MAKERERE LAW JOURNAL MARCH 2024

Volume 53 Issue 4

BANKING BEYOND THE BANKING HALL: A REVIEW OF DIGITAL BANKING IN UGANDA

Nasser Konde

Recommended Citation: Nasser Konde (2024); "Banking Beyond the Banking Hall: A Review of Digital Banking In Uganda" Volume 53 Issue 4 Makerere Law Journal pp. 116-149

BANKING BEYOND THE BANKING HALL: A REVIEW OF DIGITAL BANKING IN UGANDA

Nasser Konde*

ABSTRACT

Technology advancement has greatly revolutionized the banking industry in Uganda. This has seen the adoption of digital banking by all financial institutions in the country in order to serve their customers better and to remain relevant in the sector. The COVID-19 pandemic saw a complete shift in the way financial institutions in Uganda offered banking services to customers with many merging and closing down the various bank branches across the country and concentrating their efforts on digital banking. This paper aims at providing an insight on the nature of digital banking, the legal principles that govern digital banking, the legal regime governing digital banking, the risks involved and how to mitigate them.

1.0 INTRODUCTION

Until the early 2000s, Uganda maintained an economy largely based on a cash payment system. The introduction of the Automated Clearing House and Real Time Gross Settlement systems saw the first revolution in the financial market take place. Other payments innovations such as credit cards and agency banking soon followed, sweeping the financial sector into the era of digital financing.

Since 2009 when Mobile Money services were launched in Uganda through a partnership between Stanbic Bank Uganda and MTN Uganda, mobile money

* BIT (MUK), LLB (MUK), CCNA, Dip LP (LDC).

service providers such as MTN Uganda Limited have largely dominated the digital financial services market. The network of mobile money services is comprised of mobile network operators, commercial banks, non-bank financial institutions, Bank of Uganda, third-party operators and technology providers. Mobile network operators in partnership with supervised financial institutions offer the services.[1]

Automation and artificial intelligence is already an important part of consumer banking as more and more repetitive tasks become automated, delivering benefits not only for a bank's cost structure, but for its customers as well. Instead of having to travel to a branch office of the bank, customers can now get instant, efficient automated customer service powered by advanced artificial intelligence. [2] Customers can contact their bank any time through the internet, mobile phone or email channels and receive quick, real-time service. Digitizing money transfers for instance speeds up the process and gives customers the flexibility and freedom to view their bank accounts and transact online or with their mobile app.[3]

The COVID-19 pandemic was an unprecedented catalyst for digital banking across the globe. This so many bank branches temporarily shut down and most physical transactions minimized. In Uganda, retail bank consumers had no choice but to embrace digital banking like never before. Digital banking has made it convenient for customers to check accounts statuses, pay bills, transfer money or withdraw cash.[4]

This paper aims at providing an insight on the nature of digital banking, the legal principles that govern digital banking, the legal regime governing digital banking, the risks involved and how to mitigate them.

---

1 Augustine Idoot Obilil , "An Overview of the National Payment Systems Act 2020" available at <www.kaa.co.ug/an-overview-of-the-national-payment-systems-act-2020/ > (accessed on 21 October 2023)

2 Atiku v Centenary Rural Development Bank Limited [2022] UGCommC 146.

3 Ibid.

4 Ibid.

Chapter One offers an introduction to digital banking, Chapter Two discusses the nature of digital banking, Chapter Three discusses the legal principles governing digital banking, Chapter Four discusses the regulatory framework governing digital banking, Chapter Five discusses the risks involved in digital banking, Chapter Six discusses how risks involved can be mitigated, Chapter Seven analyzes the feasibility of the digital banking strategy and Chapter Eight offers a conclusion.

2.0 NATURE OF DIGITAL BANKING IN UGANDA

2.1 DEFINITION OF DIGITAL BANKING

Digital banking, also known as online banking or e-banking, refers to the delivery of financial services through digital channels such as the internet, mobile devices and automated teller machines.[5]

2.2 EVOLUTION OF DIGITAL BANKING

2.2.1 EARLY AUTOMATION

The first forms of digital banking can be traced back to the 1960s, when banks began using mainframe computers to automate various banking functions such as cheque processing and customer account management.[6] During the same time, Bank of America introduced the first Automated Teller Machine, which allowed customers to withdraw cash from their accounts without needing a bank teller.[7] In the 1980s, banks started offering dial up services that allowed customers to access their accounts through their home computers.[8]

---

5 Alice Ivey (2023) , "A brief history of digital banking" available at <https://cointelegraph.com/news/a-brief-history-of-digital-banking > [accessed 14 December 2023]

6 Ibid

7 Ibid

8 Ibid

2.2.2 INTRODUCTION OF ONLINE BANKING

Online banking portals were developed due to increased internet use in the 1990s and 2000s. Banks started creating online portals to enable consumers to see account balances, transfer money and pay bills from their home computers. Online banking quickly became a preferred option for many people due to its convenience. [9] In 2007, USA Federal Savings Bank became the first bank to offer mobile banking through its mobile application. Today, virtually every major bank offers a mobile banking application that allows customers to perform a wide range of transactions.[10]

2.2.3 INTEGRATION OF NEW TECHNOLOGIES

Technological advancements like internet of things, block chain and artificial intelligence have had major impact on digital banking today and will do so in the future. Block chain technology is being utilized to increase the security and effectiveness of cross-border payments.[11] Banks are exploring the use of powered chatbots and virtual assistants to improve customer care and service. Biometrics are also being used to enable customers authenticate transactions using fingerprints or facial recognition and providing real-time insights into their financial health through connected devices. [12]

2.3 FORMS OF DIGITAL BANKING IN UGANDA

Digital banking in Uganda takes the form of Internet Banking, Mobile Banking, ATM Banking, Agency Banking[13] and Mobile Money Banking.

---

9 Alice Ivey (2023) , "A brief history of digital banking" available at <https://cointelegraph.com/news/a-brief-history-of-digital-banking > (accessed 14 December 2023).

10 Ibid

11 Ibid

12 Ibid

13 Regulation 4 of The Financial Institutions (Agent Banking) Regulations 2017 defines Agency Banking as the conduct by a person of financial institutions business on behalf of a financial institution as may be approved by the central bank.

2.4 STAKEHOLDERS IN DIGITAL BANKING

2.4.1 BANK

A bank is any company licensed to carry on Financial Institutions Business as its principal business and includes all branches and offices of that company in Uganda.[14] Given the nature of digital banking a number of different banks can be involved in the conducting of banking business and these include the following;

a. Issuing Bank

This the bank that originates, issues, initiates or sends the payment on behalf of the sender.[15]

b. Intermediary Bank

This the issuing bank's bank that corresponds with the receiving bank.[16]

c. Receiving Bank

This bank receives the payment on behalf of a beneficiary or the final receipt of the funds.[17]

2.4.2 PAYMENT SYSTEM

A payment system is 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.[18] Examples of payment systems include mobile money, electronic funds transfer and Real Time Gross Settlement Systems.

2.4.3 CUSTOMER

---

14 Section 3 of The Financial Institutions Act 2004. In Ham v Daimomd Trust Bank (K) Limited and Another, the Supreme Court observed that banks that are not conducting core business in Uganda are not banks within the meaning of the definition in Section 3 and are not governed by the Financial Institutions Act 2004.

15 Barclays Bank Kenya Limited v Tamima Ibrahim Civil Appeal No. E075 of 2021.

16 Barclays Bank Kenya Limited v Tamima Ibrahim Civil Appeal No. E075 of 2021.

17 Barclays Bank Kenya Limited v Tamima Ibrahim Civil Appeal No. E075 of 2021.

18 Section 1, National Payment Systems Act 2020.

Two parameters determine whether one is a bank customer to wit; having a bank account with the bank and intention or agreement to open an account. In *Great Western Railway Company v London and County Banking Company Limited*[19], the House of Lords stated that one was not a customer of the bank where no account of any sort with the bank was ever kept. In *Woods v Martin's Bank Limited,*[20] the Court observed that the relationship of banker and customer had come into existence when the branch manager agreed to accept the Plaintiff's instruction to open an account in his name.

2.4.4 CONSUMER

A consumer is 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.[21] Given the nature of digital banking, very many individuals use banking services and products without having bank accounts in those specific banks. Case in point is parents who pay their children's' school fees using digital banking products and services like School Pay[22] and agency banking without having bank accounts. These fall under the category of consumers.

2.4.5 AGENT

An agent is a person contracted by a financial institution to provide financial institution business on behalf of the financial institution.[23] In *Ham v Diamond Trust Bank (U) Limited and Another,*[24] the Supreme Court observed that the

19 [1901] AC 414
20 [1959] 1 QB 55.
21 Guideline 3 of The Bank of Uganda Financial Consumer Protection Guidelines 2011.
22 School Pay is a digital school fees payment system that enables parents to pay school fees to schools. How it works is that the schools have an account on School Pay and give students a unique identifying number which is used by parents to pay school fees. The School Pay system is integrated with the banking system of different banks to enable parents to pay school fees through those banks to the respective schools' bank accounts.
23 Regulation 4, Financial Institutions (Agent Banking) Regulations 2017.
24 [2023] UGSC 15.

person envisaged as an agent is a natural person and an artificial person (company) not being a financial institution.

3.0 PRINCIPLES GOVERNING DIGITAL BANKING

3.1 BANKER CUSTOMER CONSUMER RELATIONSHIP

Under digital banking, a unique relationship exists of a banker-customer-consumer relationship. A bank does not only owe a duty to its customers but also consumers who use banking services without necessarily having bank accounts with the bank.[25]

3.2 DUTY OF CARE TO CONSUMERS

Banks at common law owe a duty of care to their customers to execute instructions or mandates from customers diligently bearing in mind the interests of the customers. This duty is commonly referred to as the quincecare duty of care emanating from the case of *Barclays Bank PLC v Quincecare Limited*[26]. This duty has recently been revised and reformulated by the United Kingdom Supreme Court to restrict the Banks to confirmation that the instructions or mandates emanate from a customer and not third parties with banks not having to confirm that the instructions or mandates are in the best interest of the customer or not in the case of *Philipp v Barclays Bank UK PLC*[27].

Banks, because of the Banker Customer Consumer relationship established by Guideline 3 of The Bank of Uganda Financial Consumer Protection Guidelines 2011 under digital banking, now have an expanded duty of care that extends from a bank customer to a consumer of banking services and products who does

---

25 This duty is established by Guideline 3 of The Bank of Uganda Financial Consumer Protection Guidelines 2011. Given the unique nature of digital banking, it is not only bank customers that utilize banking services. For example there are parents that pay school fees for their children using the SchoolPay system through banks yet they do not have bank accounts in those banks. A bank cannot claim not to owe a duty to such parents in case for example their school fees payments do not reflect on the school's bank account with the bank on grounds that the parents are not bank customers.

26 [1992] 4 ALLER 363.

27 [2023] UKSC 25.

not necessarily have a bank account with the bank. The bank cannot for example claim to be exempt from liability where it fails to process a payment made by a consumer on account of no existing relationship or duty of care since the consumer does not hold a bank account with the bank.

This specific scenario has played out a lot especially under agency banking where a customer let say a parent goes to a bank agent to pay school fees for their child and as the transaction is being done it fails along the way probably due to network failure and the school fees paid by the parent does not reflect on the school's bank account. The bank cannot claim to be exempt from liability simply because that particular parent does not hold a bank account with the bank.

3.3 DUTY TO RECOVER PAYMENT

A payment system operator or payment service provider must with the approval of the central bank , prescribe the manner of recovering an equivalent amount of transfer arising from a payment instruction/settlement made in the case of fraud , mistake , error or similar vitiating factors.[28]

Financial institutions equally have a common law duty to recover payments made in the case of fraud, mistake, error or similar vitiating factors. This duty has been well expounded by the United Kingdom Supreme Court in the case of *Philipp v Barclays Bank UK PLC*[29] and by the Kenyan High Court in the case of *Barclays Bank Kenya Limited v Tamima Ibrahim*[30] where the Courts observed that the Appellant banks had a common law duty to recover money fraudulently or erroneously transferred to accounts belonging to third parties.

3.4 INTEROPERABILITY

28 Section 25(3), National Payment Systems Act 2020.
29 [2023] UKSC 25.
30 Civil Appeal No. E075 of 2021.

Interoperability means a set of procedures or arrangements that allow participants in different payment systems to conduct and settle payments or securities transactions across those payment systems while continuing to operate only in their own payment systems.[31]

A number of platforms provide interoperability functions that include the following;

a. Visa

Visa enables clients to process credit and debit card payments through a direct interface to Visa's global payment system. Clients need not have physical cash to make or receive payments.[32]

b. MasterCard

MasterCard empowers digital real time payments through a payment infrastructure, bill payment, e-invoicing applications and open banking ecosystems. Its mission is to connect and power an inclusive digital economy that benefits everyone, everywhere by making transactions safe, simple, smart and accessible.[33]

c. Interswitch

Interswitch is a pan African payment ecosystem that enables interoperability of transactions and payments between predominantly African banks.[34] In Uganda, Interswitch is used by indigenous banks to enable interoperability of transactions amongst their clients.

d. Pegasus

Pegasus offers interoperability services that make it easy to transfer mobile money between different telecom companies.[35]

---

31 Section 1, National Payment Systems Act 2020.

32 Visa Developer Centre, Visa Payments Processing available at <https://developer.visa.com/capabilities/vpp> [Accessed 30 November 2023]

33 MasterCard Payment Processing available at <www.mastercardpaymentservice.com> [Accessed 30 November 2023]

34 Interswitch Group, The Gateway to Africa's Payment Ecosystem available at <www.interswitchgroup.com/uganda/home> [Accessed 30 November 2023]

35 Pegasus Technologies, "Unified Payment Solutions for your business" available at <www.pegasus.co.ug> [Accessed 30 November 2023]

3.5 IRREVOCABILITY OF PAYMENT

A payment instruction or settlement shall be valid and enforceable by and against a payment system operator and shall be final and irrevocable.[36]

A payment order cannot be made by and Court for the rectification or stay of payment instruction or settlement.[37] The above provisions of the National Payment Systems Act 2020 were retaliated by the High Court in *Translink Limited v Standard Chartered Bank (U) Limited*[38] where it observed that a bank has no duty or obligation to countermand or reverse online payments made by a customer.

4.0 REGULATORY FRAMEWORK FOR DIGITAL BANKING

4.1 NATIONAL PAYMENT SYSTEMS ACT 2020

Payment solutions such as mobile money were previously regulated by guidelines such as the Mobile Money Guidelines, 2013 which provided that Bank of Uganda was in charge of approval and supervision of mobile money services. Bank of Uganda was given the mandate to issue directives regarding mobile money operations whereas, Uganda Communications Commission was responsible for licensing and supervision of mobile network operators; ensuring that telecommunications networks were effective.[39]

Oversight of payment systems entails reporting from the payment system and payment service providers to the authorized authority and monitoring, analysis, on-site inspection and licensing of payment systems by the recognized authority. The absence of a comprehensive payment system law that supports the National

---

36 Section 25(1) , National Payment Systems Act 2020.
37 Section 25(2), National Payment Systems Act 2020.
38 Civil Suit Number 415 of 2019.
39 Augustine Idoot Obilil , "An Overview of the National Payment Systems Act 2020" available at <www.kaa.co.ug/an-overview-of-the-national-payment-systems-act-2020/ > [Accessed 21 October 2023]

Payment System had created an environment where there was a significant level of risk associated with the operation of the current systems.[40]

The hitherto inadequate oversight had a major impact on the safety of payment systems in Uganda as there was no definitive legal basis for ensuring that operators and service providers comply with operating norms and regulations. International best practice puts significant emphasis on the need for fulfilment of these functions, as they are the basis for ensuring safety in payment systems. This responsibility is typically given to the central bank of the country.[41] Informed by the above regulatory lacuna, Parliament passed the National Payments Systems (NPS) Act, 2020 in May 2020 and assented to by the President on the 29th day of July 2020. The Act has now been gazetted and is the law effectively regulating payment systems in Uganda.[42]

The Act is aimed at regulating payment systems beyond the traditional systems, providing safety and efficiency of payment systems, providing the functions of the Central Bank in relation to payment systems and providing for the establishment of the national payment systems council, among others.[43] The National Payment Systems Act 2020 regulates payment systems in the following way;

4.1.1 OBJECTIVES OF THE ACT

The objectives of the Act are to provide for the safety and efficiency of payment systems, to prescribe the framework to govern the oversight and protection of payment systems, to provide for financial collateral arrangements, to regulate operators of payment systems, to regulate payment service providers, to regulate

40 Augustine Idoot Obilil , "An Overview of the National Payment Systems Act 2020" available at <www.kaa.co.ug/an-overview-of-the-national-payment-systems-act-2020/ > (accessed on 21 October 2023)
41 Ibid
42 Ibid
43 Ibid

the issuance of electronic money and to provide for the oversight of payment instruments.[44]

4.1.2 CATEGORIES OF PAYMENT SYSTEMS

Payment systems in Uganda are categorized under the Act as payment systems operated by the central bank, [45] payment systems operated by another government entity or in partnership with a government entity in public interest,[46] payment systems operated by private entities[47]and any other payment system approved or licensed by the Central Bank under the Act.[48]

4.1.3 LICENSING

The Act prohibits the operation of a payment services without a licence issued by the Central Bank in accordance with the Act.[49] The only exception provided is payment services offered by the Central Bank. [50] Contravention of the prohibition attracts a punishment of a fine or a term of imprisonment in addition to disqualification from acquiring a licence.[51]

4.1.4 PAYMENT SYSTEMS RULES

An operator of a payment system is required to develop payment system rules to govern the payment system. [52]

---

44 Section 3 (a) – (g), National Payment Systems Act 2020.
45 Section 5 (a), National Payment Systems Act 2020. These include the Real Time Gross Settlement System; the Automated Clearing House; the Central Securities Depository for Government debt securities; cross border payment systems and any other payment system established by the Central Bank.
46 Section 5 (b), National Payment Systems Act 2020.
47 Section 5 (c), National Payment Systems Act 2020. These include switches, electronic money systems and aggregators or integrators.
48 Section 5 (d), National Payment Systems Act 2020.
49 Section 6(1), National Payment Systems Act 2020.
50 Section 6(2), National Payment Systems Act 2020.
51 Section 6 (3) (a) and (b) and (4), National Payment Systems Act 2020.
52 Section 11, National Payment Systems Act 2020.

4.1.5 OVERSIGHT OF PAYMENT SYSTEMS

The Central Bank has the oversight duty over payment systems and this duty includes regulation[53] and revocation of payment system licences.[54]

4.1.6 POWERS OF THE CENTRAL BANK

The Central Bank is accorded power to issue directives to licensees from time to time in respect of payment systems or payment instruments,[55] power to appoint an external auditor to examine a payment system service provider, participant or operator[56]and power to inspect operators of payment systems.[57]

4.1.7 OPENING OF SETTLEMENT ACCOUNTS

Every participant in a payment system is mandated to open and maintain a settlement account in the books of the Central Bank or an authorised settlement agent.[58]

4.1.8 PROTECTION OF SETTLEMENT ACCOUNTS

The balance on settlement accounts with a payment systems are immune from attachment, assignment or transfer for purposes of satisfying any debt or claim.[59]

4.1.9 EFFECT OF COMMENCEMENT OF INSOLVENCY PROCEEDINGS

Insolvency proceedings commenced against a licensee or participant have no retrospective effect on the rights and obligations of a licensee or participant arising from the participation in the payment system.[60] Transactions entered

53 Sections 12 (1) and (2), 19 (1) and (2) and 66, National Payment Systems Act 2020.
54 Section 13(1), National Payment Systems Act 2020.
55 Section 20(1), National Payment Systems Act 2020.
56 Section 21, National Payment Systems Act 2020.
57 Section 22, National Payment Systems Act 2020.
58 Section 26(2), National Payment Systems Act 2020.
59 Section 27, National Payment Systems Act 2020.
60 Section 28 (1), National Payment Systems Act 2020.

into before the commencement of insolvency proceedings but not completed prior to the commencement of insolvency proceedings are also deemed valid and enforceable despite the commencement of insolvency proceedings.[61]

4.1.10 CONSUMER PROTECTION

A payment service provider is mandated to comply with the requirements of consumer protection as prescribed by the Central Bank.[62] A payment service provider is prohibited from misleading consumers through advertisement or purporting to offer a service that is not approved in accordance with the Act.[63] Failure to comply amounts to a criminal offence punishable by a fine or imprisonment or both.[64] Payment system operators are mandated to ensure that payment services are available to the users of the payment system throughout the prescribed operational period.[65] An electronic money issuer is mandated to establish and maintain its primary data centre in relation to payment system services in Uganda.[66]

4.1.11 ESTABLISHMENT OF A SUBSIDIARY LEGAL ENTITY

A payment service provider, other than an entity solely established to issue electronic money, a financial institution or microfinance deposit taking institution, that intends to issue electronic money is required to establish a subsidiary legal entity for that purpose.[67]

4.1.12 ESTABLISHMENT OF REGULATORY SAND BOX FRAMEWORK

The Central Bank is mandated with the responsibility of establishing a regulatory sand box framework for purposes of governing the manner in which a person

61 Section 28 (3) (a) and (b), National Payment Systems Act 2020.
62 Section 65(1), National Payment Systems Act 2020.
63 Section 65 (3), National Payment Systems Act 2020.
64 Section 65 (4), National Payment Systems Act 2020.
65 Section 67, National Payment Systems Act 2020.
66 Section 68, National Payment Systems Act 2020.
67 Section 48 (1), National Payment Systems Act 2020.

may obtain limited access to the payment system eco system for purposes of testing an innovative financial product or service without obtaining a license under the Act.[68]

4.1.13 OPENING UP OF TRUST ACCOUNTS

An electronic money issuer is required to open up a trust account in a financial institution to facilitate the issuing of electronic money.[69]

4.1.14 DUTIES OF TRUSTEES

Trustees [70] have the responsibility to manage the trust account and the interest account on behalf of the customer , establish safeguard measures to protect the funds deposited on the trust account from risks that may occasion loss to beneficiaries of the funds , monitor the trust accounts to ensure that the funds in the trust account are equal in value to the electronic money issued , ensure that interest earned on the trust account is distributed for the benefit of the customer and perform any other duty as the issuer of electronic money may prescribe.[71]

4.1.15 OPENING OF SPECIAL ACCOUNT

A payment service provider who is a financial institution and intends to issue electronic money is required to open and maintain a special account in its books of accounts.[72]

---

68 Section 16 (1), National Payment Systems Act 2020.
69 Section 49 (1), National Payment Systems Act 2020.
70 A body corporate established under Section 49(5) of the National Payment Systems Act 2020 with responsibility to manage trust accounts.
71 Section 53, National Payment Systems Act 2020.
72 Section 51 (1), National Payment Systems Act 2020.

4.1.16 PROTECTION OF TRUST AND SPECIAL ACCOUNT

Funds on the trust and special are immune from attachment, assignment and transfer for satisfying any debt or claim.[73]

4.1.17 DUTIES OF ELECTRONIC MONEY ISSUER

An electronic money issuer has a number of duties that include inter alia mitigating concentration of risk, ensure that interest that accrues on trust and special accounts is directed to customers, publish audited financial statements, honour withdraws of cash or transfer of funds, monitor the creation electronic money, reconcile the electronic money value and perform any other duty as the Central Bank may prescribe.[74]

4.1.18 PERMISSIBLE TRANSACTIONS

Electronic money may be used for domestic payments , domestic money transfers , bulk transactions , cash-in and cash-out transactions , merchant and utility payments , cross-border payments or transfers , savings products , credit products , insurance products and any other transactions approved by the Central Bank.[75]

4.1.19 PROHIBITED ACTIVITIES

An electronic money issuer which is not a financial institution is prohibited from receiving and taking deposits , conducting over the top transactions unless full identification of depositor is obtained , issuing airtime as electronic money and using airtime for permissible transaction under the Act.[76] Contravention of the prohibition amounts to criminal offence that attracts a fine.[77]

---

73 Section 52, National Payment Systems Act 2020.
74 Section 53, National Payment Systems Act 2020.
75 Section 54, National Payment Systems Act 2020.
76 Section 55 (1) and (2), National Payment Systems Act 2020.
77 Section 55 (3), National Payment Systems Act 2020.

4.1.20 DORMANT ACCOUNTS

An electronic account that does not have a registered transaction for nine consecutive months is considered a dormant account.[78] An electronic money issuer is required to issue a notice of one month to a customer that they should carry out a transaction or else their account shall be suspended before the nine-month period reaches.

4.1.21 LIQUID ASSETS REQUIREMENTS

An electronic money issuer is required to keep one hundred percent of the electronic money held in a trust account and special account in liquid assets.[79]

4.1.22 PROHIBITIONS UPON TERMINATION

An electronic money issuer is prohibited from terminating or transferring his or her license to another person or entity without the written approval of the Central Bank.[80] An electronic money issuer is prohibited from terminating their business without prior approval of the Central Bank.[81] An electronic money issuer is prohibited from changing its name, controlling interest or ownership without the approval of the Central Bank.[82]

4.1.23 SUBMISSION OF RETURNS

A licensee is required to submit returns relating to the operation of the payment system or electronic payment service as may be prescribed by the Central Bank.[83]

78 Section 57(1), National Payment Systems Act 2020.
79 Section 60(1), National Payment Systems Act 2020.
80 Section 61(1), National Payment Systems Act 2020.
81 Section 61(2), National Payment Systems Act 2020.
82 Section 61(3), National Payment Systems Act 2020.
83 Section 62 (1), National Payment Systems Act 2020.

4.1.24 RETENTION OF RECORDS

A payment service provider is required to maintain a record of all payment transactions and information.[84]

4.1.25 NOTICE OF CESSATION OF BUSINESS

A licensee that intends to cease to carry on the business for which it was licensed is required to give notice of cessation of business to the Central Bank and publish the notice in a newspaper of wide circulation for at least 30 days before the date of cessation. [85] The notice must be accompanied by a cessation plan indicating that the cessation has been approved by the controlling interest, the procedure for paying all the customers, the mitigation plan for any adverse effects of the cessation of business on the payment systems ecosystem and any other matter as the Central Bank may prescribe.[86]

4.1.26 IMMUNITY OF CENTRAL BANK OFFICIALS

An officer of the Central Bank is not to be held personally liable in respect of any act done in good faith and without negligence in the performance of the functions in the Act.[87]

4.2 THE FINANCIAL INSTITUTIONS (AGENT BANKING) REGULATIONS 2017

Agency banking is governed by The Financial Institutions (Agent Banking) Regulations 2017, which prescribes a number of rules that have to be followed by financial institutions and their agents that include the following;

84 Section 63(1), National Payment Systems Act 2020.
85 Section 70(1), National Payment Systems Act 2020.
86 Section 70(2), National Payment Systems Act 2020.
87 Section 69, National Payment Systems Act 2020.

Conducting agent banking is subject to the written approval from the Central Bank.[88] Financial Institutions are prohibited from conducting agent banking with their employees, affiliates or associates.[89]

Financial institutions have obligations which include assigning agents identification numbers, a parent branch , displaying a list of agents at the respective parent branch , ensuring that technology infrastructure runs effectively , ensuring that agents have appropriate equipment , ensuring that agents receive appropriate training , ensuring appropriate management and supervision of all agents , setting limits and monitoring compliance and compensating agents for services rendered.[90] Financial institutions approved to conduct agent banking must enter into a written agreement with each agent before the agent conducts business on behalf of the financial institutions. [91]

An agent is prohibited from offering financial services on behalf of a financial institution without a valid agency agreement.[92] The contents of the agency are prescribed and include specifications of the scope of liability of any acts or omissions of the agent, services to be provided by the agent, activities the agent is prohibited from engaging in, remuneration arrangement, anti-money laundering and countering the financing of terrorism arrangements, transaction limits of the agent and exclusion of agent's employees from being treated as employees of the financial institution.[93]

Consumer protection safeguards are also provided for including putting in place adequate policies and procedures to address consumer protection , ensuring that agents conduct business in accordance with the consumer protection requirements applicable to financial institutions , transactions are effected in

88 Regulation 5 (1), Financial Institutions (Agent Banking) Regulations 2017.
89 Regulation 6 (2), Financial Institutions (Agent Banking) Regulations 2017.
90 Regulation 9 (2), Financial Institutions (Agent Banking) Regulations 2017.
91 Regulation 10 (1), Financial Institutions (Agent Banking) Regulations 2017.
92 Regulation 10 (3), Financial Institutions (Agent Banking) Regulations 2017.
93 Regulation 10 (3), Financial Institutions (Agent Banking) Regulations 2017.

real time , two factor authentication , generation of financial statements and display in a conspicuous place at premises of agent banking signage including parent branch , agent's unique identification number and a dedicated telephone line.[94]

Permissible activities by an agent include collection and forwarding of information and documents for account opening or applications for payment instruments, cash deposit and cash withdrawal, payment services including bill payments, money transfers, facilitating disbursements and repayment of loans, receipt and forwarding of documents in relation to loans and leases and any other permitted products, payment of retirement and social benefits and account balance inquiry.[95]

Prohibited activities by an agent include offering financial institution business on its own accord , conducting agency banking with a criminal record , conducting banking services not specifically permitted in the agency agreement , carrying out transactions when the system is down or in the customer's absence , carrying out transactions when the system generated receipt or acknowledgment of the transaction cannot be generated , charging fees directly to customers , undertaking cheque deposits or encashment of cheques , distributing cheque books , distributing debit cards or credit cards , conducting foreign exchange transactions , sub-contracting other persons to provide agency banking services , providing agency banking at a location other than the physical address of the agent , opening accounts and granting loans and being a guarantor to the financial institutions clients.[96]

94 Regulation 17(1) and (2), Financial Institutions (Agent Banking) Regulations 2017.
95 Regulation 14, Financial Institutions (Agent Banking) Regulations 2017.
96 Regulation 15, Financial Institutions (Agent Banking) Regulations 2017.

4.3 THE BANK OF UGANDA FINANCIAL CONSUMER PROTECTION GUIDELINES 2011

4.3.1 APPLICATION

The Guidelines apply to all financial services providers regulated by Bank of Uganda in respect of business they transact in Uganda and the agents of all financial services providers regulated by Bank of Uganda in respect of business the agent transacts in Uganda.[97]

4.3.2 OBJECTIVES

The objectives of the guidelines are to promote fair and equitable financial services practices by setting minimum standards for financial service providers in dealing with consumers, increase transparency in order to inform and empower consumers of financial services, foster confidence in the financial services sector and provide efficient and effective mechanisms for handling consumer complaints relating to the provision of financial products and services.[98]

4.3.3 KEY PRINCIPLES

The key principles governing the relationship between a financial services provider and a consumer are three and include fairness, reliability and transparency.

4.3.4 SCOPE OF FAIRNESS

Financial service providers are expected to act fairly and reasonably in all dealings with consumers. [99] However fairness is given multiple facets to further include provision of information and advice to a consumer,[100] suitability of advice,[101] prohibition of conditional sales,[102] explaining the nature and scope of

97 Guideline 2, Bank of Uganda Financial Consumer Protection Guidelines, 2011.
98 Guideline 4, Bank of Uganda Financial Consumer Protection Guidelines 2011.
99 Guideline 6 (1) (a), Bank of Uganda Financial Consumer Protection Guidelines 2011.
100 Guideline 6 (2), Bank of Uganda Financial Consumer Protection Guidelines 2011.
101 Guideline 6 (3), Bank of Uganda Financial Consumer Protection Guidelines 2011.
102 Guideline 6 (4), Bank of Uganda Financial Consumer Protection Guidelines 2011.

guarantorship,[103] providing a cooling off period,[104] provision of statements of deposit and loan accounts,[105] providing a 30 days' notice of changes to terms and conditions,[106] prohibition of claim of unreasonable costs and expenses[107] and prohibition of closure of account without giving a consumer 14 days' notice.[108]

4.3.5 SCOPE OF RELIABILITY

Financial service providers are supposed to update the consumers' data,[109] have reliable self-service banking channels,[110] safeguard consumer information and not disclose it to third parties,[111] protect consumers' accounts and provide relevant information to enable them safeguard their accounts[112] and ensure that staff are competent , well trained and are ably supervised.

4.3.6 SCOPE OF TRANSPARENCY

Financial service providers must ensure that any information that is given to a consumer is transparent[113], the contracts and other documentation relating to the financial products and services they provide are summarized in a key facts document written in plain language,[114] the terms and conditions provided highlight to a consumer the fees , charges , penalties , relevant interest rates and any other consumer liabilities,[115] disclose interest rates,[116] provide a consumer with a schedule of fees and charges for the product the consumer has chosen[117]

---

103 Guideline 6 (5), Bank of Uganda Financial Consumer Protection Guidelines 2011.
104 Guideline 6 (6), Bank of Uganda Financial Consumer Protection Guidelines 2011.
105 Guideline 6(7), Bank of Uganda Financial Consumer Protection Guidelines 2011.
106 Guideline 6(8), Bank of Uganda Financial Consumer Protection Guidelines 2011.
107 Guideline 6(9), Bank of Uganda Financial Consumer Protection Guidelines 2011.
108 Guideline 6(10), Bank of Uganda Financial Consumer Protection Guidelines 2011.
109 Guideline 7(1), Bank of Uganda Financial Consumer Protection Guidelines 2011.
110 Guideline 7(2), Bank of Uganda Financial Consumer Protection Guidelines 2011.
111 Guideline 7(3), Bank of Uganda Financial Consumer Protection Guidelines 2011.
112 Guideline 7(4), Bank of Uganda Financial Consumer Protection Guidelines 2011.
113 Guideline 8(1), Bank of Uganda Financial Consumer Protection Guidelines 2011.
114 Guideline 8(2), Bank of Uganda Financial Consumer Protection Guidelines 2011.
115 Guideline 8(3), Bank of Uganda Financial Consumer Protection Guidelines 2011.
116 Guideline 8(4), Bank of Uganda Financial Consumer Protection Guidelines 2011.
117 Guideline 8(5), Bank of Uganda Financial Consumer Protection Guidelines 2011.

and ensure that all advertising and promotional materials are fair , clear and not misleading.[118]

4.3.7 COMPLAINTS HANDLING MECHANISM

A financial services provider shall have in place and operate appropriate and effective complaint procedures,[119] inform consumers about the complaints-handling procedures,[120] investigate and determine complaints,[121] keep the complainant informed of the complaint-handling process,[122] go through the complaint-handling process within 2 weeks,[123] identify and remedy recurring systemic problems[124] and provide Bank of Uganda with a report of its receipt and handling of complaints every six months.[125]

5.0 RISKS INVOLVED IN DIGITAL BANKING

5.1 FRAUD

5.1.1 NATURE OF FRAUD

Fraud in digital banking occurs in various forms but some of the most common forms of fraud in digital banking include the following;

a. Authorized Push Payment fraud

Authorized Push Payment fraud is a form of fraud where a victim is induced by fraudulent means to authorize their bank to send a payment to a bank account controlled by a fraudster.[126]

118 Guideline 8(6), Bank of Uganda Financial Consumer Protection Guidelines 2011.
119 Guideline 9(2), Bank of Uganda Financial Consumer Protection Guidelines 2011.
120 Guideline 9(3), Bank of Uganda Financial Consumer Protection Guidelines 2011.
121 Guideline 9(4), Bank of Uganda Financial Consumer Protection Guidelines 2011.
122 Guideline 9(5), Bank of Uganda Financial Consumer Protection Guidelines 2011.
123 Guideline 9(6), Bank of Uganda Financial Consumer Protection Guidelines 2011.
124 Guideline 9(7), Bank of Uganda Financial Consumer Protection Guidelines 2011.
125 Guideline 9(8), Bank of Uganda Financial Consumer Protection Guidelines 2011.
126 Philipp v Barclays Bank UK PLC [2023] UKSC 25.

b. Pull Payment fraud

Pull Payment fraud is a form of fraud where payments are extracted from a victim's bank account or debited to a card by fraudster without the victim's authority.[127]

c. Business Email Compromise fraud

Business Email Compromise is a form of fraud in which a cyber-criminal compromises email correspondences between by altering the contents of those emails to their advantage without the knowledge of the parties to achieve a fraudulent or criminal objective.[128]

5.2 CYBER ATTACKS

Cyber-attacks in digital banking mainly take the broad form of account take over and automatic transfer systems. Financial Institutions' cyber security departments should be aware of the different types of attacks that these two categories include to manage risk in their systems and set up appropriate security measures to prevent threats.[129]

5.2.1 ACCOUNT TAKE OVER

Account Take Overs happen when cyber criminals acquire account details of a legitimate user and then use the account as their own. Account Take Over often begins with compromised credentials that have been stolen or obtained through trickery.[130] In *Atiku v Centenary Rural Development Bank Limited*[131], someone was able to access the plaintiff's phone and mobile banking password and withdrew funds from her bank account using the mobile banking application on her phone.

---

127 Ibid.
128 Hawarden v Edward Nathan Sonnensberg Inc [2023] ZAGPJHC 14.
129 "Online banking fraud: what it is and how to prevent it" available at <www.cleafy.com> [Accessed 8 October 2023]
130 Atiku v Centenary Rural Development Bank Limited [2022] UGCommc 146.
131 [2022] UGCommc 146.

Phishing, smishing, vishing and hacking are the most common examples of Account Take Over attacks. Cyber criminals can spread infectious malware on the victim's device via clickable links contained in an email[132] or an SMS[133] that look genuine. Once the malware is downloaded and installed, it gains complete access to the victim's device, giving the cyber criminals the opportunity to perform Account Take Overs. Cyber criminals can also trick victims directly via voice calls[134] and convince them to perform a straightforward illegal activity without the need to spread any malware.[135] This is what cyber criminals did to Mr. and Mrs. Philipp in *Philipp v Barclays Bank UK PLC*[136] when they convinced them to transfer money from their bank account to another account by convincing them over the phone that they are police officers and that their money is not safe on their bank account.

5.2.2 AUTOMATIC TRANSFER SYSTEMS

Attacks through Automatic Transfer Systems do not require taking over the victim's account. The attack happens while the victim actively operates on the target account by tampering with the account without the victim noticing it.[137]
In *Hawarden, v Edward Nathan Sonnensberg Inc* [138] cyber criminals hacked into the email correspondence between the Plaintiff and Defendant and altered the account number provided by the Defendant to the Plaintiff without the Plaintiff and Defendant noticing causing the Plaintiff to transfer funds to an account belonging to the cyber criminals.

132 Known as phishing.
133 Known as smishing.
134 Known as vishing.
135 Supra (no.6).
136 [2023] UKSC 25.
137 Supra (no.6).
138 [2023] ZAGPJHC 14.

6.0 MITIGATION OF RISKS INVOLVED

6.1 CYBER SECURITY PROTOCOLS

Financial institutions offering digital banking are obliged to provide secure mechanisms for their customers to conduct their banking safely. As such, they have a duty to put in place robust fraud detection solutions to protect their systems and customers. These solutions include cyber security protocols[139], which ensure that digital banking systems are secure and should be regularly reviewed for that purpose.[140]

6.2 SECURE TECHNOLOGY INFRASTRUCTURE

Financial institutions have a duty to take reasonable measures to ensure that their digital banking systems and technology are secure and are regularly reviewed and updated for this purpose. Their systems should be able to detect suspicious transaction or withdraws when they take place. The systems should equally ensure that digital banking transactions can be traced and checked as long as they are received by the system.[141]

6.3 CUSTOMER SENSITIZATION AND SUPPORT

For security measures to be effective, financial institutions should provide the customer with regularly updated information on how to access digital banking services, including details about their customer ID, selection of appropriate passwords and the availability of additional authentication or security options, how to maintain their security and what their liability for unauthorized transactions will be.

---

139 Cyber security protocols are cyber security measures put in place to ensure that systems are safe and secure from cyber-attacks. These may include password encryption, setting up of firewalls, routine password resets and routine cyber-attack drills or manoeuvres.

140 Atiku v Centenary Rural Development Bank Limited [2022] UGCommc 146.

141 Ibid.

7.0 FEASIBILITY OF BEYOND THE BANKING HALL STRATEGY

7.1 PROS OF DIGITAL BANKING

7.1.1 COST EFFECTIVE

The cost of opening up and running a physical branch of a bank is so high as opposed to setting up and operating a digital platform to offer digital banking services to customers. The Independent quoted banking officials, who had this to say regarding the cost effectiveness of digital banking;

> *"Indeed, Sentongo (the head of digital banking at Stanbic Uganda) said if Arinaitwe and others can transact using digital tools, there is no need of opening branches everywhere because they are expensive. It costs approximately 2 million US Dollars to put up a fully-fledged commercial bank branch. Investing in centralized IT systems that would ably handle transactions without face-to-face meetings between customers and the bank, would make a good investment."* [142]

7.1.2 FINANCIAL INCLUSIVENESS

Digital banking has disrupted the financial services in Uganda enabling millions of poor people to access banking services, providing them with a digital financial footprint. [143] Many of these poor people, would not have been able to access conventional banking services due to a number of barriers like; illiteracy, poverty and lack of physical access to banks.

7.1.3 CONVENIENCE TO CUSTOMERS

Digital banking enables banks to effectively serve customers and at their convenience. This is because, the banks are able to reach out to the customers easily and faster as opposed to the customers reaching out to the banks. This is

---

142 The Independent (2017), "Digital banking: Why it is good for business and jobs" available at <https://www.independent.co.ug/digital-banking-good-business-jobs/> [Accessed 4 February 2024]

143 Daily Monitor (2021), "Digital banking necessary for financial inclusiveness" available at <https://www.monitor.co.ug/uganda/business/prosper/digital-banking-necessary-for-financial-inclusiveness-1686112> [Accessed 5 February 2024]

the case when customers have to physically approach the banking hall at a physical branch of the bank. In an interview with The Independent on 20th February 2017, Mr. William Sekabembe, the then Chief of Business and Executive Director of DFCU Bank Uganda Limited had this to say on the bank's strategy on digital banking;

"We are investing heavily in technology so we can serve our customers without necessarily opening new branches in all parts of the country". [144]

7.2 CONS OF DIGITAL BANKING

7.2.1 SUSCEPTIBLE TO FRAUD

Digital banking is not without risks of fraud. As digital banking channels have multiplied, so have the routes that fraudsters can use. With increased automation, financial institutions have become some of the most targeted by fraudsters, due to their immediate access to funds and their ability to transfer them.[145]

7.2.2 DIFFICULTY TO ADAPT TO DIGITAL BANKING

Some bank customers, especially those of old age, have had a difficulty in adapting to digital banking, due to its heavy reliance on technology. Mubiru J in *Atiku v Centenary Rural Development Bank*[146] noted as follows, "Senior citizens believe that mobile phones are for talking and not conducting banking transactions." This demographic is the most bankable, as compared to that of the youth, who best appreciate digital banking due to their being well vast with technology; yet it is not well vast with technology, thus finds it difficult to adopt and embrace digital banking.

---

144 The Independent (2017), "Digital banking: Why it is good for business and jobs" available at <https://www.independent.co.ug/digital-banking-good-business-jobs/> (Accessed 4 February 2024).

145 Atiku v Centenary Rural Development Bank Limited [2022] UGCommC 146.

146 [2022] UGCommC 146.

7.2.3 TECHNOLOGICAL HURDLES

The use of digital baking services is faced with a number of technological hurdles. These include lack of technical knowledge, poor technology infrastructure, lack of gadgets and poor internet penetration. These affect the adoption of digital banking by bank customers hence greatly impacting the banks digital banking strategy.

7.3 WEIGHING THE PROS AND CONS

Weighing the pros and cons of digital banking, depends on which side of the spectrum you are on. From a banks point of view, the pros of digital banking which include; cost effectiveness, financial inclusiveness and customer convenience far outweigh the cons. This is so, even when digital fraud has proved to be a very big setback to the banks profit margin, as banks have been made to pay heavy damages to customers that are victims of digital fraud in a number of cases.[147]

From a customer's vantage point, the cons of digital banking which include; fraud, adaptation challenges and technological hurdles far outweigh the pros. This is so, even when customers benefit greatly from the convenience that digital banking offers. There is thus a need for banks to balance their needs and those of their customers in order to be in position to better serve their customers. For example, banks should not completely go digital and only offer digital banking. They should be in position to maintain the physical banking component alongside digital banking. This will enable customers that have challenges with digital banking services to continue accessing banking services. Banks should equally have continuous sensitization and training sessions on digital banking to help customers best adapt to digital banking.

147 Philipp v Barclays Bank UK PLC [2023] UKSC 25 and Barclays Bank v Tamima Ibrahim Civil Appeal Number E075 of 2021

8.0 CONCLUSION

The nature of digital banking and its confluence with technology makes it very necessary in today's modern day and age. It's adaption by financial institutions and their customers is inevitable. Indeed, all financial institutions in Uganda and their customers have either wholly, or partly adopted digital banking for ease of business and service delivery. The principles governing digital banking are very unconventional as they are a mix of principles governing technology and law. This makes digital banking very technical and complicates its appreciation and regulation. It is, however, helpful that digital banking does not depart a lot from conventional banking. Some of the principles governing it are, relatable to those of conventional banking. Case in point, is the banker customer consumer relationship in digital banking that is relatable to the banker customer relationship in conventional banking.

Many jurisdictions, including Uganda, have enacted laws to regulate how digital banking is conducted. Uganda's laws provide clear regulation of digital banking in addition to providing consumer protection. Amendments to the law to respond to technological changes will go along-way in improving regulation of digital banking. With the benefits that accrue to digital banking comes the challenges. This, however, does not take away the said benefits as they far much outweigh the challenges. Financial institutions ought to take steps to ensure the safety of digital banking for their consumers. This includes investing in technological infrastructure, technical capacity building and sensitization of the general public about the risks involved in digital banking.

Digital banking has come to stay as the advancements in technology and the growth of the banking industry do not permit the return to the old banking days and ways; of banking in the banking hall, at the counter and at a bank branch. Banking today ought and I nay say must be done beyond the banking halls, at the convenience of the bank's customer or else banks will not be having any customers. This is much cheaper for the banks as it reduces on operations costs

like paying salaries to employees, renting bank premises and purchasing stationery. It is much convenient for the bank customer as they are able to access banking services 24 hours a day as opposed to the 9am to 5pm banking hours at a bank branch and at their convenience, wherever they are as opposed to travelling to the bank branch carry out a transaction.

LIST OF REFERENCES

Alice Ivey (2023), "A brief history of digital banking" available at <https://cointelegraph.com/news/a-brief-history-of-digital-banking > (accessed 14 December 2023).

Atiku v Centenary Rural Development Bank Limited [2022] UGCommc 146.

Augustine Idoot Obilil, "An Overview of the National Payment Systems Act 2020" available at <www.kaa.co.ug/an-overview-of-the-national-payment-systems-act-2020/ > (accessed on 21 October 2023).

Bank of Uganda Financial Consumer Protection Guidelines 2011.

Barclays Bank PLC v Quincecare Limited [1992] 4 ALLER 363.

Barclays Bank v Tamima Ibrahim Civil Appeal No. E075 of 2021.

Daily Monitor (2021), "Digital banking necessary for financial inclusiveness" available at <https://www.monitor.co.ug/uganda/business/prosper/digital-banking-necessary-for-financial-inclusiveness-1686112> (accessed 5 February 2024).

Financial Institutions (Agent Banking) Regulations 2017

Financial Institutions Act 2004

Ham Enterprises Limited and 2 others v Diamond Trust Bank (U) Limited and Another [2023] UGSC 15

Hawarden v Edward Nathan Sonnenbergs Inc [2023] ZAGPJHC 14.

National Payment Systems Act 2020.

"Online banking fraud: what it is and how to prevent it" available at <www.cleafy.com> [Accessed 8 October 2023]

Philipp v Barclays Bank UK PLC [2023] UKSC 25.

The Independent (2017), "Digital banking: Why it is good for business and jobs" available at <https://www.independent.co.ug/digital-banking-good-business-jobs/> [Accessed 4 February 2024).