# CUSTOMER AWARENESS AND RESPONSE TO DIGITAL BANKING FRAUD IN UGANDA'S FINANCIAL SECTOR

**ALISON DESIRE NAIKOBA**

**CKS21B11/134**

**A DISSERTATION SUBMITTED TO THE SCHOOL OF LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF UGANDA CHRISTIAN UNIVERSITY**

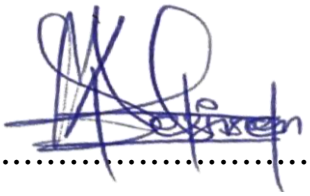
**May,2025**

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

## DECLARATION

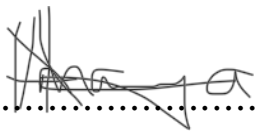
**I, NAIKOBA ALISON DESIRE,** declare that this dissertation has been carried out by the university regulations and has not been submitted for any other academic award. Works cited or referred to have been acknowledged.

Signature  .....

Date.....22nd May 2025.....

**APPROVAL**

This dissertation by Naikoba Alison Desire, titled "***Customer awareness and response to digital banking fraud in Uganda's financial sector***," was supervised by me and is approved for submission to the examining authority.

Signature:  .....

Date: .....22nd May 2025.....

Norah Amanya,

Supervisor/Lecturer of Laws.

School of Law- Uganda Christian University.

## DEDICATION

This academic paper is specially dedicated to my father Mr. Martin Oscar Kintu and mother Mrs. Namuyaga Jennipher Rose for the confidence they have instilled in me to complete this work, to my brothers and sisters Arnold, Alvin, Aldrine, Emma, Keith, Kelvin, Elvis, Sharon and Lorna for their support, inspiration and prayers to enable me finish this work successfully.

Last but not least, to my good friend Vivian Wanyana and my other friends Nakamya Maria Josephine, Nakayiza Sarwa Kubira, et al for their love, support, and encouragement.

**ACKNOWLEDGEMENT**

First and foremost am grateful to my supervisor, Ms Norah Amanya, whose tireless guidance and involvement in my research have greatly improved my skills as a researcher, and for also ensuring that my dissertation is excellent.

I am grateful to my parents, brothers, sisters, and friends for the commitment that they have taken in ensuring that I successfully finish my research.

**“MAY YOU ALL EXPERIENCE THE LORD’S BLESSINGS”**

**ABSTRACT**

In the last few decades, financial institutions have made huge investments in technology to reduce their cost and improve customers' experience. This is because technology was growing, affecting various economic sectors the banking industry. Digital banking then manifested itself because the internet and mobile devices were widely adopted. This system came with an intolerable evil, "fraud." Security and customer trust are, however, necessary to maintain the bank customer relationship. This study, therefore, goes on to discuss the level of customer awareness and response to digital banking fraud in Uganda's financial sector, looking at the different types of digital banking fraud. This inspection was done through different case studies as a diagnostic technique involving theoretical analysis of cases adjudged by courts in Uganda, existing literature, and legislation. This study observes that the financial institutions have tried to promote customer awareness but face some challenges in promoting the same. The study, therefore, suggests measures that financial institutions can implement to enhance customer awareness and prevent digital banking fraud.

**TABLE OF CONTENTS**

# CHAPTER ONE

## 1.0 GENERAL INTRODUCTION

## 1.1 OVERVIEW OF THE LEGAL PROBLEM

Uganda's financial sector involves the businesses and institutions that manage money and provide intermediary services to transfer and allocate financial capital in an economy.[1] Digital banking came up because the internet and mobile devices were adopted worldwide; however, the COVID-19 pandemic triggered the growth of digital banking across the globe. Digital banking increases access to a broad spectrum of financial services among the unbanked population. However, growth in the use of digital banking has created new gaps for fraud, which causes financial loss to customers and financial institutions.

The Bank of Uganda takes the upper hand in maintaining a safe and sound financial sector and has strengthened the regulatory framework, ensuring consumer protection from fraud, for example, authorised push payment fraud, card trapping, and account takeover under Ugandan law. The regulatory framework promotes transparency, fairness, accountability, and facilitates proper regulation. Bank of Uganda in June, 2011, issued the ***Financial Consumer Protection Guidelines***[2]. To all supervised financial institutions to promote fair and equitable financial services practices by setting minimum standards for financial services providers in dealing with consumers, increase transparency, foster confidence in the financial services sector and to provide efficient and effective mechanisms for handling consumer complaints relating to the provision of financial products and services under

[1]https://taslafadvocates.com/users-guide-a-legal-guide-to-ugandas-financial-sector/#:~:text=Introduction,financial%20capital%20in%20an%20economy.
[2] Bank of Uganda Financial Consumer Protection Guidelines, 2011

guideline 4.

In 2022, the ***National Payments Systems Regulations*** were updated to include Consumer Protection Regulations for institutions licensed under the National Payment Systems Act, Cap 59.

The legal framework has been strengthened by enacting new laws for example, the ***Micro Finance Deposit-Taking Institutions Act, Cap 58, and the Financial Institutions Act, Cap 57.*** Awareness of the existence of these laws among these financial institutions is limited, and may not be able to implement their requirements for consumer protection.

"Digital banking refers to the transformation of traditional banking services into digital formats, allowing customers to manage their financial accounts, conduct transactions, and access various banking services through digital channels."[3] Digital banking was initiated as an advanced, feasible and fruitful method of monetary operations, and banks are offering digital banking channels such as mobile wallets, online banking, internet banking, and electronic banking to deliver efficient services to customers. Digital banking links banks to entrepreneurs, suppliers, employees, and new markets, allowing for social distancing and helping foster financial inclusion in remote or impoverished places where financial institutions are not physically present.[4]

Despite the streamlined performance of digital banking, there is a probability of fraud to this system. Fraudsters target financial institutions in particular, because

[3] Alex Malyshev, Banking Software, March 12, 2025

[4] Elisa Indriasarri, Harjanto Prabowo, Ford Lumban Gaol, Betty Purwandari, Digital Banking; Challenges, Emerging Technology Trends, and Future Research Agenda

they are instantaneously accessible. “Fraud is defined as a deceitful practice or wilful device resorted to with intent to deprive another of his right or in some manner to do him an injury.”[5] Every individual is susceptible to fraud, including educated people, banking sites, and apps themselves have unpatched vulnerabilities hacked by expert fraudsters.

There are different kinds or types of digital banking fraud, among which include;

- Vishing, also known as a phone call scam
- Phishing, also known as an email scam
- Spear Phishing, i.e., targeted email scam
- Skimming, which is an ATM Scam
- SIM Swap, i.e., mobile number scam
- Smishing, i.e., SMS Scam
- Website spoofing, i.e. fake website scam
- Malware attack, i.e., Gadget Virus attack.[6] [6]

One of the solutions to digital banking fraud is creating customer awareness in regards to fraud, as it helps to protect an individual’s confidential information. The “Bank of Uganda,” which is the “Central bank,” has the legal responsibility of regulating banking business and promoting customer awareness. It is given this mandate under Article 162 of the ***Constitution of the Republic of Uganda, 1995,*** as amended. Other institutions responsible for promoting awareness include the Financial Intelligence Authority, the Uganda Bankers Association, the National Information Technology Authority-Uganda, and the Financial Sector Deepening

[5] Black’s law dictionary, 12th edition.

[6] https://www.aubank.in/blogs/8-different-types-of-digital-banking-frauds.

Uganda. Customer awareness encompasses educating consumers about different types of fraud and how it happens to help them recognise and protect themselves from being victims of the same. This is done through public service announcements, for example, through running radio and print adverts, through digital channels like social media posts, and carrying out campaigns to educate customers about agency banking, mobile wallets, and risk mitigation.

The institutional frameworks face challenges in promoting customer awareness for example geographical barriers that limit their movement form one place to another, some of the customers are illiterate which makes it hard to pass on information and limited resources to use in the carrying out of their work.

## 1.2 RESEARCH QUESTIONS

i) What is the impact of the increase in digital banking fraud on consumer trust in Uganda's financial sector?
ii) What role does the role customer education play in mitigating the risk associated with different types of digital banking fraud?
iii) What is the adequacy of the legal framework to digital banking fraud in Uganda's financial sector?
iv) What measures can financial institutions implement to enhance customer awareness and prevent digital banking fraud in Uganda's Financial sector?

## 1.3 RESEARCH OBJECTIVES

General objective

To examine the measures financial institutions can implement to enhance customer awareness and prevent digital banking fraud in Uganda's financial sector.

Specific objectives

i) To examine the adequacy of the legal framework for digital banking fraud in Uganda's financial sector
ii) To assess the impact of the increase in digital banking fraud on customer trust in Uganda's financial sector.
iii) To determine the role customer education plays in mitigating the risk associated with different types of digital banking fraud.

## 1.4 SIGNIFICANCE OF THE STUDY

This research will facilitate the fractional completion of the requirement of the degree in Bachelor of Laws. The study will also increase prior research as far as the awareness and response to digital banking fraud is concerned. This research will also contribute to legal scholarship by examining whether the legal framework effectively addresses digital banking fraud and customer protection obligations. The results of the study will show the loopholes in digital banking that lead to fraud and hence prompt the concerned stakeholders to bridge the loopholes in the system. The study shall also improve the researcher's capacity to upgrade skills in the field of research.

## 1.5 LITERATURE REVIEW

This section focuses on the analysis of the already available literature on customer awareness and response to digital banking fraud in Uganda's Financial Sector. In recent years, digitalisation has revolutionised the banking sector and made it easy for banks to offer banking services. While digital banking is convenient to both banks and consumers, it has some specific challenges, among which include fraud. It should therefore be noted that extensive research has been performed on digital banking,

particularly on types of digital banking fraud that customers face, the effect of digital banking fraud on customer trust in the financial sector, and the role played by customer awareness in mitigating digital banking fraud. This section will therefore provide an overview of customer awareness and digital banking fraud.

Risk and security were looked at as one of the challenges faced in digital banking.[7] The privacy of customers can be invaded by fraudsters. "Fraud has evolved from being perpetrated by casual fraudsters to being committed by well-thought-out crime and fraud rings that use classy ways to take control of accounts and commit fraud."[8] There is an increase in digital banking fraud, which affects the customer relationship in that banks suffer weighty expenses by paying back monetary losses to customers, and bank customers suffer weighty expenses by paying back monetary losses to customers.

In the circumstances, it should be noted that virtual banking leans on the quality of digital applications used therein, given the huge potential financial loss caused by vulnerabilities. Banking, as a sector, requires secure, strong, and dependable systems to ensure smooth functioning and public trust. The banks, however, are challenged by security threats that the apps are exposed to because they are convenient and easy to use to get money from. The security risks involve the third-party risks that are perpetrated by fraudsters.[9]

Chang's (2008) interpretive findings suggest that scammers such as advance fee

---

[7] Elisa indrisarri, Harjanto Prabowo, Ford Lumban Gaol, Betty Purwandari, Digital Banking; Challenges, Emerging Technology Trends and future Research Agenda.

[8] Abend, V., Peretti, B., Bach, A., Barry, K &Donahue, D. (2008). Cyber Security for the Banking and Finance Sector, Homeland Security, PP.1-17.

[9] Shubham Khandal, Customer awarenesson UPI and mobile banking: An exploratory Study.

automatic behaviour of victims. According to Chiemeke, Evwiekpaefe & Chete (2006), most of the banks execute extremely well in providing up-to-date information, and consequently, they noted further improvements on security and provisions of key ingredients of internet banking. Chang's findings show that different methods are used to commit fraud, and Chiemeke's show that the banks provide customers with information; however, what banks provide is information on things like privacy of credentials, data concerning their customer ID, choosing of appropriate passwords, and how to maintain their security. The study therefore suggested a need to inform digital banking users of the methods employed by fraudsters or the types of digital banking fraud, because it would help them recognize and avoid digital banking fraud.

In a study by Shewangu Dzomira, his findings confirm the survey carried out in banking by Deloitte's (2015) in India that there is a lack of customer awareness in respect of internet fraud, a category under digital banking fraud.[10] "Narayanan, Koo, Brian & Cozzarin (2012) concluded from a study that product characteristics and the education level of the head of the household critically affect consumer decision making on internet transactions."[11] Whereas the first study acknowledges the fact that there is a lack of customer awareness, the second suggests that one's education level can determine the extent to which they may be defrauded despite customer awareness. That is not to say that those who are highly educated cannot be defrauded, but it happens to a lesser extent. All in all, there is a need for financial

[10] Shewangu Dzomira, Banks and Bank systems, December 2016, Financial consumer protection: Internet banking fraud awareness by the banking sector.

[11] Narayanan, M., Koo, B. &Cozzarin, B.p (2012). Fear of Fraud and Internet Purchasing, Applied Economics Letters, Volume 19, pp. 1615-1619.

institutions to promote customer awareness without relying on the customer's level of education. As clients grow chicer, banks need to consider the use of technology and information campaigns to react to their constantly changing requirements.

Information is only displayed when individuals decide to use the various digital banking for example, when they log onto an app. However, the proven strength of this information is quite unknown. The knowledge of digital banking fraud being low suggests for engagement in digital banking transactions by customers without adequate knowledge of possibilities. There is, therefore, a good chance of being a digital scam victim.

In the banking system, fraud includes undertakings that rely on deception to achieve their outcome and are carried out virtually. Digital fraud is grouped into "unauthorised retail payment transactions, manipulating bank customers to issue retail payments, fraud related to other banking products, and fraud through customers' data or banks' systems."[12]

"The landscape for cybercrime shows a general increase in the reported cases to the Uganda Police Force for example between 2017 and 2019, the reported cyber cases to police steadily grew by 25.2 percent from 158 to 248.[13] This growth in cybercrime was driven by electronic fraud, internet banking, and mobile money payments due to weak internal controls, limited training on cybersecurity in banks and telecommunication companies."[14]

---

[12] Digital fraud and banking: Supervisory and Financial Stability Implications, November, 2023, page 7

[13] Uganda Bankers Association, Bend But do not break, How the Financial Sector can thrive in the Era of the 4th Industrial Revolution, Annual Bankers' Conference 2021, page 03

[14] Ibid.

Various bills, acts, and policies have been enacted and institutions established by the government of Uganda to fight cybercrime in the financial sector. The government has enacted the following laws: the Computer Misuse Act, the Electronic Signatures Act, the Access to Information Act, and the Regulation of Interception of Communications Act. However, the Enforcement of these laws is feeble, implementation is not effective due to limited budget and capacity. "Moreover, there is limited awareness of these existing laws among the stakeholders in the financial sector and the general public."[15]

There are extensive domestic, regional, and international ambitions for managing digital banking fraud. "These include initiatives related to raising public awareness and customer empowerment, statements regarding control measures and security protocols, supervising banks' digital fraud risk management practices, collaboration with multiple authorities to detect, respond to, and disrupt fraud activities, and cross-border cooperation."[16]

In conclusion, despite government progress in creating a facilitative environment for digital services, being diligent is required to increase public awareness of cybercrime. Creating awareness among customers equips them with the requisite knowledge to avoid the risk of fraud and handle customer scams when they occur. A case in point is the Safaricom M-PESA in Kenya, which has invested significantly in customer awareness campaigns. The company found that customer awareness through clear communication messages is the most effective preventive tool for fighting customer scams. The company uses SMS texts, radio announcements in local

[15] Uganda Bankers Association, Bend But do not break, How the Financial Sector can thrive in the Era of the 4th Industrial Revolution, Annual Bankers' Conference 2021, page 05.
[16] Digital fraud and banking: Supervisory and Financial Stability Implications, November, 2023, page 15.

dialects, local skits, and newspaper adverts to empower customers to identify cyber threats, prevent cyber attacks, and seek correct redress to mitigate cyber threats.[17]

## 1.6 METHODOLOGY

The study will be mainly qualitative although quantitative data shall be obtained from secondary sources. Documentary review method, which looks at articles already published, law journals, views by the public expressed through media internet resources, textbook, law reports and direct observation methods will be used.

### 1.6.1 Population and sampling techniques

The survey data tools and instruments will include interview guides and survey guides.

The data collection process will include conducting personal interviews with people from the customer service and marketing/communications department of financial institutions.

The study will also include conducting key informant interviews that will involve the researcher carrying out semi-structured interviews with people from the customer service and marketing/communications departments of financial institutions across the country. The interviews are to be recorded or transcribed where possible, and this method shall provide information from personal experiences of different individuals, therefore providing accurate information.

The research study shall also rely on case review which shall allow a discussion on

[17] Uganda Bankers Association, Bend But do not break, How the Financial Sector can thrive in the Era of the 4th Industrial Revolution, Annual Bankers' Conference 2021, page 07.

some of the cases from Uganda's banking sector.

### 1.6.2 Data analysis and presentation

The data generated from the interview guides will be edited to discover and rectify any possible errors and omissions that may occur to be able to ensure correlation across the audience from the interviews. The recordings will also be presented as a narration and edited to reflect the objective responses from the audience.

### 1.6.3 Ethical considerations

The research is to be conducted with utmost care, and the consent of the audience is to be sought before an interview is conducted. Confidentiality and anonymity of the interviewed individuals of the mass population will be paramount in conducting these interviews, as it will provide a comfortable and safe environment for them to provide the desired information. Integrity and absolute work ethics will be the guiding rules for conducting these interviews.

## CHAPTER TWO

# 2.0 IMPACT OF NON-LEGAL ASPECTS OF DIGITAL BANKING ON THE FINANCIAL INSTITUTION SECTOR.

## 2.1 Introduction

This segment looks at non-legal aspects concerning digital banking diving into how digital banking developed in Uganda, the challenges experienced by customers while using digital banking for example security vulnerabilities, and how the banks themselves have tried to promote safety for customers while using the digital banking system.

This chapter in general looks at the non legal aspects including customer concerns but the legal aspects of digital banking. To understand this chapter, we shall look at the history of the legal framework governing e-banking in Uganda.

## 2.2 History of digital banking in Uganda.

The pre-independence commercial banking sector was dominated by five foreign-owned banks before independence, and they were usually very conservative in their lending policies, wherein loans were given strictly on a commercial basis, and because they were foreign-owned, they were shielded from political interference in their lending policies. These foreign-owned banks discriminated against Africans because most of them were unable to meet the criteria required of them to access the commercial loans, for example, securities such as land titles, and most of them engaged in agriculture and animal husbandry, which were non-commercial ventures.

The ***Uganda Credit and Savings Bank Act***[18] ***w***hich created the Uganda Credit and Savings Bank was enacted by the colonial government in the early 1950s to deal with the foreign bank discrimination. This bank was established to provide loans to Africans to invest in agriculture and to increase access to credit by African business and farmers.[19]

After independence, there was dissatisfaction with foreign-controlled banks in (1962-1993). They faced criticism for lending on short term for the financing of trade carried out externally and the giving of startup funds to start ventures from companies owned abroad. "The independent government regarded this as irrational and unjust and as a constraint on its development objectives."[20]

In the 1960s and 1970s, reforms started taking place in the banking sector to fill the gaps in financing and influence the direct allocation of credit through administrative controls.[21]The Uganda Credit and Savings Bank was transformed into Uganda Commercial Bank in 1965, the now Stanbic Bank. Bank of Uganda was then created in 1966, and in 1972, the Cooperative Bank to fulfil development objectives based on government development plans. In the early 1970s, 49% of the shares of banks owned by foreigners were acquired by the government, but not those in Standard Chartered Bank. Most of the foreign banks closed their branches in other parts of the country, but in Kampala.

---

[18] Cap 90, 1964, Revised Laws of Uganda.

[19] G.P. Tumwine-Mukubwa, Essays in African Banking Law and Practice (2nd edition, 1998) page 1.

[20] G.P. Tumwine- Mukubwa, Essays in African Banking Law and Practice (2nd edition, 1998) page 2.

[21] Brownbrige M. and Harvey C. Banking in Africa, 1998.

The Uganda Commercial Bank and Cooperatives Bank then expanded, filling the void left by the foreign banks. This expansion was, however, done with an inadequate legal framework among which included the Banking Act.[22] Enacted in 1955 made it mandatory for banks to have a paid-up capital of one million shillings. The Banking Act repealed that act.[23] as amended by the Banking (Amendment) Act[24]. This act was efficient in that the banking business was limited to companies incorporated in Uganda but inadequate because of the powers possessed by the minister in the Central Bank giving command in regards to financial and economic policy, and the bank had to comply.

Financial technology, which dates back as far as the 1850s, with Bank of America being among the first institutions to develop the idea of digital banking to take over the labour-intensive techniques of banking, was introduced into the commercial banking sector in Uganda in 1997 when the Bankom, an automated teller machine, was brought. Bank of Uganda in the year 2009 then issued a no-objection letter to MTN-Uganda Ltd, which launched its operations and went on to register eleven thousand sixteen "(11,016) accounts in the first month and leading to the establishment of the ***National Information Technology Authority, Uganda Act."***[25] (NITA-U Act) and the commencement of a second mobile money provider in Uganda (Zain-Airtel).

Bank of Uganda, in 2011, also went on to issue more no-objection letters to mobile

---

[22] Cap 88, Revised Laws of Uganda, 1964.
[23] No. 16 of 1969.
[24] Act No.34 of 1969.
[25] No. 4 of 2009.

money service providers, allowing individuals to pay their bills through mobile money, launching the first bill payments with the National Water and Sewerage Corporation. Warid Telecom Ltds and "M cash" then joined the mobile money market in 2012, and in 2013, the Bank of Uganda issued the ***Mobile Money guidelines***. Ezee money also joined the market, mobile money cash out service (MTN Interswitch), Online E-commerce retailing (Jumia), and community-based mobile transportation (Safeboda), mobile wallet service by Centenary Bank and Airtel Uganda were then launched in Uganda over the years.

Micropay, which provides e-payment services for small businesses in Uganda, also joined the market. MTN started a partnership with Commercial Bank of Africa and offered the Savings and Loan Product (MoKash), which allows MTN Mobile Money Customers to deposit funds into a MoKash Savings account and take out loans using their mobile phones. Mobile money interoperability was launched by MTN-Uganda and Airtel-Uganda, where users of either mobile money service could be able to transfer or make payments to either mobile money provider.

In 2016, the Financial Institutions Act of 2004 was then amended to facilitate development of Islamic Banking, and included provisions for Islamic financial business allowing contracts that comply with principles of Shari'ah, Agent Banking and the amendments therein facilitated the establishment of agent banking which allowed financial institutions to authority agents to extend their services to underserved areas, Bancassurance, where a bank and an insurance company partner and the bank acts as a distributor of insurance products to its customers. The amendment removed the restrictions and allowed banks to sell insurance services to

their customers.

The Financial Technology Service Providers Association was then embodied as a unifying voice for international and local FinTechs and Fintech stakeholders in Uganda, with a vision of acting as a catalyst in developing Uganda's Digital Financial Services. Agency and digital banking were put to sea in Uganda in 2018, and in 2019, the ***National Information Technology Authority, Uganda Act*** (NITA-U Act)[26] Issued the Data Protection and Privacy Act.

The National Payment Systems Act[27] It was formally approved and enacted in Uganda in May 2020, ensuring the efficacy and safety of systems for payments, both traditional and electronic payment methods. MFS Africa Limited a financial technology company that provides mobile financial solutions across Africa acquired Beyonic, a digital payments services provider, for enterprises that were operating in Ghana, Uganda, Tanzania and Kenya in 2020 to bring cross border payments to African Small and Medium Enterprises (SMEs) and in 2021, the fist Fin tech license was issued to Pegasus Technologies by Bank of Uganda. Licenses were also issued to Airtel and MTN Uganda Limited. The Global stocks investing product (Chipper) was also launched.

Over the years, the growth of digital banking in Uganda's Financial sector has modified the operation of banks, customer interactions, and how financial services are delivered. There has been an improvement in efficiency, profitability, and

[26] No. 4 of 2009.
[27] 2020.

services enjoyed by customers. Traditional banking, characterised by conventional branches and processes that are hand-operated, is increasingly giving way to an automated and agile innovation because customers anticipate instant and mobile-friendly banking. Banks, therefore, go on to embrace digital transformation.

The embracing of these digital technologies, in Uganda's financial sector, has gaps that perpetrate digital banking fraud. Fraudsters target financial institutionsbecause their funds are easily accessible. When customers encounter fraud, they withdraw their deposits from the financial institutions.

### 2.3 Challenges faced by customers while using digital banking.

Digital banking, which is a technological evolution, started when the world recovered from the Napoleonic wars.[28] Banking activities such as checking the balance on the account, withdrawing money, transferring, depositing money, and applying for loans are done online, that is to say, they are digitized. Digital banking gives customers the luxury of doing banking activities without going to the bank or leaving the comfort of their homes, as it is intended to be convenient in that it is available 24 hours a day. Digital banking also gives individuals more efficient tariffs as the fees and rates charged to customers are reduced due to the integration of other platforms with the digital banking services. Digital banking also prioritises security and provides multi-factor authentication that guarantees account security, for example, biometric authentication and one-time password (OTP).

Despite the convenience, customers face a challenge of security vulnerabilities,

[28] Peter Ellinger, [2013] Banking law and practice I their conceptual and historical perspectives, page 44.

where the peril of fraud exposes customers and banks to swindlers. Cybersecurity in digital banking has challenges, for example, identifying customers online, storing customer data safely, to protecting their payments.[29]

Some customers are also financially illiterate, which makes them more vulnerable to fraud and phishing scams, as they are unable to appreciate the importance of keeping their particulars confidential (privacy issues). Customers are also susceptible to unauthorised access, especially in circumstances where they seek help from dishonest individuals to be able to use digital banking. This means that financially illiterate customers appear to report security vulnerabilities more often compared to those who are literate, but it is hard for financial institutions to protect them from swindlers because they may fail to comprehend the repercussions, and hence, suffer a loss.

Some senior citizens in the country are illiterate, and some aren't, but financial institutions take a typical approach to their e-products.[30] They are all handled equitably. It is inaccurate to presume that the elders aren't tech-savvy and will not apply digital products. Although many are rigid and prefer going to the bank to carry out whatever transaction they need to, they have special financial needs, and if not addressed, could cost them their finances.

In the case of ***Aida Atiku v Centenary Rural Development Bank***[31] Aida, the plaintiff who alleged that she was suffering from cataracts, which resulted in severely

[29] Five Key digital banking challenges that financial institutions need to address, Lumin Digital.
[30] Ranjan Akash, Digital Banking Issues faced by the elderly and the optimal measures to resolve them, (2024) Volume 8, IJSREM, Page 2.
[31] Civil suit no.0754 of 2020.

impaired vision, took reasonable precautions in having her daughter make out the savings account opening form. She then suffered an account takeover fraud, and the court concluded that she undertook the transactions either because she authorised them or was negligent. This fraud therefore took place because her information was shared, and gave a fraudster access to her savings. After all, evidence on record showed that all transactions were authorised from her phone.

The above case also showed that Aida was a senior citizen and tech-savvy and needed assistance to be able to use the banking services, and in particular, the digital banking services. The help she got landed her into unforeseen consequences of being defrauded.

### 2.4 Duties of the bank in promoting security in the digital banking system.

The COVID-19 pandemic was an extraordinary stimulant for the adoption of e-banking in the world. Consumer efforts to visit the offices of banks to carry out ordinary transactions were frustrated, and instead inspired to use digital banking during this period.[32] Temporary shutting down of offices was done, minimising physical interactions. Retail bank consumers in Uganda were therefore compelled to embrace these self-service channels as they had never heard of them. Mobile banking was at hand, aiding customers to scrutinise account 15 status, cover expenses, assign money, and cash out from ATMs. Customers were also able to get hold of their bank anytime by using email, mobile, or internet channels and receive, without delay, instantaneous decisions. E- payments led to a speedy process, and

[32] Ranjan Akash, Digital Banking Issues faced by the elderly and the optimal measures to resolve them, (2024) Volume 8, IJSREM, Page 2.

customers were given the latitude and independence to access their bank information and carry out their financial activities online.

"Financial institution vendors are usually troubled by cybersecurity, and numerous continue to transmit to their customers communications at regular intervals, warning them of fraudsters and the precautions that they need to take."[33] Customers tend to develop a phobia and hence distrust of digital media. This means that the challenges have to be addressed so that confidence is instilled in the customers for them to be able to use the various digital banking services. Financial Institutions promote customer awareness through using SMS texts, radio announcements in local dialects, local skits, and newspaper adverts to empower customers to identify cyber threats, prevent cyber-attacks, and seek correct redress to mitigate cyber threats.[34]

With the growth of digital banking, banks must put in place strong fraud prevention and precaution measures to promote the security of customer transactions, assets, systems, and to store their data safely due to the risk of fraud. As digital channels multiply, so do the routes used by fraudsters. Fraudsters mostly target financial institutions due to their immediate outflow of funds. Online businesses that require users to enter login or registration credentials have to protect their accounts.

---

[33] Ranjan Akash, Digital Banking Issues faced by the elderly and the optimal measures to resolve them, (2024) Volume 8, IJSREM, Page 2.

[34] Uganda Bankers Association, Bend But do not break, How the Financial Sector can thrive in the Era of the 4th Industrial Revolution, Annual Bankers' Conference 2021, page 07.

Financial institutions offering digital services are should therefore provide safe mechanisms for customers to conduct their online banking, to ensure security of digital banking systems and technology, regularly reviewed, and updated. Banks ought to detect suspicious transaction or withdrawal.

In the case of ***Abacus Parental Drugs Limited v Stanbic Bank(U) Limited***[35] The plaintiff argued that the defendant bank should have ascertained the true beneficiary bank names before effecting the wrong withdrawals. The court also stated that the bank did not show that the online payment system had sufficient security features to safeguard against incorrect payments following its contractual obligations. "The bank had a duty to put in place robust fraud detection and prevention solutions to protect its system and customers." At the bare minimum, the online banking system should have flagged the repeated use of the same account numbers in the names of different beneficiaries.

Banks also ought to guarantee that transactions on their e-platform can be tracked down and scrutinised, given they have been received by their systems. This was seen in the case of ***Aida Atiku v Centenary Rural Development Bank***.[36]**,** where the defendant was able to adduce evidence of the transaction that had been carried out by the plaintiff or while using the plaintiff's contact and credentials. The duty of the bank also extends to tracing and checking transactions made by its systems, as per the case of ***Stanbic Bank Uganda Limited v Moses Rukidi Babigogo***.[37]

---

[35] Civil Suit no.0322 of 2022.
[36] Civil suit no.0754 of 2020.
[37] HCCA No. 0028 of 2023.

Banks in Uganda, to promote security, have provided their customers with periodically upgraded data on accessibility to e-banking services, customer ID, election of appropriate passwords, how to maintain their security through the availability of additional authentication or security options, for example, biometric authentication and one-time password (OTP). In ***Aida Atiku v Centenary Rural Development Bank*****,** "one of the interventions made available to the plaintiff to enhance the level of protection of her funds deposited on the account was her registration for SMS notifications so that she could receive alerts when any transaction was going on her account."

Banks also go on to educate consumers on their responsibility for unauthorised transactions under the contract that has been signed. For example, where a customer shares their transactions with anyone, it entails the possibility of losing any safety offered by the bank against unauthorised transactions and this can result into the customer being responsible for any illegitimate transactions on his or her account and in such cases the customer will not be reimbursed for any consequent damage.

In the case of ***Olanya Hannington v Acullu Hellen***[38] Justice Mubiru held that "it is trite law that when a document containing contractual terms is signed, then in the absence of fraud or misrepresentation, the party signing it is bound. Courts are also hallowed by the legal maxim that it is the business of courts to rewrite contracts between parties. They are bound by the terms of their contracts, unless coercion,

[38] Civil Appeal No.0038 of 2016

fraud, or undue influence are pleaded and proved.[39]

Many senior citizens are vulnerable to online fraud and tend to assume that mobile phones are communicative and not making banking operations. Financial institutions have therefore gone on to educate their customers, the senior citizens, on the preindication and imminent threats in digital banking so that they can build trust in the online banking system and prevent account takeovers. While educating their customers, banks also inform their customers of the applicable terms and conditions of using e-banking, any applicable fees, and their maximum limits, which may be altered occasionally and are available on demand.

"Fraud like account takeover starts with compromised credentials that have been obtained through trickery,"[40] and because customers reuse and share their PINs, the risk of account takeover skyrockets. The financial institutions, therefore, recommend change of the non-permanent password given, for example, when opening a bank account, to a confidential password, since inflexibility may be interpreted as dereliction of duty of the customer.

Financial institutions also go on to inform their customers of the procedure they ought to follow to report a data breach, accounts, or disputed transactions using digital banking services. They are also provided with acceptable ways to inform their bank of all the security breaches and easy-to-reach contact points to report such activity as soon as they learn of it.

---

[39] Pius Kimaiyo Langat v Co-operative Bank of Kenya Ltd (2017) eklr.
[40] Aida Atiku V Centenary Rural Development Bank Civil suit no.0754 of 2020.

The financial institutions play a major role in promoting security but their role is supplemented by the customer's responsibility to ensure that fraud is done away with. The customers should always keep their banking information, user IDs, passwords and PIN numbers confidential.[41] On the acquisition of the login credentials of a legitimate user, and fraudsters misappropriate the account, then account takeover happens. This therefore means that digital bank customers should keep their credentials confidential. Where their accounts have been tampered with, the customers have a duty of reporting the same to their relevant bank authorities.

## 2.5 Conclusion

In conclusion, the chapter majorly discusses the non legal aspects of digital banking diving into how digital banking developed in Uganda from the traditional methods of banking to the development of financial technology, the challenges experienced by customers while using digital banking among which include financial illiteracy and fraud and how the banks themselves have tried to promote safety for customers while using the digital banking system for example through promoting awareness and putting in place a robust security system for their online banking system.

The next chapter, which is chapter three, shall mainly discuss the legal regime governing digital banking looking at international, regional and the domestic perspective.

[41] Aida Atiku V Centenary Rural Development Bank Civil suit no.0754 of 2020.

## CHAPTER THREE

# 3.0 LEGAL REGIME GOVERNING DIGITAL BANKING IN THE FINANCIAL SECTOR

## 3.1 INTRODUCTION

The legal regime governing the digital banking sector is pivotal in shaping the dynamics of this industry. It involves international laws which are greatly challenged by cross border regulations encompassing different requirements across different jurisdictions and high compliance cost of implementing these laws.

Ensuring compliance with regulatory standards is a legal obligation crucial for maintaining customer trust in e-banking. E-banking is a crucial element of a global economy and, therefore, serves as an example of how regulatory frameworks can influence consumer protection.[42] The regulatory frameworks play a crucial role in ensuring stability, transparency, and fairness.

Effective regulation starts with a sound legal and regulatory framework. The essential ingredients of a functional regulatory and supervisory legal framework are laid down in various international standards for financial sector supervision. In the financial sector, the legal framework must provide for transparency and strong regulatory oversight.[43] "While regulatory compliance in banking is essential, it presents several challenges for digital banks, for example cross cross-border regulations, cost of compliance, and so on."[44]

The analysis of this chapter is premised on three primary frameworks: the

---

[42] Onyeka Chrisanctus Ofodile, Digital Banking Regulations; A comparative review between Nigeria and the USA, [2024] Volume 6, Finance and Accounting Research Journal.
[43] Financial Sector Assessment a Hand Book, Chapter 9, Assessing the Legal infrastructure for Financial Systems
[44] https://www.ezbob.com/regulatory-compliance-in-digital-banking/.

international, the regional, and the domestic legal framework. Each of these frameworks is explored in depth with a focus on the legal principles, statutes and case law on customer awareness and digital banking fraud.

## 3.2 INTERNATIONAL LEGAL FRAMEWORK.

The international legal framework governing digital banking embodies the rules, regulations, and practices governing the activities of financial institutions operating across national borders, shaped by a network of global standards, laws, and guidelines developed by various international bodies. This field encompasses the digital transfer of money and having consolidated banking services on a global scale. International banking and finance law is influenced by numerous treaties, conventions, and regulatory bodies.

## 3.3 THE BASEL COMMITTEE ON BANKING SUPERVISION (BCBS)

"The Basel Committee on Banking Supervision (BCBS) was founded in Basel at the end of 1974 to enhance the security and reliability of the international banking system." The Committee fosters exchanges of information and cooperation between supervisory authorities, as well as issuing minimum standards and guidelines for worldwide supervision of banks.[45] The BCBS also strengthens banking regulation, governance, and risk management and brings about greater financial stability globally. This committee, therefore, sets and promotes global banking regulation standards and monitors their implementation.

The BCBS issued the **Basel Accord,** which sets international prudential banking

[45] https://www.finma.ch/finma/international-activities/policy-and-regulation/bcbs/.

regulation standards. A reform package in 2010 called Basel III was published by the Basel Committee to bolster capital and liquidity requirements, and in 2017, it published its final Basel III standards." The second pillar of Basel III covers the supervisory review process, which ensures that banks have sufficient capital to back all risks and also requires management of these risks"[46] fraud inclusive. It also focuses on stress testing, capital adequacy, and liquidity requirements.

"Digital fraud is relevant to the work of the committee because it looks at financial losses to banks resulting from digital fraud suffered by banks themselves directly due to the need to refund their customers for the losses they have suffered be it the banks' fault or not. In extreme cases, such financial losses could reduce banks' capital resources and shock-absorbing capacity, which may have spillover effects to other banks or market participants."[47] It also considers reputational risks to banks and supervisors resulting from high profile digital fraud incidents for example enhanced by broad coverage, public discontent.

"This could translate to a broader, system-wide loss of trust in the integrity and resilience of banks that could lead to, for example, mass bank deposit withdrawals."[48] Both the Basel II and III standards require banks to gather data on all damages from internal and external fraud, though generally from the core division of e-fraud. The Bank of Uganda is currently implementing the Basel II Capital

---

[46] https://www.finma.ch/finma/international-activities/policy-and-regulation/bcbs/.

[47] Digital fraud and Banking: Supervisory and financial stability implications.

[48] Digital fraud and Banking: Supervisory and financial stability implications.

Accord and currently implementing some elements of Basel III. The Bank of Uganda is implementing Basel standards by revising the minimum capital adequacy requirements and minimum capital requirements[49]. The Basel Committee, despite fearing the loss of trust in the digital banking sector due to the increase in digital banking fraud, did not put in place measures to mitigate the fraud and increase customer awareness.

### 3.4 UNICTRAL MODEL LAWS

"The United Nations Commission on International Trade Law (UNICTRAL) is responsible for enacting model laws that facilitate cross-border trade and commerce among States in the International Community." UNICTRAL Model Laws, which are pivotal legislations for providing fundamental guidelines for states to facilitate the suitable operation of International Trade, are developed under the guidance of the United Nations with a target of harmonising and standardising trade practices across borders.[50]

Among the laws applicable to digital banking is the **UNCITRAL Model Law on Electronic Commerce of 1996**. This law makes e-commerce conducted using electronic means easier by providing national legislators with a set of additionally permissible rules for removing legal impediments and enlarging legal applicability

---

[49] https://afmpanga.com/banking-regulation-2024-law-and-practice/#:~:text=Adherence%20to%20Basel%20Standards,required%20capital%20requirements%2C%20among%20others.

[50] https://blog.ipleaders.in/all-about-uncitral-model-laws/#:~:text=The%20UNCITRAL%20Model%20Laws%20aim,and%20predictability%20in%20trade%20practices

for electronic commerce.

Another law applicable in the event is the **UNCITRAL Model Law on Electronic Transferable Records (MLETR)**. Electronic Transferable records are digital equivalents to traditional movable documents like bills of lading, bills of exchange, promissory notes, and house receipts. "This law aims to enable the seamless digitalization of trade by ensuring that electronic records can be used and trusted in the same way as their paper counterparts, thereby promoting efficiency, reducing transaction costs, and enhancing security and traceability of international trade operations."[51]

The UNCITRAL model laws generally govern digital banking, promoting its efficiency and transition from the traditional mode of banking. These laws however do not identify the risks involved in this system i.e. fraud. Where the law fails to identify the risks involved in this kind system, it means that no measures to mitigate the risks can be put in place to curb this.

### 3.5 INTERNATIONAL MONETARY FUND GUIDELINES

"The International Monetary Fund was created to promote international monetary cooperation and oversee the stability of the international monetary system as well as contribute to the countries' economic and financial stability, it therefore plays a key role in this new evolving space of digital banking."

The International Monetary Fund does not have specific guidelines about digital banking. It, however, proposes firmly established principles in foundational requirements and best practices and emphasizes the benefits of user onboarding and

[51] MLETR: An Overview of UNCITRAL's Model Law on Electronic Transferable Records, [2024].

public consultation to mitigate cyber risks[52] Fraud inclusive. This plays a central role in offering technical support to member countries.

### 3.6 EUROPEAN UNION REGULATIONS.

The idea behind the European Union Regulatory framework is to monitor and control risks while favouring the desired innovation of digital finance, which includes digital banking. The European Commission, together with the European Central Bank, therefore conducts regular reviews of the European Union Regulatory Framework and checks its ability to face risks. "In 2020, the commission tabled a major digital Finance strategy to provide a sound, EU-level regulatory and supervisory framework in several digital Finance domains."[53] Uganda is a non-member of the European Union, but incentives provided by this body economically, politically, and legally mandate Uganda to comply with the regulations.

"The council adopted the **Digital Operation and Resilience Act** in 2022 to ensure that the European Financial sector can cope with severe operational disruptions." It goes on to provide requirements for the security of network and information systems of companies and organisations operating in the financial sector. These requirements are homogeneous across all EU member states. This act also aims to promote consumer protection.

"The European Union also established a framework for European Digital Identity known as the ***European Digital Identity (EUDI) Regulation*****,** building on the 2014 Regulation on electronic Identification and trust services for electronic transactions

[52] Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch: Cyber Resilience of the Central Bank Digital Currency Ecosystem, August 2024.
[53] Digital Finance Legislation: Overview and State of Play.

in the internal market (eIDAS Regulation).” The EUDI promotes digital identity by enabling the creation of a universal, trustworthy, and secure European digital identity wallet. “The EUDI also promotes a harmonized security approach, facilitating widespread acceptance of digital identities throughout the European Union.”[54]

The EUs comprehensive directives and regulations such as the **Markets in Financial instruments directives (MiFID)** and the capital requirements directive have a profound influence on international banking practices. For example, the MiFID’s capital requirements particularly, the MiFID II ensures that firms have adequate capital to cover their risks, fraud inclusive.

The laws discussed above focus only on the security of the networks and leave out customer awareness. Security of networks and customer awareness go hand in hand, in that in case the security of these networks is tampered with, then the customers know what to do and will not be affected, avoiding financial loss. If the security of networks is tampered with and the customers are not educated on what to do if something like that happens, they will end up suffering financial loss.

### 3.7 REGIONAL LEGAL FRAMEWORK

The regional legal framework governing digital banking consists of the laws, treaties, and other legal instruments applying within a specific geographic area, for example, a continent, region, or group of countries. Regional legal frameworks play an important role and complement international legal standards. The regional legal framework concentrates on resolving local issues and can differ between regions,

[54] https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation#:~:text=Service%20providers%20legally%20obliged%20to,by%20the%20other%20member%20states.

and serves as a basis for potential national laws.

### 3.7.1 AFRICAN DEVELOPMENT BANK

"The African Development Bank was created in 1963 in Khartoum, Sudan, where 23 newly independent African countries signed the agreement establishing the institution." "On September 10th, 1964, the agreement came into force when 20 member countries subscribed to 65% of the Bank's Capital stock."[55] Uganda is a member of the African Development Bank and therefore subscribes to its regulations thereunder.

The bank-established initiatives that apply to the digital banking system in Uganda, especially the ***Africa Digital Financial Inclusion Facility (ADFI)***, launched in June 2019, whose vision is to ensure widespread access to quality digital financial services as a driver of inclusive growth across Africa. ADFI aims to catalyze financial inclusion by investing in digital financial solutions with beneficiaries including regional bodies and communities.

The ADFI provides funding to different projects that aid in digital fraud mitigation. These may not be particularly relevant to Uganda but Africa as a whole, for example, the African Cyber Security Resource Centre was funded with 42 million grant to fight cyber crime across the continent.[56]

This initiative looks at the using of digital means to be able to provide financial services to individuals who are not served by traditional financial institutions with an aim of making these financial services more accessible. It however does not look

[55] AfDB in Brief, May 2013.
[56] https://www.afd.fr/en/actualites/communique-de-presse/afd-supports-digital-financial-inclusion-women-africa.

at the fact that there are risks involved and the need to educate these individuals about the risks involved.

### 3.7.2 THE COMMON MARKET FOR EASTERN AND SOUTHERN AFRICA (COMESA)

"COMESA was initially established in 1981 as the Preferential Trade Area for Eastern and Southern Africa (PTA) within the framework of the Organisation of the African Unity's (OAU) Plan of Action and the Final Act of Lagos." The PTA transformed COMESA in 1994. "COMESA is one of the eight regional Economic Communities (RECs) recognised by the African Union."[57] COMESA has different regulatory frameworks that are aimed at curbing digital banking fraud, among which include the Model Policy Framework on Digital Retail Payments for Micro, Small, and Medium-Sized Enterprises, the Model Law on Electronic Transactions and Digital Financial Inclusion Initiatives.

The key pillars of the **Model Policy Framework on Digital Retail Payments for Micro, Small, and Medium-Sized Enterprises,** among others, include cybersecurity, wherein cyberattacks are a looming threat to the payments. "Individual Financial Services Providers (FSPS) must safeguard and undertake a regular assessment of the cybersecurity of their services and report the results to the supervisory authorities."[58]

This pillar focuses on cybersecurity neglecting the customer awareness. Cybersecurity and customer awareness go hand in hand, in that in case cyber security is jeopardised, then the customers know what to do and will not be affected avoiding

[57] COMESA in brief.
[58] The Model Policy Framework on Digital Retail Payments for Micro, Small & Medium sized Enterprises in COMESA Towards Digital Financial Inclusion for MSMEs in the Region, page 20.

financial loss. If cybersecurity is jeopardised and the customers were not educated on what to do if something like that happens, they will end up suffering financial loss.

Another pillar of the policy framework is consumer protection. The recent development of digital banking is penetrating the market, which is more vulnerable to digital banking fraud, and has inadequate solutions. Despite the fast-paced development of financial systems, there is a lack of knowledge on handling risks linked to these systems. Given the incentive in integration and cross-border trade, this framework offers fundamental understanding and pushes for the strengthening of consumer protection oversight across the entire COMESA Region."[59] Which Uganda is part of. The policy goes on to give recommendations/ proposed measures to member states to be able to promote cybersecurity and Consumer Protection.

"The COMESA Business Council is also implementing a Digital Financial Inclusion (DFI) programme that supports the design, development, and deployment of an integrated regional digital retail payment scheme that is low-cost, interoperable, and fraud-resistant, serving Micro Small and Medium-sized enterprises (MSMEs), for the COMESA Region".[60] This looks at how resistant the system would be to fraud, but does not look at what would happen in case the system is susceptible to fraud. It does not look at the fact that customers being defrauded could destroy the trust that they have in these systems. It also does not look at what they would do to educate their customers in case they suffer a loss due to fraud.

[59] The Model Policy Framework on Digital Retail Payments for Micro, small & Medium sized Enterprises in COMESA Towards Digital Financial Inclusion for MSMEs in the Region, page 23.
[60] https://comesabusinesscouncil.org/digital-financial-inclusion/.

### 3.7.3 EAST AFRICAN COMMUNITY

"The East African Community was established in 1999 with the signing of the treaty on the 30th day of November." The treaty then entered into force on 7th July 2000. The East African Community Organisation provides for cooperation, including the maintenance of a common market and the operation of common services between Burundi, the DRC, Kenya, Rwanda, Somalia, South Sudan, Tanzania, and Uganda.

"The EAC established the **EAC Model ICT Regulatory Framework** to establish a harmonised approach for the regulation of ICT services and networks."[61] This framework ensures that member states put in place laws that clearly define the responsibilities of the different players, including the consumers.[62] Member states, Uganda inclusive, shall ensure that the consumer rights are protected, while requiring ICT Service providers to take appropriate measures on consumers' data protection.

The model regulatory framework mandates member states to ensure that they put in place a legal framework for safeguarding computer systems and ICTs, including criminalisation of offences thereto[63]. Member states also must ensure that there is a regulatory framework that provides for E-transactions under **Section 18** of the **EAC Model ICT Regulatory Framework**.

"The **EAC Model Policy on Electronic Transactions**, member states of the East African Community, have assimilated different forms of E-transactions, comprising mainly online and mobile payments." Uganda, in particular, has adopted various

---

[61] Section 1, EAC Model ICT Regulatory Framework.
[62] Section 13, EAC Model ICT Regulatory Framework.
[63] Section 17, EAC Model ICT Regulatory Framework.

forms of E-transactions with some electronic ordering and delivery, but mainly electronic payments and banking, largely by the private sector. One of the objectives of the policy is to propose measures to ensure the safety and confidence of the consumers of E-transactions under section 3, paragraph (d).

The regulations under the East African Community encourage member states to put in place different laws governing the data protection of consumers, criminalising offences thereto. In Uganda, some of these laws were enacted, but however lacking in the aspect of defining what digital banking fraud is and penalties for those who carry out the fraud and their traceability. Financial institutions are only encouraged to ensure that they can identify the fraud, but it is not stipulated under the law.

Financial institutions are also left to determine the liability of who is liable in case of this fraud, as stipulated in their contracts.

The EAC policy has reduced the level of digital banking fraud due to the enactment of the laws; however, their enforceability is limited by budgetary constraints.

### 3.8 DOMESTIC LEGAL FRAMEWORK

Domestic legal frameworks, also known as national legal frameworks, play a crucial role, especially where a country has not ratified many international instruments or developed frameworks for regulating digital banking. "The Supreme law governing digital banking in Uganda is **The Constitution of the Republic of Uganda, 1995,** as amended, and it is binding on all people and authority on the land therefore the constitution is the law that governs the land and all the laws formed must conform to it as provided for under Article 2."[64]

[64] The 1995 Constitution of the Republic of Uganda as amended.

The constitution under article 8A (1)[65] "Provides that Uganda shall be governed based on principles of national interest and common good enshrined in the national objectives and directive principles," and under Article 8A (2), "provides that Parliament shall make relevant laws for purposes of giving full effect to clause (1) of the article." Parliament is therefore given the powers to make laws to put into force the different objectives that are provided for in the 1995 constitution of Uganda as amended. "The state also must provide a peaceful, secure, and stable political environment, which is necessary for economic development under objective 3, paragraph 5 of the constitution."

The following legislations govern digital banking in Uganda

- The Financial Institutions Act, Cap 57
- National Payment Systems Act, Cap 59
- National Payment Systems (Consumer Protection) Regulations, 2022.
- Consumer Protection Guidelines of 2013
- Bank of Uganda Financial Consumer Protection Guidelines, 2011
- Financial Institutions (Agent Banking) (Amendment) Regulations, 2023.

### 3.8.1 FINANCIAL INSTITUTIONS ACT, CAP 57.

Article 8A (2) of the Constitution provides that "Parliament shall make relevant laws for the purposes of giving full effect to clause (1) of the article." Parliament is therefore given the powers to make laws to put into force the different objectives that are provided for in the 1995 constitution of Uganda as amended. It is through

[65] The 1995 Constitution of the Republic of Uganda as amended.

this provision that parliament enacted the Financial Institutions Act.

**Section 2 of the FIA** defines an agent to mean "a person contracted by a financial institution to provide financial institution business on behalf of the financial institution under the act," and "agent banking to mean the conduct by a person of financial institution business on behalf of a financial institution as may be approved by the Bank of Uganda. Agent banking is one of the modes of digital banking practiced in Uganda."

Agent Banking is also governed by the Financial Institutions (Agent Banking) (Amendment) Regulations of 2023. The regulations establish the bank's liability as long as the agent operates within the terms of the agreement and the regulations.

The FIA provides for what agent banking is, but not the rules that would govern fraud in respect to agent banking and customer awareness.

### 3.8.2 NATIONAL PAYMENT SYSTEMS ACT

The National Payments System Act has an objective "to provide for the safety and efficiency of payment systems."[66] "A payment system is defined under section 3 to mean a system used to effect a transaction through the transfer of monetary value and includes the institutions, payment instruments, persons, rules, procedures, standards, and technologies that make such a transfer possible". "A payment services provider shall comply with the requirements of consumer protection as may be prescribed by the Bank of Uganda."[67]

The act provides for compliance with consumer protection, but does not necessarily

---

[66] Section 2(a) National Payments Systems Act, Cap 59.

[67] Section 65(1) National Payments Systems Act, Cap 59.

outline what the banks ought to do to protect consumers from digital banking fraud and how to promote consumer awareness of the same.

### 3.8.3 BANK OF UGANDA FINANCIAL CONSUMER PROTECTION GUIDELINES, 2011.

The Bank of Uganda Financial Consumer Protection Guidelines, 2011, apply to all financial service providers regulated by the Bank of Uganda and all the agents of all financial services providers regulated by the Bank of Uganda. They go on to define a consumer to "meaning an individual or a small firm who uses, has used, or is or maybe contemplating using any of the products or services provided by a financial services provider."[68]

One of the objectives of the guidelines is to foster confidence in the financial services sector and to provide efficient and effective mechanisms for handling customer complaints relating to the provision of financial products and services.[69] "The guidelines go on to provide that the relationship between a financial services provider shall be guided by three key principles, that is, fairness, reliability, and transparency." "The terms and conditions provided by a financial services provider shall highlight to a consumer the fees, charges, penalties, any other consumer liabilities or obligations in the use of the financial product or service."[70]

The guidelines also provide that "financial services providers shall ensure that information about their procedures for handling complaints is easily available at their branches, websites, and any other communication channels that they use, and the financial services provider shall investigate the complaint it has received

[68] Paragraph 3 of the Bank of Uganda Financial Consumer Protection Guidelines, 2011.
[69] Paragraph 4 (c) and (d) of the Bank of Uganda Financial Consumer Protection Guidelines, 2011.
[70] Paragraph 8(3) of the Bank of Uganda Financial Consumer Protection Guidelines, 2011.

competently, promptly, and impartially."

The laws discussed above aim at ensuring the efficiency of the digital banking services, and also provide that they provide mechanisms for handling consumer complaints in respect of e-services. They, however, do not identify the risk of fraud that could be involved. They also do not outline the role the financial institutions play in trying to mitigate this risk, and in particular, by carrying out customer education. This would help boost the customer's confidence in the digital banking sector.

## 3.9 CONCLUSION

The discussions in this chapter examined the legal regime governing customer awareness and digital banking fraud in Uganda. The study shows deficiencies within the available laws in mitigating digital banking fraud in Uganda, as most of the laws only aim for making sure that the system is efficient by providing security to these systems while neglecting the implementation of customer awareness. This ends up frustrating customer trust in the financial institution sector.

Chapter 4 of the study is going to address the findings of the research, recommendations, and a conclusion about the research made.

# CHAPTER FOUR

## 4.0 SUMMARY OF FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

## 4.1 INTRODUCTION

As the final chapter in the dissertation, it summarises the findings of this entire research and, where applicable, suggests necessary solutions to the challenges faced in research. The main goal of this research was to investigate the measures financial institutions can implement to enhance customer awareness and prevent digital banking fraud in Uganda's Financial Sector.

## 4.2 SUMMARY OF FINDINGS

It was established that COVID-19 led to the rapid growth of digital banking across the globe. Consumers were discouraged from visiting bank branches and instead pushed to used e-banking during this period. Financial institutions offer digital banking services through channels such as e-wallets and banking.

The results demonstrated that, notwithstanding the productivity and ease of digital banking, there is fraud in this system. The different kinds or types of digital banking fraud include the following;

- Vishing, also known as a phone call scam
- Phishing, also known as an email scam
- Spear Phishing, i.e., targeted email scam
- Skimming, which is an ATM Scam
- SIM Swap, i.e., mobile number scam
- Smishing, i.e., SMS Scam

- Website Spoofing, i.e., fake website scam
- Malware attack, i.e., Gadget Virus attack.

The findings suggest that the increase in digital banking fraud frustrates customer trust in Uganda's financial sector. The user training, however, encourages different individuals to identify the tactics used by fraudsters, avoid scams, protect their information, and take appropriate action when they suspect any fraud.

The results cast light on the international and regional legal regimes that are there to ensure that member states enact laws that govern digital banking, digital financial inclusion. They, however, do not specify when it comes to fraud and customer awareness.

It is therefore vital to understand that the legal regime governing digital banking in Uganda has loopholes concerning digital banking fraud and customer awareness. The legal framework provides for the effectiveness of e-banking and promotion of security and data protection of consumers. The legal regime, however, does not provide for the carrying out of customer awareness to be able to mitigate digital banking fraud.

From the results, it is clear that the legal regime aims at fostering credence in the financial services sector and providing highly functional systems for handling customer grievances while using e-products and services. This means that institutions ought to have a system in place for handling complaints related to digital banking fraud.

Overall, it is clear that customer education aids in mitigating digital banking fraud in a way that different individuals can identify the tactics used by fraudsters, avoid

scams, protect their information, and take appropriate action when they suspect any fraud. This, in the end, boosts customer trust in the banking sector.

In conclusion, the discussion on the legal regime governing digital banking in Uganda, internationally, regionally, and domestically, was able to show the loopholes, especially regarding customer awareness. The laws discuss consumer protection, which encompasses things like promoting cybersecurity, but neglect the promotion of customer awareness on the different types of digital banking fraud that they are susceptible to.

Safaricom M-PESA in Kenya has invested significantly in customer awareness campaigns and found that customer awareness through clear communication messages is the most effective preventive tool for fighting customer scams. Safaricom uses SMS text messages among others to promote customer awareness.

## 4.3 RECOMMENDATIONS

There is a need to promote safety in Uganda's Financial Sector in regards to digital Banking. This is because the world is growing and greatly revolving around the internet in everything, including banking. This makes it convenient for customers to be able to easily access banking services from different financial institutions.

Clear guidelines or regulations on digital banking be put in place. These guidelines should criminalise digital banking fraud and prescribe mechanisms for the recovery of evidence about digital banking fraud. The guidelines should also prescribe the modes through which customer awareness in regards to digital banking fraud should be carried out. Most of the available laws were more applicable to the traditional system of Banking. The lawmakers ought to understand the different services offered to customers under digital banking and how they can be affected by fraud. The Bank

of Uganda should implement the guidelines put in place by the legislators.

Existing laws in Uganda be assessed and revised as appropriate to clearly define what digital banking fraud is and point out the liabilities of both the bank and the customers when it comes to digital banking fraud. The lawmakers should also introduce policies, regulations and supervision, and review processes that enable the financial institutions to develop an effective system for promoting customer awareness in the financial institution sector.

Financial institutions ought to understand the different types of digital banking fraud that their customers are most likely to face, particularly by finding out the reasons why fraudsters can easily commit fraud on their systems and how they can do it. This helps them to cover up the loopholes in their systems.

Financial institutions should also take up the responsibility and carryout customer awareness on digital banking fraud, i.e., how it happens, why customers must protect themselves against such risk, the liabilities of both the bank and customers about digital banking fraud, and what customers can do in case they encounter digital banking fraud. Financial institutions can also utilise the inherent protections in the digital ID systems to avoid scams, for example, auditing login attempts to detect structural misuse of digital IDs to access accounts, including through lost, compromised, stolen, or sold digital ID credentials/authenticators.

## 4.4 CONCLUSION

The results of the study conclude that the use of digital banking fraud is associated with fraud that frustrates the relationship between customers and their banks. The customers can withdraw from those banks where they suffer financial loss as a result of fraud.

To be able to conduct this study, research questions were used to be able to identify the gaps in the legal framework governing digital banking in Uganda. It was found that the legal framework promotes the efficiency of digital banking services, but does not look at the risks involved, and when it looks at the risks involved, it focuses on promoting cybersecurity. This tends to ignore the importance of customer awareness in mitigating digital banking fraud in Uganda's financial sector.

The legal framework governing digital banking in Uganda ought to be revised to be able to incorporate provisions defining what digital banking fraud is, customer and financial institution liability and responsibility in regards to the same and measures, especially customer awareness required to mitigate the risk of digital banking fraud.

## BIBILIOGRAPHY


**NATIONAL LAWS**

Banking (Amendment) Act, No. 34 of 1969

Banking Act, Cap 88, 1964.

Banking Act, No.16 of 1966

Consumer Protection Guidelines of 2013

Financial Institutions (Agent Banking) (Amendment) Regulations, 2023

National Information Technology Authority, Uganda Act, no.04 of 2009

National Payment Systems (Consumer Protection) Regulations, 2022.

National Payment Systems Act, Cap 59

The Access to Information Act, Cap 95

The Bank of Uganda Financial Consumer Protection Guidelines, 2011.

The Computer Misuse Act, Cap 96.

The Constitution of the Republic of Uganda, 1995, as amended

The Electronic Signatures Act, Cap 98

The Financial Institutions Act, Cap 57,

The Micro Finance Deposit-Taking Institutions Act, Cap 58,

The Regulation of Interception of Communications Act, Cap 101.

Uganda Credit and Savings Bank Act, Cap 90, 1964

**INTERNATIONAL LAWS**

Africa Digital Financial Inclusion Facility (ADFI), 2019

Basel Accord

Digital Operation and Resilience Act, 2022.

EAC Model ICT Regulatory Framework

EAC Model Policy on Electronic Transactions

European Digital Identity (EUDI) Regulation

International Monetary Fund guidelines

Markets in Financial Instruments Directives (MiFID)

Model Policy Framework on Digital Retail Payments for Micro, Small, and Medium-Sized Enterprises

Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, 2014.

UNCITRAL Model law on electronic commerce of 1996.

UNCITRAL Model Law on Electronic Transferable Records (MLETR)

**LIST OF CASES**

Abacus Parental Drugs Limited v Stanbic Bank(U) Limited Civil suit no.0322 of 2022

Aida Atiku v Centenary Rural Development Bank Civil suit no. 0754 of 2020

Olanya Hannington v Acullu Hellen Civil Appeal No. 0038 of 2016.

Pius Kimaiyo Langat v Co-operative Bank of Kenya Ltd (2017) eklr.

Stanbic Bank Uganda Limited v Moses Rukidi Babigogo HCCA No. 0028 of 2023.

**LIST OF BOOKS**

Brownbridge, M. and Harvey, C. Banking in Africa, 1998.

Bryan A. Garner, Black's Law Dictionary, 12th ed, 2024.

G.P. Tumwine- Mukubwa, Essays in African Banking Law and Practice (2nd edition, 1998), page 2.

**LIST OF ARTICLES**

Abend, V., Peretti, B., Bach, A., Barry, K. & Donahue, D. (20008). Cyber Security for the Banking and Finance Sector, Homeland Security, pp.1-17

AfDB in Brief, May 2013.

Alex Malyshev, Banking Software, March 12, 2025.

Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch: Cyber Resilience of the Central Bank Digital Currency Ecosystem, August 2024.

Chiemeke, S.C., Evwiekpaefe, A.E & Chete, F.O. (2006). The adoption of internet banking in Nigeria; An Empirical Investigation, Journal of Internet Banking & Commerce, Volume 11, Issue 3, p.4.

COMESA in brief.

Deloitte. (2015). India Banking fraud survey, Edition II, April 2015. Deloitte Touche Tohmastu India Private Limited.

Digital Finance Legislation: Overview and State of Play.

Digital fraud and banking: Supervisory and Financial Stability Implications, November 2023.

Elisa indrisarri, Harjanto Prabowo, Ford Lumban Gaol, Betty Purwandari, Digital Banking; Challenges, Emerging Technology Trends and future Research Agenda.

Financial Sector Assessment A Handbook, Assessing the Legal Infrastructure for Financial Systems.

Five Key digital banking challenges that financial institutions need to address, Lumin Digital.

MLETR: An Overview of UNCITRAL's Model Law on Electronic Transferable Records, [2024].

Narayanan, M., Koo, B. &Cozzarin, B.p (2012). Fear of Fraud and Internet Purchasing, Applied Economics Letters, Volume 19, pp. 1615-1619

Onyeka Chrisanctus Ofodile, Digital Banking Regulations; A comparative review between Nigeria and the USA, [2024] Volume 6, Finance and Accounting Research Journal.

Peter Ellinger, [2013] Banking law and practice I their conceptual and historical

perspectives.

Ranjan Akash, Digital Banking Issues faced by the elderly and the optimal measures to resolve them, (2024) Volume 8, IJSREM

Shewangu Dzomira, Banks and Bank systems, December 2016, Financial consumer protection: Internet banking fraud awareness by the banking sector.

Shubhan Khandal, Customer Awareness on UPI and mobile banking: An exploratory Study.

The Model Policy Framework on Digital Retail Payments for Micro, Small & Medium-sized Enterprises in COMESA Towards Digital Financial Inclusion for MSMEs in the Region

Uganda Bankers Association, Bend But do not break, How the Financial Sector can thrive .

**WEBSITES**

https://taslafadvocates.com/users-guide-a-legal-guide-to-ugandas-financial-sector/#:~:text=Introduction,financial%20capital%20in%20an%20economy

https://www.aubank.in/blogs/8-different-types-of-digital-banking-frauds

https://www.ezbob.com/regulatory-compliance-in-digital-banking

https://www.finma.ch/finma/international-activities/policy-and-regulation/bcbs

https://afmpanga.com/banking-regulation-2024-law-and-practice/#:~:text=Adherence%20to%20Basel%20Standards,required%20capital%20requirements%2C%20among%20others

https://blog.ipleaders.in/all-about-uncitral-model-laws/#:~:text=The%20UNCITRAL%20Model%20Laws%20aim,and%20predictability%20in%20trade%20practices

https://www.digital-strategy.ec.europa.eu/en/policies/eudi-regulation#:~:text=Service%20providers%20legally%20obliged%20to,by%20the%20other%20member%20states

https://www.comesabusinesscouncil.org/digital-financial-inclusion

https://www.afd.fr/en/actualites/communique-de-presse/afd-supports-digital-financial-inclusion-women-africa