma Village are operated by women.

4.2.2 Findings on the age group of respondents

The table below presents the findings on the age group of the respondents;

Table 3: Table showing the age group of respondents

Age (1=18-27, 2=28-37, 3=38-47, 4=48-57, 5=57+)					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	54	58.1	58.1	58.1
	2	28	30.3	30.3	88.4
	3	10	10.7	10.7	100.0
	5	0	0.0	0.0	
	Total	93	100.0	100.0	

Source: Primary Data

The findings show that the majority of the mobile money agents (58.1%) fell within the 18–27 age bracket. This was followed by the 28–37 age group consisting of 30.3%, the 38–47 group having 10.7%, and those aged 57 and above at 0.0%. These results show that mobile money agents in Namagoma Village are mainly young individuals.

4.2.3 Findings on the Highest level of education attained

The table below shows the findings on the highest level of education attained by respondents.

Table 4: Table showing the highest level of education attained by respondents

Education (1=Primary, 2=Secondary, 3=University, 4=Other)					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	69	74.2	74.2	74.2
	3	16	17.2	17.2	91.4
	4	8	8.6	8.6	100.0
	Total	93	100.0	100.0	

Source: Primary Data

The findings show that the largest proportion of mobile money agents in Namagoma Village (74.2%), had attained a secondary level of education. Mobile money agents with a university education made up 17.2% while 8.6% of them fell into the "Other" category.

4.2.4 Findings on the Time worked in mobile money business

The table below represents the findings on the time worked in mobile money business in Namagoma.

Table 5: A Table showing the time worked in mobile money business in Namagoma

Experience (1=Below 1 yr, 2=1-3 yrs, 3=3-5 yrs, 4=Above 5 yrs)					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	28	30.1	30.1	30.1
	2	37	39.8	39.8	69.9
	3	21	22.6	22.6	92.5
	4	7	7.5	7.5	100.0
	Total	93	100.0	100.0	

Source: Primary Data

These findings show that the highest percentage of mobile money agents (39.8%) in Namagoma Village had worked in the mobile money business for 1 to 3 years. Agents who had worked for less than 1 year accounted for 30.1%, followed by those with 3 to 5 years (22.6%). Finally, those with over 5 years of experience reported 7.5%. These results show that majority of mobile

money agents possess a reasonable amount of practical experience in the mobile money industry.

4.2.5 Number of mobile money transactions processed in a day

The findings on the number of mobile money transactions processed in a day by respondents are represented in the table below;

Table 6: Table showing the number of mobile money transactions processed in a day by respondents

Transactions Per Day (1=0-50, 2=51-100, 3=101-200, 4=200+, 5=Not Sure)					
		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**1**	**31**	**33.3**	**33.3**	**33.3**
	2	**25**	**26.9**	**26.9**	**60.2**
	3	**14**	**15.1**	**15.1**	**75.3**
	4	**9**	**9.7**	**9.7**	**85.0**
	5	**14**	**15.0**	**15.0**	**100.0**
	Total	**93**	**100.0**	**100.0**	

Source: Primary Data

The findings in the table show that a majority of the respondents (33.3%) process between 0 and 50 mobile money transactions per day. This is followed by 26.9% who process 51-100 transactions, 15.1% processing 101-200 transactions, and 9.7% handling over 200 transactions daily. Additionally, there were 15.0% of the respondents were unsure of their daily transaction volume. These findings point out that most mobile money agents handle a low to moderate volume of daily transactions.

4.3 Findings on the effect of risk identification practices on fraud prevention

The findings are based on a Likert scale of 1: Strongly Disagree, 2: Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly Agree.

Table 7: Table showing findings on the effect of risk identification practices on fraud prevention

Descriptive Statistics		
	Mean	**Std. Deviation**
We received formal training on fraud prevention from our mobile money provider.	**3.82**	**1.48**
We are well-trained to identify common fraud risks like SIM swaps and phishing.	**3.71**	**1.55**
We have clear procedures for identifying suspicious customer behaviour or transactions.	**3.78**	**1.32**
Our systems effectively flag technological weaknesses (e.g., authentication failures).	**3.35**	**1.310**
We have control measures that easily identify potential internal fraud or collusion.	**3.51**	**1.470**
Regularly identifying new risks has directly helped us prevent fraud incidents.	**4.02**	**1.055**
We struggle to stay updated on new fraud tricks used by criminals in this area.	**2.81**	**1.587**
Our manual identification processes (e.g., checking IDs) make it hard to spot fakes.	**3.75**	**1.398**
We rarely receive timely alerts about new fraud types from our service providers.	**2.76**	**1.470**
We usually only identify risks after a fraud incident has already occurred.	**2.18**	**1.326**

Source: Primary Data

The mean scores were interpreted in a way that statements with a mean above 3.0 indicated a trend toward agreement, questions with a mean around 3.0 indicated a neutral stance and statements with a mean below 3.0 indicated a trend towards disagreement. The findings in the table above show that the respondents generally agreed that regularly identifying risks has

helped the prevent fraud incidents reflected by the highest mean score of 4.02 and a standard deviation of 1.055. Respondents also agreed that they received formal training on fraud prevention (Mean = 3.82, SD = 1.48) and have clear procedures for identifying suspicious behaviour (Mean = 3.78, SD = 1.32).

On the other hand, the respondents largely disagreed with the statement that they usually only identify risks after a fraud incident has already occurred, which is reflected by the lowest mean score of 2.18 and a standard deviation of 1.326. Overall, the findings imply that mobile money agents in Namagoma have adopted a proactive approach to risk identification rather than waiting for fraud to happen.

4.4 Findings on the effect of risk analysis on fraud prevention

The findings are based on a Likert scale of 1: Strongly Disagree, 2: Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly Agree.

Table 8: Table showing findings on the effect of risk analysis on fraud prevention

Descriptive Statistics		
	Mean	**Std. Deviation**
We effectively analyse the likelihood and impact of the fraud risks we identify.	**3.91**	**1.259**
Our business uses real-time transaction monitoring to analyse unusual patterns.	**3.82**	**1.31**
Customer awareness campaigns help us analyse and respond to new fraud trends.	**4.22**	**1.10**
The training we receive helps us analyse situations to determine if they are fraud.	**4.05**	**1.24**
Our analysis of past fraud incidents helps us predict and prevent future ones.	**4.41**	**0.92**
We classify risks according to their severity when identified.	**3.65**	**1.43**
We lack sufficient historical records to accurately estimate future fraud risks.	**3.3788**	**1.58614**
The complexity of digital systems makes it hard to understand how	**3.9242**	**1.36224**

fraud happens.		
Pressure to serve customers quickly prevents us from analysing suspicious deals.	**3.2727**	**1.70561**
We do not have the right tools to deeply analyse transaction patterns.	**3.3485**	**1.60281**

Source: Primary Data

The findings in the table above show strong agreement among respondents that analysing past fraud incidents helps predict and prevent future ones, reflected by a high mean score of 4.41 and a standard deviation of 0.92. Respondents also agreed that customer awareness campaigns help them in analysing and responding to new fraud trends that may occur (Mean = 4.22, SD = 1.10), and that their training helps them analyse situations to determine potential fraud (Mean = 4.05, SD = 1.24).

On the other hand, the statement suggesting that pressure to serve customers quickly prevents them from analysing suspicious deals recorded the lowest mean score of 3.27 with a standard deviation of 1.706, indicating a more neutral stance. The results indicate that risk analysis in this sector is heavily driven by experiential learning and customer interactions rather than advanced digital tools.

4.5 Findings on the effect of risk mitigation strategies on fraud prevention

The findings are based on a Likert scale of 1: Strongly Disagree, 2: Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly Agree.

Table 9: Table showing findings on the effect of risk mitigation strategies on fraud prevention

Descriptive Statistics		
	Mean	Std. Deviation
Transaction limits (e.g., daily limits) are effective for reducing fraud losses.	3.14	1.644
Security awareness training for agents is one of the best ways to mitigate fraud.	4.35	1.051
ID Verification for large transactions effectively reduces fraud.	3.14	1.616

We have a clear incident response plan for what to do immediately after fraud.	2.59	1.569
Continuous monitoring of transactions effectively identifies and stops fraud.	4.08	1.101
We reconcile cash and e-float daily to detect discrepancies.	4.01	1.063
We sometimes bypass security protocols to speed up service for trusted clients.	4.06	1.153
Strict fraud prevention measures often result in losing impatient customers.	2.3333	1.36250
The lack of biometric tools (e.g., fingerprint scanners) makes mitigation difficult.	3.2273	1.52714
Employees frequently forget to strictly follow established security limits.	2.8030	1.57108

Source: Primary Data

The mean scores were interpreted in a way that statements with a mean above 3.0 indicated a trend toward agreement, questions with a mean around 3.0 indicated a neutral stance and statements with a mean below 3.0 indicated a trend towards disagreement. The findings on the effect of risk mitigation strategies on fraud prevention show that respondents strongly agreed that security awareness training for agents is one of the best ways to mitigate fraud reflected by the mean score of 4.35 and a standard deviation of 1.051. Continuous monitoring of transactions (Mean = 4.08, SD = 1.101) and daily reconciliation of cash and e-float (Mean = 4.01, SD = 1.063) were also seen as highly effective operational controls.

The respondents also agreed that they sometimes bypass security protocols to speed up service for trusted clients (Mean = 4.06, SD = 1.153). Furthermore, respondents disagreed that strict measures result in losing impatient customers (Mean = 2.33, SD = 1.363), and they indicated a lack of clear incident response plans for immediate action after fraud occurs (Mean = 2.59, SD = 1.569).

Ultimately, the finding reveal that while agents prioritize fraud mitigation like training and cash reconciliation, these efforts are weakened by the fact that some of the bypass security protocols

for trusted clients. Consequently, the mobile money agents remain largely unprepared to manage the impact of fraud when it occurs

4.6 Findings on the effect of regulatory compliance on fraud prevention

The findings are based on a Likert scale of 1: Strongly Disagree, 2: Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly Agree.

Table 10: Table showing findings on the effect of regulatory compliance on fraud prevention

Descriptive Statistics		
	Mean	**Std. Deviation**
Strictly following Know-Your-Customer (KYC) protocols helps prevent fraud.	**4.05**	**1.04**
Mandatory SIM card registration rules have been effective in reducing fraud.	**4.10**	**1.187**
Adhering to Bank of Uganda guidelines is essential for our fraud prevention.	**3.83**	**1.399**
Internal compliance audits by the provider help us fix control weaknesses.	**3.79**	**1.295**
We find the regulatory rules for mobile money to be clear and easy to follow.	**4.21**	**1.021**
Regulatory requirements are often too complex for us to implement fully.	**3.5455**	**1.41619**
Compliance costs (e.g., licenses) reduce our ability to invest in security tools.	**3.3485**	**1.59318**
Regulatory enforcement in Namagoma is inconsistent and weak.	**3.3636**	**1.56536**
The process for reporting suspicious activities to regulators is difficult.	**3.2727**	**1.64125**
There is a gap between official regulations and what is practical in our daily work.	**2.483**	**1.42114**

Source: Primary Data

The mean scores were interpreted in a way that statements with a mean above 3.0 indicated a trend toward agreement, questions with a mean around 3.0 indicated a neutral stance and statements with a mean below 3.0 indicated a trend towards disagreement. The findings in the above table above show that mobile money agents in Namagoma generally find regulatory rules for mobile money to be clear and easy to follow which is reflected by the highest mean of 4.21 and a standard deviation of 1.02. The table also shows that there was also strong agreement that mandatory SIM card registration rules have been effective in reducing fraud (Mean = 4.10, SD = 1.18) and that strictly following Know-Your-Customer (KYC) protocols helps prevent fraud (Mean = 4.03, SD = 1.04).The respondents asserted that there is no discrepancy between official regulations and their practical application in daily work, as indicated by the lowest mean of 2.48 and a standard deviation of 1.

CHAPTER 5

DISCUSSION OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

. This chapter is presentation of the discussion, conclusions and recommendations and areas of further studies of the study

5.1 Discussion of findings

5.1.1 The Effect of Risk Identification Practices On Fraud Prevention

The research revealed that that risk identification directly boosts fraud prevention by facilitating the early detection of suspicious fraud activities before they happen. Consistent identification of upcoming risks helps in the prevention of fraud incidents as the respondents agreed. . This practical approach to fraud prevention allows agents to recognize the weak areas in their businesses and stop transactions that seem fraudulent. This conclusion is supported by Mackenzie et al. (2024), who documented a positive correlation between the frequency of risk assessments and a decrease in threat incidents in organisation

On the other hand, there was contradiction in the findings on the study. Data collected from the questionnaires indicated that agents acknowledged receiving formal training on fraud prevention but then the open-ended responses revealed that there is a significant deficiency in training for many individuals entering the mobile money business. A number of agents rely on acquiring knowledge primarily from their colleagues. This superficial training limits their capacity to recognize complicated fraud schemes that may emerge. The difference between their perceived training and actual formal instruction corresponds with Arim et al. (2022). They recognized that inadequate talent management as a significant risk making practical risk identification in digital financial services necessary.).

5.1.2 The Effect of Risk Analysis On Fraud Prevention

Risk analysis increases fraud prevention by enabling agents to understand patterns and anticipate future fraudulent activities. This is through the careful examination of past incidents of fraud. The findings of the study indicated consensus among mobile money agents that the analysis of

previous fraud events helps in forecasting and preventing future occurrences of fraud. Mobile money agents in Namagoma depend on customer awareness initiatives from service providers in order to prevent fraud.

The findings differ with technological standpoint that was proposed by Botchey et al. (2020).They advocated for the application of machine learning algorithms to examine fraud in real time. The mobile money agents in this study do not use any complicated digital tools to analyse risks. The findings validate the human based strategies highlighted by Guma Ali et al. (2020), who indicated that customer awareness initiatives and agent training are important elements of effective fraud prevention. Mobile money agents only identify weak spots by analysing patterns derived from past experiences to prevent fraud.

5.1.3 The Effect Of Risk Mitigation Strategies On Fraud Prevention

Risk mitigation enhances fraud prevention because it limits the opportunities for fraud to happen by establishing controls like transaction monitoring and cash reconciliation. The respondents agreed that security awareness training, continuous transaction monitoring, and daily reconciliation of cash and e-float are highly effective controls. The study also revealed a significant contradiction regarding the mitigation strategies. The mobile money agents admitted to bypassing security protocols to speed up service for trusted clients and yet security protocols are necessary. This risk really weakens the risk mitigation controls and also creates openings for other types of fraud.

5.1.4 The Effect Of Regulatory Compliance On Fraud Prevention

Regulatory compliance enhances fraud prevention through regulations like Know-Your-Customer (KYC) guidelines and SIM registration. These regulations obstruct anonymous fraud from happening. The results demonstrated that the mobile money agents see regulatory rules as clear and straightforward to adhere to as per the questionnaire. There was a general agreement in the study that compulsory SIM card registration and strict following of KYC protocols are effective in mitigating fraud risks. The research also indicated that regulatory compliance serves as the most effective foundation for fraud prevention in mobile money business.

This aligns with Ebong et al. (2021), who pointed out that regulatory frameworks offer the most sustainable approach to fraud prevention. The findings of the emphasized that delayed customer care responses from service providers make financial losses worse when fraud happens. This shows that despite the fact that national regulations are effective, the necessary support for practical enforcement of the regulations is most times not enough.

5.2 Conclusion

The study concludes that risk management practices directly influence fraud prevention in mobile money businesses. Risk identification allows mobile money agents to identify threats early. Risk analysis also helps them learn from past patterns of fraud occurrences while risk mitigation establishes daily boundaries in operations. The evidence backs a comprehensive risk management strategy where these four elements collaboratively facilitate the reduction of fraud. However , the effectiveness of these risk management practices is significantly undermined by human behaviour and structural business obstacles.

5.3 Recommendations

The following recommendations have been proposed; Mobile money service providers like MTN and airtel should enforce compulsory formal training for all new mobile money agents instead of depending on alternative learning methods.

The service providers should to evaluate the amount of commission give to mobile money agents. This would reduce the financial pressure that leads to internal fraud.

The time taken by customer service departments to respond fraud cases should be already shortened. This would enable mobile money agents to freeze accounts when they suspect fraudulent activities.

5.4 Areas of Further studies

i. A study should examine the influence of mobile money commission frameworks has on internal agent fraud.
ii. Additional research is also required to investigate what determines security protocols mobile money agents for trusted clients.

REFERENCES

Association of Certified Fraud Examiners (ACFE). (2020). 32nd Annual ACFE Global Fraud Conference. Retrieved from https://www.acfe.com/fraud-resources/fraud-prevention-and-deterrence?s=2024-novdec-im-a-cfe-erin-ellebracht

Datadome. (2025). AI fraud detection: What it is and how it works. Retrieved from https://datadome.co/learning-center/ai-fraud-detection/

Fraudio. (2023). The evolution of fraud detection systems. Retrieved from https://www.fraudio.com/blog/the-evolution-of-fraud-detection-systems

Fraud.com. (2021). The history and evolution of fraud. Retrieved from https://www.fraud.com/post/the-history-and-evolution-of-fraud

International Business Machines (IBM). (2024). What is fraud detection? Retrieved from https://www.ibm.com/think/topics/fraud-detection

Mappanyukki, R., Nengzih, N., & Endri, E. (2024). Fraud prevention: A study of skepticism moderating variable. Journal of Governance and... Retrieved from https://www.semanticscholar.org/paper/Fraud-prevention%3A-A-study-of-skepticism-moderating-Mappanyukki-Nengzih/8aa62b13f50576b1f347709cdd37ffcb948521bb

SAS. (2024). Fraud prevention: What it is & why it matters. Retrieved from https://www.sas.com/en_us/insights/fraud/fraud-prevention.html

Threatmark. (2025). 10 Key trends driving the fraud prevention industry in 2025. Retrieved from https://www.threatmark.com/10-trends-driving-fraud-prevention/

U.S. Postal Inspection Service (USPIS). (1872). The ages of fraud. Retrieved from https://www.uspis.gov/history-spotlight-2023/the-ages-of-fraud-part-1

U.S. Postal Inspection Service (USPIS). (1909). The ages of fraud. Retrieved from https://www.uspis.gov/history-spotlight-2023/the-ages-of-fraud-part-1

Kadens, E. (2024). The persistent limits of fraud prevention in historical perspective. Retrieved from https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1535&context=nulr

LexisNexis Risk Solutions. (2025). The impact of fraud. Retrieved from https://risk.lexisnexis.com/fraud-impact-files/index.html

Thales Group. (2025). A history of cybersecurity: Tracing the decades-old fight against malware, phishing, and fraud. Retrieved from https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/magazine/history-cybersecurity-tracing-decades-old-fight

KPMG. (2024). Great Britain criminalises the failure to prevent fraud. Retrieved from https://kpmg.com/de/en/home/insights/2024/01/uk-penalty-for-missing-fraud-prevention.html

Ken Research. (2024). Europe Fraud Detection and Prevention Market. Retrieved from https://www.marketresearch.com/Ken-Research-v3771/Europe-Fraud-Detection-Prevention-40710124/

Innovate Finance. (2025). UK lost $33.2bn to fraud and scams in 2024 - the most in the EU. Retrieved from https://www.compliancecorylated.com/news/uk-lost-33-2bn-to-frauds-and-scams-in-2024-the-highest-in-europe/

GBG. (2025). Emerging fraud trends in Southeast Asia (SEA) for 2025: how to stay ahead with advanced fraud prevention solutions. Retrieved from https://www.gbg.com/apac/blog/emerging-fraud-trends-in-southeast-asia-for-2025/

DBS Bank. (2025). Emerging fraud trends in Southeast Asia (SEA) for 2025: how to stay ahead with advanced fraud prevention solutions. Retrieved from https://www.gbg.com/apac/blog/emerging-fraud-trends-in-southeast-asia-for-2025/

Sumsub. (2023). New African fraud statistics: Cryptocurrency Fraud Spikes, Deepfake Fraud Emerges, and Forced Verification Alarms. Retrieved from https://sumsub.com/newsroom/new-african-fraud-statistics-cryptocurrency-fraud-spikes-deepfake-fraud-emerges-and-forced-verification-alarms/

Dojah. (2024). Top 8 Fraud Prevention and KYC Startups in Africa. Retrieved from https://dojah.io/blog/top-8-fraud-prevention-startups-in-africa

Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review. (2025). https://arxiv.org/html/2502.00201v1

Equity Bank. (2025). Combating Financial Fraud in Africa Through Digitization and Financial Inclusion. Retrieved from https://fitspa.ug/combating-financial-fraud-in-africa-through-digitization-and-financial-inclusion/

Edu, J., Hooper, M., Maple, C., & Crowcroft, J. (2023, June). Exploring the risks and challenges of the national electronic identity (NeID) system. In IET Conference Proceedings CP846 (Vol. 2023, No. 14, pp. 118-123). Stevenage, UK: The Institution of Engineering and Technology.

Edu, J., Hooper, M., Maple, C., & Crowcroft, J. (2023). Exploring the Risks and Challenges of the National Electronic Identity (NeID) System. ArXiv. https://arxiv.org/abs/2310.15813

Bank of Uganda. (2024). BoU Governor speaks out on mobile money fraud complaints. Nexus Media Uganda. https://nexusmedia.ug/bou-governor-speaks-out-on-mobile-money-fraud-complaints/

Deloitte. (2024). Challenges in fraud enforcement and mobile money fraud schemes. [Report]. Accessible summary: https://arxiv.org/pdf/2509.03545.pdf

Financial Sector Deepening Uganda. (2023). Mobile money fraud losses and regulatory audits. Uganda Bankers Association Report. https://ugandabankers.org/250521-UBAreport2024.pdf

KPMG. (2023). Integrated risk management and fraud detection in mobile money. [Industry summary].

Owino, J., & Namanya, M. (2025). The role of KYC in preventing identity-based fraud in mobile financial services.

PwC. (2025). Monitoring insider threats in mobile money: Risk management gaps. [Report].

Uganda Communications Commission. (2023). Regulatory Standards and Compliance for Mobile Money Operators. [Policy framework].

Uganda Legal Information Institute. (2023). Anti-Corruption Act of 2009. https://ulii.org/ug/legislation/act/2009/4

Alhassan, M. D., Gunu, U., & Ofori, D. (2023). Mobile money, financial inclusion, and digital payment ecosystem: A literature review. Journal of Money, Banking and Finance, 9(2), 41-58.

Al-Thani, D., Lari, M., & Zaki, N. (2022). A review of financial fraud detection methods. Journal of Information Assurance and Security, 17(1), 1-12.

Ameyaw, M. N., Korang, J., & Adu, S. (2024). Financial compliance as a cornerstone of corporate integrity and risk management. Journal of Financial Regulation and Compliance, 32(1), 1-17.

Button, M. (2022). Fraud prevention and control: A strategic approach. Routledge.

Kshetri, N. (2021). Evolving regulatory landscape of the global financial system. In The Palgrave Handbook of Technological Finance (pp. 1-25). Palgrave Macmillan.

Otiwu, K. C., Awa, H. O., & Ugwu, C. I. (2022). Understanding the adoption of mobile money services: An integrated model. Journal of Global Information Management, 30(7), 1-24.

Purdy, G. (2020). The evolution of risk management. In G. Purdy (Ed.), ISO 31000:2018—Risk management—A guide to implementation (pp. 51-65). John Wiley & Sons.

Tchankova, L. (2023). A modern approach to enterprise risk management. Risk Management and Insurance Review, 26(1), 115-135.

Arim, A., & Wamema, J. (2022). Towards an improved framework for e-risk management for digital financial services (DFS) in Ugandan banks. Journal of Information and Organizational Sciences, 46 (2), 123-145.

Arinze, E., Aleke, J. U., & Nnachi, A. B. (2024). Mobile money adoption in Uganda. Idosr Journal of Computer and Applied Sciences, 9 (2), 45-62.

Bongomin, G. O. C., & Ntayi, J. M. (2020). Mobile money adoption and usage and financial inclusion: Mediating effect of digital consumer protection. Journal of Economic Structures, 9 (1), 1-24.

Guma, A., Dida, M., & Sam, A. (2020). Evaluation of key security issues associated with mobile money systems in Uganda. Information, 11 (12), 592.

Kyomuhendo, M., Mutebi, J., Venkatachalam, M., & Sewanyina, M. (2025). Assessing mobile money security threats and user satisfaction in Bushenyi District, Uganda. Asian Journal of Advanced Research and Reports, 19 (1), 1-15.

Mackenzie, D., & Njunwamukama, S. (2024). Strengthening Fintech security in Uganda: An analysis of insider threats and effective risk management strategies. International Journal of Technology and Systems, 9 (2), 78-95.

Milly, N., Xun, S., Meena, M., & Cobbinah, B. B. (2021). Measuring mobile banking adoption in Uganda using the Technology Acceptance Model (TAM2) and perceived risk. Journal of Financial Innovation, 7 (1), 1-25.

Museba, T. J., Ranganai, E., & Gianfrate, G. (2021). Customer perception of adoption and use of digital financial services and mobile money services in Uganda. Journal of Enterprising Communities: People and Places in the Global Economy, 15 (2), 213-230.

Ali, G., Dida, M., & Sam, A. (2020). Evaluation of key security issues associated with mobile money systems in Uganda. Information, 11 (12), 592. https://doi.org/10.3390/info1112059

Arim, A., & Wamema, J. (2022). Towards an improved framework for e-risk management for digital financial services (DFS) in Ugandan banks. Journal of Information and Organizational Sciences, 46 (1), 109-147. https://doi.org/10.31341/jios.46.1.6

Arinze, E., Aleke, J. U., & Nnachi, A. B. (2024). Mobile money adoption in Uganda. Idosr Journal of Computer and Applied Sciences, 9 (1), 45-62.

Asongu, S., Biekpe, N., & Cassimon, D. (2020). Understanding the greater diffusion of mobile money innovations in Africa. Telecommunications Policy, 44 (8), 102005. https://doi.org/10.1016/j.telpol.2020.102005

Bongomin, G. O. C., & Ntayi, J. M. (2020). Mobile money adoption and usage and financial inclusion: Mediating effect of digital consumer protection. Cogent Business & Management, 7 (1), 1815815. https://doi.org/10.1080/23311975.2020.1815815

Botchey, F., Qin, Z., & Hughes-Lartey, K. (2020). Mobile money fraud prediction - A cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and naïve Bayes algorithms. Information, 11 (8), 383. https://doi.org/10.3390/info11080383

Ebong, J., & George, B. (2021). Financial inclusion through digital financial services (DFS): A study in Uganda. Journal of Risk and Financial Management, 14 (9), 393. https://doi.org/10.3390/jrfm14090393

Katusiime, L. (2021). Mobile money use: The impact of macroeconomic policy and regulation. Journal of Risk and Financial Management, 14 (7), 301. https://doi.org/10.3390/jrfm14070301

Koomson, I., Martey, E., & Etwire, P. M. (2022). Mobile money and entrepreneurship in East Africa: The mediating roles of digital savings and access to digital credit. Information Technology and People, 35 (4), 1304-1325. https://doi.org/10.1108/ITP-10-2020-0713

Lorenz, E. N., & Pommet, S. (2020). Mobile money, inclusive finance, and enterprise innovativeness: An analysis of East African nations. Research Policy, 49 (7), 104044. https://doi.org/10.1016/j.respol.2020.10404

Arim, A., & Wamema, J. (2022). Towards an improved framework for e-risk management for digital financial services (DFS) in Ugandan banks. Journal of Information and Organizational Sciences, 46(1), 1-28.

Bongomin, G. O. C., & Ntayi, J. M. (2020). Mobile money adoption and usage and financial inclusion: Mediating effect of digital consumer protection. Digital Business, 1(1), 1-15.

Botchey, F., Qin, Z., & Hughes-Lartey, K. (2020). Mobile money fraud prediction - A cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and naïve Bayes algorithms. Information, 11(8), 383.

Guma Ali, Dida, M., & Sam, A. (2020). Evaluation of key security issues associated with mobile money systems in Uganda. Information, 11(9), 432.

Lorenz, E. N., & Pommet, S. (2020). Mobile money, inclusive finance, and enterprise innovativeness: An analysis of East African nations. Journal of Development Studies, 56(4), 1-18.

Macdonald, I. (2023). The impact of anonymous ratings on consumer fears of fraud in Kenya and Uganda. Financial Technology Review, 3(2), 45-52.

Mackenzie, D., & Njunwamukama, S. (2024). Strengthening fintech security in Uganda: An analysis of insider threats and effective risk management strategies. International Journal of Technology and Systems, 12(3), 78-95.

Mihretu, A. M., Mdumuka, J., Shetto, M., Rice, O. P., Iradukunda, P., Chamisso, T. T., Mwangi, V., & Byiringiro, Y. (2023). Effective mitigation strategies for social engineering

attacks in mobile money services: A case study in Kenya. In 2023 IEEE AFRICON (pp. 1-6). IEEE.

Mugume, R., & Bulime, E. W. N. (2022). Post-COVID-19 recovery for African economies: Lessons for digital financial inclusion from Kenya and Uganda. African Development Review, 34(2), 234-248.

Sulieman, D. M., & Salleh, F. (2020). Anti-money laundering risk posed by mobile money services in Sub-Saharan Africa. International Journal of Financial Crime, 27(4), 512-528.

Arinze, E., Aleke, J. U., & Nnachi, A. B. (2024). Mobile money adoption in Uganda. Idosr Journal of Computer and Applied Sciences.

Bongomin, G. O. C., & Ntayi, J. M. (2020). Mobile money adoption and usage and financial inclusion: Mediating effect of digital consumer protection.

Ebong, J., & George, B. (2021). Financial inclusion through digital financial services (DFS): A study in Uganda. Journal of Risk and Financial Management.

Guma, A., Dida, M., & Sam, A. (2020). Evaluation of key security issues associated with mobile money systems in Uganda. Information., .11.(12).

Katusiime, L. (2021). Mobile money use: The impact of macroeconomic policy and regulation.

Nana Ameyaw, M., Idemudia, C., & Iyelolu, T. V. (2024). Financial compliance as a pillar of corporate integrity: A thorough analysis of fraud prevention. Finance & Accounting Research Journal.

Creswell, J. W., & Creswell, J. D. (2022). Research design: Qualitative, quantitative, and mixed methods approaches (6th ed.). Sage Publications.

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. Biometrics & Biostatistics International Journal, 5(6), 215-217.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607-610.

APPENDIX I: QUESTIONNAIRE

UGANDA CHRISTIAN UNIVERSITY

SCHOOL OF BUSINESS

A QUESTIONNAIRE FOR THE MOBILE MONEY AGENTS IN NAMAGOMA

Dear respondent,

I am currently conducting a study entitled "The Effect of Risk Management on Fraud Prevention in Mobile Money Businesses in Namagoma." I request you to spare some time and answer the following questions. Thank you for your time and co-operation.

SECTION A. BIO DATA

Instructions: -

a) Tick the boxes where applicable:

1. Gender

a) Male ☐ b) Female ☐

2. Age bracket (years)

a) 18-27 ☐ b) 28-37 ☐ c) 38-47 d) 48-57 ☐ e) 57+ ☐

3. Highest level of education attained

a) Primary ☐ b) Secondary ☐ c) University ☐ d) Other ☐

4. How long have you worked in a mobile money business.

a) Below 1 year ☐ b) 1-3 years ☐ c) 3-5 years ☐ d) Above 5years ☐

5. On average, how many mobile money transactions do you process per day?

(a) 0 – 50 ☐ (b) 51 – 100 ☐ (c) 101 – 200 ☐ (d) 200+ ☐ (e) Not sure ☐

SECTION B. The Effect Of Risk Identification Practices On Fraud Prevention

Using the scale: 1=Strongly Disagree, 2=Disagree, 3=Not Sure, 4=Agree, 5=Strongly Agree

	Statement	1	2	3	4	5
1	We received formal training on fraud prevention from our mobile money provider.					
2	We are well-trained to identify common fraud risks like SIM swaps and phishing.					
3	We have clear procedures for identifying suspicious customer behaviour or transactions.					
4	Our systems effectively flag technological weaknesses (e.g., authentication failures).					
5	We have control measures that easily identify potential internal fraud or collusion.					
6	Regularly identifying new risks has directly helped us prevent fraud incidents.					
7	We struggle to stay updated on new fraud tricks used by criminals in this area.					
8	Our manual identification processes (e.g., checking IDs) make it hard to spot fakes.					
9	We rarely receive timely alerts about new fraud types from our service providers.					
10	We usually only identify risks after a fraud incident has already occurred.					

SECTION C. The Effect Of Risk Analysis On Fraud Prevention

Using the scale: 1=Strongly Disagree, 2=Disagree, 3=Not Sure, 4=Agree, 5=Strongly Agree

	Statement	1	2	3	4	5
1	We effectively analyse the likelihood and impact of the fraud risks we identify.					
2	Our business uses real-time transaction monitoring to analyse unusual patterns.					
3	Customer awareness campaigns help us analyse and respond to new fraud trends.					
4	The training we receive helps us analyse situations to determine if they are fraud.					
5	Our analysis of past fraud incidents helps us predict and prevent future ones.					
6	We classify risks according to their severity when identified.					
7	We lack sufficient historical records to accurately estimate future fraud risks.					
8	The complexity of digital systems makes it hard to understand how fraud happens.					
9	Pressure to serve customers quickly prevents us from analysing suspicious deals.					
10	We do not have the right tools to deeply analyse transaction patterns.					

SECTION D. The Effect Of Risk Mitigation Strategies On Fraud Prevention

Using the scale: 1=Strongly Disagree, 2=Disagree, 3=Not Sure, 4=Agree, 5=Strongly Agree

	Statement	1	2	3	4	5
1	Transaction limits (e.g., daily limits) are effective for reducing fraud losses.					
2	Security awareness training for agents is one of the best ways to mitigate fraud.					
3	ID Verification for large transactions effectively reduces fraud.					
4	We have a clear incident response plan for what to do immediately after fraud.					
5	Continuous monitoring of transactions effectively identifies and stops fraud.					
6	We reconcile cash and e-float daily to detect discrepancies.					
7	We sometimes bypass security protocols to speed up service for trusted clients.					
8	Strict fraud prevention measures often result in losing impatient customers.					
9	The lack of biometric tools (e.g., fingerprint scanners) makes mitigation difficult.					
10	Employees frequently forget to strictly follow established security limits.					

SECTION E. The Effect Of Regulatory Compliance On Fraud Prevention

Using the scale: 1=Strongly Disagree, 2=Disagree, 3=Not Sure, 4=Agree, 5=Strongly Agree

	Statement	1	2	3	4	5
1	Strictly following Know-Your-Customer (KYC) protocols helps prevent fraud.					
2	Mandatory SIM card registration rules have been effective in reducing fraud.					
3	Adhering to Bank of Uganda guidelines is essential for our fraud prevention.					
4	Internal compliance audits by the provider help us fix control weaknesses.					
5	We find the regulatory rules for mobile money to be clear and easy to follow.					
6	Regulatory requirements are often too complex for us to implement fully.					
7	Compliance costs (e.g., licenses) reduce our ability to invest in security tools.					
8	Regulatory enforcement in Namagoma is inconsistent and weak.					
9	The process for reporting suspicious activities to regulators is difficult.					
10	There is a gap between official regulations and what is practical in our daily work.					

SECTION F: Open Ended Question

Mention one challenge that affects your ability to prevent fraud in your business.

……

Mention one possible solution to this challenge.

……

Hazel Kalindwa

THE EFFECT OF RISK MANAGEMENT PRACTICES ON FRAUD PREVENTION IN MOBILE MONEY BUSINESSES IN NAMAGOMA

Quick Submit

Quick Submit

Uganda Christian University

Document Details

Submission ID
trn:oid:::1:3534344843

Submission Date
Apr 12, 2026, 12:41 PM GMT+3

Download Date
Apr 12, 2026, 12:48 PM GMT+3

File Name
Kalindwa_Hazel_REDSRTN.docx

File Size
4.6 MB

41 Pages

11,151 Words

67,103 Characters

turnitin Page 1 of 52 - Cover Page Submission ID trn:oid:::1:3534344843

25% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Exclusions

▸ 17 Excluded Matches

Match Groups

178 Not Cited or Quoted 24%
Matches with neither in-text citation nor quotation marks

14 Missing Quotations 1%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

1 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

23% Internet sources
15% Publications
17% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Hazel Kalindwa

THE EFFECT OF RISK MANAGEMENT PRACTICES ON FRAUD PREVENTION IN MOBILE MONEY BUSINESSES IN NAMAGOMA

Quick Submit

Quick Submit

Uganda Christian University

Document Details

Submission ID
trn:oid:::1:3534896627

Submission Date
Apr 13, 2026, 12:43 AM GMT+3

Download Date
Apr 13, 2026, 9:50 PM GMT+3

File Name
Kalindwa_Hazel_RED5RTN_2.docx

File Size
4.6 MB

40 Pages

10,879 Words

64,807 Characters

turnitin Page 1 of 42 - Cover Page Submission ID trn:oid:::1:3534896627

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (i.e., our AI models may produce either false positive results or false negative results), so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.