ANALYZING THE INFLUENCE OF DATA PROTECTION AND PRIVACY STRATEGIES ON CYBERSECURITY EFFECTIVENESS IN THE BANKING SECTOR

FAHAD SSEBUGUZI

B20B11/1062

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

May, 2024

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I, SSEBUGUZI FAHAD declare that this dissertation is of my original work, It has not been presented for any academic award in any institution of higher learning here or elsewhere for examination and it has not been generated by any generative Ai.

SSEBUGUZI FAHAD

Signature…… Date…./…./….

ABSTRACT.

Data protection and privacy is a fundamental component in the fulfillment of a right to privacy. Sadly, the goal of ensuring that the right to privacy is administered and structured in banks and equipping people with the knowledge and resources to address their right has remained elusive. Therefore, this study is aimed at analyzing the influence of data protection and privacy strategies on cyber security effectiveness in the banking sector. In particular, the study sought to; determine the data protection and privacy strategies that have been employed by various banks, the legal and regulatory framework governing data protection and privacy in banks and how these strategies influence cyber security effectiveness in banks.

The study concludes that Data protection and privacy strategies used by banks influence cyber security effectiveness. This is because the strategies are seen as the first line of defense in ensuring cyber security in banks. Once they are effectively implemented, there will be less or no cyber security incidents in the banking sector.

The study also recommends that there also need to have a Data protection regulatory body of specifically banks and other financial institutions that monitors and regulators how data protection and privacy policies are administered by banks. This is because banks deal with a lot of data collected from various bank customers and those that access financial services from banks.

DEDICATION

I dedicate this dissertation to the Almighty Allah who has given me the gift of life. I also dedicate it to my parents Mr. KISEKKA MUHAMMAD and Ms. NAMANYANJA SARAH, brothers, sisters and my entire family who have always been there for me throughout my academic life. I am proud to have a strong and supportive family. Thank you for the support.

For God And My Country.

APPROVAL

This dissertation has been under my supervision and is now ready for submission to Uganda Christian University

Signature……. Date…/…./….

Mr. JOEL BASOGA

(Supervisor)

ACKNOWLEDGEMENTS

This dissertation would not have been a success without the assistance of my academic supervisor MR. JOEL BASOGA for his good research skills and guidance in this research work, thank you for your constructive criticisms and guidance. I want to express my sincere gratitude to him for all that he has done for me. I am deeply indebted. His motivation, friendly treatment, encouragements and her research skills gave me impetus to complete this dissertation during challenging periods.

I am also grateful to the various authors for their works be without their effort, this research dissertation would have been hard to accomplish.

I also thank my supportive family for their patience, compassion, and guidance. I would not have been what I am now without having such an incredible family support and encouragement to be a better person I am forever grateful for your love. Moreover, I will never forget to thank my true friends who have been there for helping me along the way till this dissertation was finally done.

My heartfelt gratitude goes to my family for their moral and financial support. I will never forget all the comfort they gave me especially when the going got tough. Without them, I would never have finished this dissertation.

Lastly am thankful to my brothers and my sisters my friends; and those who directly and indirectly rendered me their assistance. May Allah bless you all.

Contents

CHAPTER ONE

Introduction

In today's globally connected digital landscape, the banking sector faces multiple challenges related to cybersecurity. As financial institutions are now increasingly relying on technology for their operations, safeguarding data and ensuring privacy have become critical imperatives.[1] The intersection of data protection, privacy strategies, and cybersecurity effectiveness is an round area that demands careful investigation.

The banking sector is one of the most crucial sectors in the modern economy[2]. It handles large amounts of financial transactions, personal data, and confidential information. The protection and privacy of these data and information are essential for ensuring the trust and confidence of customers, stakeholders, regulators, and the society at large. Nevertheless, the banking sector also faces various challenges and threats in the digital era, such as cyber attacks[3], data breaches[4], identity theft, fraud, and compliance issues. These challenges and threats affect the protection and privacy of the data and information, causes significant financial, and legal damages to the banks and their customers.

To get through with these challenges and threats[5], the banking sector needs to adopt and implement effective data protection and privacy strategies such as encryption, authentication, access control, audit, and consent. These strategies aim to protect the data and information from

---

[1]McKinsey Digital; Safeguarding against attack in an increasingly digital world. Accessed on 22nd April 2024 (Boehm, 2020)https://www.mckinsey.com/capabilities/mickinsey-digital/our-insights/safeguard-against-cyberattack-in-an-increasingly-digital-world

[2] "Exclusive: Largest & Smallest Banks By Assets Named As Total Industry Assets Hit Shs45.4Tn In 2022" by Taddewo William Senyonyi https://businessfocus.co.ug/exclusive-largest-smallest-banks-by-assets-named-as-total-industry-assets-hit-shs45-4tn-in-2022/#:~:text=Uganda's%20banking%20industry%20total%20assets,based%20on%20their%20financial%20statements accessed on 22nd April 2024.

[3]"cybersecurity is number one risk for global banks, but geopolitical risk tops European banks' concern," press release by Sarah Graham accessed on 22nd April 2024 https://www.ey.com/en_gl/news/2023/01/cybersecurity-is-number-one-risk-for-global-banks-but-geopolitical-risk-tops-european-banks-concerns

[4] For example the scandal between stanbic bank and Pegasus where over shs 10 billion was stolen by hackers https://eagle-co-ug.cdn.ampproject.org/v/s/eagle.co.ug/2020/12/11/stanbic-bank-employee-arrested-over-recent-shs10-billion-electronic-scam/?amp=&amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=From%20%251%24s&aoh=17138640911327&csi=1&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Feagle.co.ug%2F2020%2F12%2F11%2Fstanbic-bank-employee-arrested-over-recent-shs10-billion-electronic-scam%2F accessed on 22nd April 2024

[5] Challenges like cyberattacks, data breaches, identity theft and compliance issues.

unauthorized access, use, disclosure, modification, or destruction and to respect the rights and preferences of the data subjects as in accordance with the existing laws. However, the data protection and privacy strategies we to look at are not on majorly legal and organizational aspects. They need to be aligned with the relevant laws, regulations, standards, and best practices, as well as the expectations and needs of the data subjects and other stakeholders.

Moreover, data protection and privacy strategies are not independent from cyber security, but rather interrelated and interdependent. Cyber security aims to protect the data and information, as well as the systems, networks, and devices that process, store, and transmit them, from cyberattacks and incidents. Cyber security involves prevention, detection, response, and recovery measures, such as risk assessment, threat intelligence, incident management and recovery planning. Data protection and privacy strategies can support and enhance cyber security by reducing the exposure and impact of cyberattacks and incidents and by increasing trust and cooperation among the stakeholders. Nevertheless, data protection and privacy strategies can also pose challenges and risks for cyber security such as increasing the complexity and cost of security systems, creating conflicts with legal and regulatory requirements and exposing weaknesses to cyberattacks.

Therefore, it is important to understand how data protection and privacy strategies influence cyber security effectiveness in the banking sector, and what are the best practices can enhance both aspects. This is the main research topic of this dissertation, and aims to provide a comprehensive and comparative analysis of the impact of data protection and privacy strategies on cyber security effectiveness in the banking sector, and to propose recommendations and strategies for improving them.

Problem Statement.

The banking industry in Uganda struggles with a threat of cyber-attacks, data breaches and privacy violations[6]. While data protection and privacy strategies are key components of risk management, their impact on overall cybersecurity effectiveness remains a subject of question.

[6] "Ugandan banks lost over $4 millio to hackers in the past one year" report released by Interpol Uganda https://www.theeastafrican.co.ke/tea/business/hackers-skim-4m-off-banks-in-uganda-359339 accessed on 22nd April 2024

This research aims to explore the influence of data protection and privacy strategies on the security posture of banks.

Research questions

1. What is the legal regime of data protection and privacy for banks?
2. What are the legal obligations of banks under the current data protection and privacy legal framework?
3. How do data protection and privacy strategies affect cyber security effectiveness in the banking sector?
4. What are the main data protection and privacy strategies adopted by banks in Uganda?
5. What are the main challenges and opportunities for integrating data protection and privacy strategies with cyber security strategies in the banking sector?

Significance of the study

This thesis will contribute to the existing literature and knowledge on the relationship between data protection, privacy, and cyber security in the banking sector. It will address a timely and relevant issue for the banking sector and the society, as data protection, privacy, and cyber security are increasingly becoming strategic and competitive factors for the banks, as well as essential rights and values for the customers and the public. Fourth, it will benefit the banking industry and the policy makers, by offering practical guidance and solutions for improving data protection, privacy, and cyber security in the banking sector, and by suggesting areas for further research and innovation.

Objectives of the study

- The main objective of this study is to analyze the impact of data protection and privacy strategies on cyber security effectiveness in the banking sector, and to provide recommendations and strategies for improving them.

The specific objectives are:

- To assess the legal frameworks for data protection and privacy in the banking sector.

- To examine the data protection and privacy strategies adopted by banks in Uganda and contexts, and evaluate their strengths, weaknesses, opportunities, and threats.
- To propose and justify recommendations and strategies for enhancing data protection and privacy strategies and cyber security effectiveness in the banking sector, based on the empirical findings and the literature review.

Hypothesis.

There is an urgent need to sector specific data privacy regulations for banks in Uganda. Data protection and privacy strategies have a significant influence on the cyber security effectiveness in the banking sector. Their implementation strongly affects the exposure banks to data breach and cyber security incidents.

Limitations of the study

First, the study will focus on the banking sector, which may be limited by time and confidentiality. Second, the study will rely on secondary data and sources, such as official documents, reports, publications, and statistics, which may not be accurate, up-to-date. Third, the study will face some practical and ethical challenges, such as access to information and confidentiality.

Scope of the study.

This research will be carried out in Uganda from January 2024-May 2024.

The subject scope for this research topic is the intersection of data protection, privacy, and cyber security in the banking sector. It covers the following subjects:

The legal and regulatory frameworks and standards for data protection, privacy, and cyber security in Uganda and their implications for the banking sector

The data protection and privacy strategies and practices adopted by banks in Uganda and contexts, such as encryption, authentication, access control, audit, and consent.

Definition of key terms.

Data is defined by the Data Protection and Privacy act[7] as information which is processed by means of equipment operating automatically in response to instructions given for that purpose; is recorded with the intention that it should be processed by means of such equipment; is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or forms part of an accessible record.

Data privacy, sometimes also referred to as information privacy, is an area of data protection that concerns the proper handling of sensitive data including, notably, *personal data* but also other confidential data, such as certain financial data and intellectual property data, to meet regulatory requirements as well as protecting the confidentiality and immutability of the data.[8]

Literature review.

The banking sector operates in a dynamic environment where technological advancements and digitalization have revolutionized financial services[9]. However, this progress comes with inherent risks, particularly in the realm of cybersecurity. Protecting sensitive customer data, maintaining privacy, and ensuring robust security measures are critical imperatives for financial institutions. This literature review explores existing research, case law, and scholarly writings to understand the intricate relationship between data protection, privacy strategies, and cybersecurity effectiveness in the banking industry.

Nasser Konde in his article, "Banking Beyond the Banking Hall"[10] reviews the state of Digital banking in Uganda from its genesis up. He highlights the existing legal framework of Digital banking in Uganda, the feasibility of digital banking and also the existing risks and challenges that Digital banking presents in the Banking sector of Uganda. He opines that the principles governing digital banking are very unconventional as they are a mix of principles governing technology law. He expresses that digital banking should depart from conventional banking for example the banker customer relationship in digital banks is relatable to the banker customer

---

[7] Section 2 of the Data Protection and Privacy Act, 2019

[8] Arletta Gorecka, *Competition law and privacy: extensive data acquisition as the "eye" of the problem*, Network Law Review, Winter 2023

[9] IMF Working Paper (WP/21/46), "Stay competitive in the Digital Age: The Future of Banks" https://www.imf.org/-/media/files/publication/WP/2021/English/wpiea2021046-print-pdf.ashx

[10] Nasser Konde (2024); "Banking Beyond the Banking Hall: AReview of Digital Banking in Uganda." Volume 53 Issue 4 Makerere Law Journal pp. 116-149

consumer relationship in conventional banking. The article also asserts that even though Uganda has enacted laws to regulate how digital banking is conducted, it does not take away the fact that financial institutions ought to take steps to ensure the safety of digital banking for their consumers.

In as much as the article brings out the legal framework that has been put in place to protect digital banking consumers, how to mitigate the risks involved in digital banking, it does not address the need for financial institutions and central bank to put up data privacy and data protection strategies and how they can influence cyber security effectiveness in the bank sector and that is what my research will look at.

According Racheal Nabisubi in her article, "Banks brace themselves for data protection concern."[11] The article highlights the fact that banks collect and process personal data for various reasons. The article notes that personal information collected by banks has a possibility that it can be shared to third parties with the consent of bank customers. The article highlights how financial institutions in Uganda are handling the issue of data protection and privacy concerns that they are faced with by setting up regulatory guidelines for data privacy policies. The article provides quotes from different stake holders in different financial institutions in Uganda, where they discuss the concern of data protection in banks, the existing regulatory frame on data protection in banks, the risks involved when unlawful persons access this data, and the infrastructure that has been put in place to protect bank customers' personal data. The article also discusses that banks must be duly registered with the Personal Data Protection Office.

However the article only provides a brief overview of the topic and lacks in-depth analysis, it does not address the concerns of data protection and privacy in banks. The article also only based on industrial reports and expert opinions, lacking empirical research and data analysis. I intend to use the article's limitations to justify the need for further research and in-depth analysis on the influence of data protection and data privacy strategies on cybersecurity effectiveness in the banking sector.

[11] Racheal Nabisubi; "Banks brace themselves for data protection concerns," by prosper Magazine (Monitor.co.ug) https://www.monitor.co.ug/uganda/business/prosper/banks-themselves-for-data-protection-concerns-3717764 accessed on 22nd April 2024.

Patricia Akankwatsa in her article, "Banks strive to counter cyber threats,"[12] notes the discussions that were held at the Annual Bankers Conference 2023 were the industry's leaders, experts and stakeholders. The article discusses the fact that there has been a significant increase in the number of entrants in the financial ecosystem and the emergency of digital finance[13]. The article discusses fact that there a numerous benefits[14] , the innovations have come with associated risks, especially cyber risks that the financial institutions are aware of and are constantly developing strategies to mitigate against them.

However the article overemphasizes on the technological aspects of innovations and fintech institutions, neglecting the importance of data protection and privacy strategies in ensuring cyber security effectiveness in the banking sector. The article also does not pay much attention to cyber security risks as it only talks about the risk but does not provide how banks can solve these risks that are associated with the technological advancements in the banking sector. This research will investigate and compare the regulatory frameworks governing data protection and privacy in Uganda and highlight the best practices and areas of improvement.

The concept of privacy by design advocates integrating privacy considerations into the design and development of systems and processes. Banks that adopt privacy by design principles demonstrate a proactive approach to safeguarding customer information. Research by Cavoukian and Jonas[15] highlights the effectiveness of embedding privacy controls from the outset, reducing vulnerabilities and enhancing overall cybersecurity.

Research by Kshetri[16] indicates that data protection and privacy strategies significantly impact cybersecurity effectiveness. Banks that prioritize data protection demonstrate better resilience against cyber threats. Privacy-enhancing technologies, such as homomorphic encryption and anonymization, contribute to overall security. However, challenges persist in balancing privacy rights with effective security measures.

---

[12] Patricia Akankwatsa; "Banks strive to counter cyber threats." By Independent.co.ug : https://www.indepedent.co.ug/banks-strive-to-counter-cyber-threats/

[13] Bank of Uganda Annual report (2021-2022) provided that the Bank of Uganda has issued licenses to 25 fintech as payment system providers and payment system operators

[14] Increase in innovations and fintech institutions

[15] Cavoukian, A. and Jonas, J. (2012) Privacy by Design in the Age of Big Data. Eurocontrol Int, 1-17

[16] **Kshetri, N.**: "The Privacy-Enhancing Technologies Landscape: A Critical Review" (2019).

This literature review underscores the critical role of data protection and privacy strategies in bolstering cybersecurity effectiveness within the banking sector. By analyzing case law, scholarly writings, and regulatory frameworks, we gain insights into best practices, challenges, and areas for improvement. As financial institutions continue their digital transformation, a holistic approach that harmonizes data protection, privacy, and security remains paramount.

CHAPTER SYNOPSIS

CHAPTER 1; this chapter will cover the Introduction of the problem, statement of the problem, Objectives of the study, research questions, the methods as well as the scope of the study.

CHAPTER 2; This chapter state the laws and regulations that I will analyze.

CHAPTER 3; This chapter will analyze the approach banks have taken in data protection and I will also look at data security incidents that have occurred.

CHAPTER 4; The chapter will make summaries, conclusions and recommendations on the best way forward upon. I undertake to make practical recommendations for addressing the problem identified in my research

CHAPTER TWO ; THE LEGAL FRAMEWORK ON DATA PROTECTION IN THE BANKING SECTOR.

2.1; Introduction

In an era where information is a critical asset, the protection of data has become a cornerstone of business integrity and trust, especially in the banking sector. The advances in digital technologies transformed the way banks operate, leading to increased efficiency and better customer service. However, this digital transformation also brings significant risks related to cyber security and privacy concerns. In Uganda, the legal system has been evolving to address these challenges, ensuring that financial institutions can safeguard their operations against cyber threats while respecting the privacy rights of individuals.

The legal framework in Uganda, comprising the constitution of the Republic of Uganda, the Financial Institutions Act 2004, the Data Protection and Privacy Act 2019, the Computer Misuse Act, the Electronic Signatures Act 2011, the Electronic Transactions act 2011 and other laws that provide an approach to managing these risks. These laws not only reflect Uganda's commitment to protecting the interests of consumers and maintaining the stability of the financial system but also align with global trends and standards in data protection and cyber security.

Legal regime on Data Protection.

The 1995 Constitution of the Republic of Uganda.

Article 27 provides for a person’s right to privacy and article 27(2) provides that;” No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.” This establishes protection of people’s private data in Uganda.

The parliament shall have power to make laws on any matter for the peace, order, development and good governance of Uganda.[17] Through this the parliament has come up with laws regulate data protection in Uganda. And they include the following;

The Data Protection and Privacy act of 2019 (DPPA).

Uganda's Data Protection and Privacy Act 2019 seeks to protect Uganda's citizens and their personal data by outlining and implementing rules for processing personal data and sensitive personal data by entities within or outside the country. Uganda's data protection law further bestows rights upon individuals, allowing them to control how their data is collected and processed. The Data Protection and Privacy Act 2019 applies to both public and private entities[18].

Objectives of the Act

An Act to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters.

Application of the Act

This Act applies to a person, institution or public body; (a) collecting, processing, holding or using personal data within Uganda; (b) outside Uganda who collects, processes, holds, or uses personal data relating to Ugandan citizens [19]. Since Banks collect personal data from its customers this act applies to them.

Data collection principles.

The Data protection and privacy act provides for the principle of data collection that every person collecting data[20] must adhere to and they include; (a) be accountable to the data subject for data collected, processed held or used; (b) collect and process data fairly and lawfully; (c) collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data; (d) retain personal data for the period authorised by law or for which the data is required; (e)

[17] Article 79(1) of the constitution of Uganda
[18] Data protection and prvacy Act (2019) – Uganda accessed on 23rd April 2024 https://www.ardentprivacy.ai/data-privacy-uganda/
[19] Section 1 of the Data Protection and Privacy Act, 2019
[20] Including banks

ensure quality of information collected, processed, used or held; (f) ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and (g) observe security safeguards in respect of the data[21]. Since banks collect personal data from their customers, they need to abide by these principles in formulation of their policies.

Rights of Data Subjects;

The act enshrines the rights of individuals to have their data protected, including the right to (a) correct or delete personal data about the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or (b) destroy or delete a record of personal data about the data subject held by the data controller which the controller no longer has the authority to retain.[22] The data subjects for banks since banks collect data from them, these rights apply to customers.

Obligation of data controllers and Processors.

Banks as data collectors since they collect data from their clients and this data is stored and used by them, they have specific obligations regarding the handling of personal data including adopting appropriate, reasonable, technical and organizational measures to prevent loss, damage, or unauthorized destruction and unlawful access to or unauthorized processing of the personal data[23]

Processing personal data outside Uganda[24]

Where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that;(a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this Act; or (b) the data subject has consented.[25] Since some banks are international banks and they sometimes store and process information outside Uganda they must abide with this provision.

---

[21] Section 3 of the Data Protection and Privacy Act, 2019
[22] Section 16 of the Data Protection and Privacy Act, 2019
[23] Section 20 of the Data Protection and Privacy Act, 2019
[24] Section 19 of the Data Protection and Privacy Act, 2019

[25] Ibid

The National Information Technology act 2009

The act provides for the establishment of the National Information Authority and the objects of act include, " to promote standardization in the planning, acquisition, implementation, delivery, support and maintenance of information technology equipment and services, to ensure uniformity in quality, adequacy and reliability of information technology usage throughout Uganda,"[26] and its functions which include "to identify and advise Government on all matters of information technology development, utilization, usability, accessibility and deployment including networking, systems development, information technology security, training and support."[27]

The Access to Information Act, 2005

This Act provides for the right of access to information pursuant to Article 41 of the Constitution, which is essential for transparency and accountability in the banking sector.[28]

The Computer Misuse Act, 2011 (as amended).

This Act makes provisions for the safety and security of electronic transactions and information systems, preventing unauthorized access[29], offence on abuse or misuse of information systems including computers and provides for the protection of personal data.

The Registration of Persons Act, 2015

This Act provides for the mandatory registration of all persons in Uganda[30], the issuance of national identification numbers and cards, and the establishment of a national identification register, which can be relevant for customer identification processes in banks.

The Electronic Signatures Act, 2011

The Electronic Signatures Act, 2011 of Uganda is highly important for online banking transactions because it provides the legal basis for the use and recognition of electronic signatures, which are essential for the authentication of electronic records and transactions in the digital banking environment.

---

[26] Section 4 of the National Information Technology Act, 2009
[27] Section 5 of the National Information Technology Act, 2009
[28] Section 3 of the Access to information Act, 2005
[29] Section 17 of the computer misuse act 2011
[30] Section 54 of the Registrations of Persons Act 2015

Section 3 provides of legal recognition[31] and the Act gives electronic signatures the same legal status as handwritten signatures, ensuring that transactions conducted electronically are legally binding.

Part IV of the Act provides for security and It establishes a public key infrastructure for the authenticity and security of documents[32], which is crucial for the integrity of online banking transactions.

Section 18 provides for authentication and recognizes different signature-creating technologies[33], allowing banks to use various methods for verifying customer identities during online transactions.

Section 8 provides for trust, by providing for the regulation and use of electronic signatures, the Act helps in building trust in electronic banking systems, as customers can be assured that their transactions are secure and their data is protected[34].

Section 4 provides for compliance[35]; Banks are required to comply with the provisions of the Act, which includes using certified and secure methods for creating and verifying electronic signatures, thereby enhancing the overall cyber security posture of the banking sector.

The Electronic Transactions Act, 2011

This Act provides for the use, security, facilitation, and legal recognition of electronic transactions and documents which is crucial for the digital operations of banks

Section 5 provides for legal recognition of Electronic Transactions. The Act gives legal recognition to electronic records and signatures, ensuring that transactions conducted electronically are as legally valid as those done through traditional means[36]

Section 4 provides for security and facilitation: It aims to enable and facilitate secure electronic communication and transactions[37] which is essential for the credibility and reliability of online banking services.

---

[31] Section 3 of the electronic signatures act, 2011
[32] Part IV of the electronic signatures act, 2011
[33] Section 18 of the electronic signatures act, 2011
[34] Section 8 of the electronic signatures act, 2011
[35] Section 4 of the electronic signatures act, 2011
[36] Section 5 of the electronic transactions act, 2011

Section 4 also provides for technology neutrality. By promoting technology neutrality[38], the Act allows banks to use various forms of technology for electronic transactions without being constrained by legislation that favors one technology over another.

Section 4 further provides for legal certainty and public confidence[39]. The Act provides legal certainty for electronic transactions, which helps to build public confidence in the use of electronic banking services.

Section 4 also provides for E-Government services[40]. It encourages the use of e-Government services, which can include electronic payments and other interactions between banks and government entities.

Section 4 provides for international standards[41]. sThe Act ensures that electronic transactions in Uganda conform to the best practices by international standards, which is important for banks that operate globally or have international clients

Consumer Protection[42]: It develops a safe, secure, and effective environment for consumers, which is vital for protecting customer information and transactions in the digital space.

The legal regime governing financial institutions.

Financial institutions in Uganda are regulated by the financial institutions act of 2004.

The act repealed the Financial Institutions Act cap 54. The act sets out the licensing requirements, capital adequacy, corporate governance, supervisory framework within which banks must operate.

Licensing requirements;

A person shall not transact any deposit-taking or other financial institution business in Uganda without a valid license granted for that purpose under this Act.[43] A company proposing to

---

[37] Section 4(1)a of the electronic transaction Act, 2011
[38] Section 4(1)c of the electronic transaction Act, 2011
[39] Section 4(1)d of the electronic transaction Act, 2011
[40] Section 4(1)e of the electronic transaction Act, 2011
[41] Section 4(1)f of the electronic transaction Act, 2011
[42] Part IV of the electronic transaction Act, 2011
[43] Section 4(1) of the financial institutions Act 2004

transact or carry on business as a financial institution shall apply, in writing, to the Central Bank for a license.[44] This is legal definition of a bank.

Corporate governance.

The Act requires the board of directors to oversee the implementation of effective internal controls. The board shall have responsibility ensuring and reporting to the shareholders at the annual general meeting of the financial institution, that the internal controls and systems, and management information systems of the financial institution (i) are designed to provide reasonable assurance as to the integrity and reliability of the financial statements of the financial institution and to adequately safeguard, verify and maintain accountability of its assets; (ii) are based on established and written policies and procedures, and are implemented by trained and skilled officers with an appropriate segregation of duties; and (iii) are continuously monitored, reviewed and updated by the board of directors to ensure that no material breakdown occurs in the functioning of such controls, procedures and systems[45]. This enables the financial institution to set up policies and guidelines in order to protect its customer's private data

Supervisory framework

A financial institution shall furnish to the Central Bank at such times and in such form as the Central Bank may prescribe, all information and data of its operations in Uganda including periodic returns called for by the Central Bank and the audited balance sheet and profit and loss account and those of any company which is a subsidiary, affiliate, associate or holding company to that financial institution.[46]

The Central Bank may, upon request made to it by any monetary or financial regulatory authority in the ordinary course of its business, disclose any of the information provided under this section to that monetary or financial regulatory authority within or outside Uganda; except that the Central Bank shall, before disclosing any information under this section, first satisfy itself that the information is required for the proper discharge of the functions of the requesting monetary authority or financial regulatory authority[47]

---

[44] Section 10(1) of the financial institutions Act 2004
[45] Section 55(1) of the financial Institutions Act 2004
[46] Section 80 of the financial institutions Act, 2004
[47] Section 80(5) of the financial institutions Act, 2004

The Bank of Uganda Financial Consumer Protection Guidelines, 2011.

These Guidelines apply to; (a) all financial services providers regulated by Bank of Uganda in respect of business they transact in Uganda and (b) the agents of all financial services providers regulated by the bank of Uganda in respect of business the agents transacts in Uganda.[48]

Objectives of the Guidelines.

To promote fair and equitable financial services practice by setting minimum standards for financial services providers in dealing with consumers; (b) increase transparency in order to inform and empower consumers of financial services; (c) foster confidence in the financial services sector; and (d) provide efficient and effective mechanism for handling consumer complaints relating to the provision of the financial products and service.[49]

Key principles.

The relationship between a financial service provider and a consumer shall be guided by three key principle; (a) fairness[50]; (b) reliability[51] (c) Transperency[52].

A financial service provider shall not disclose any information about a consumer to the third party except where; (i) all financial service provider is compelled by law to disclose the information; or (ii) the disclose is made with express consent of the consumer.[53]

At common law there exists a relationship between the banker and its customer. What is the nature of the relationship? In the case of Esso Petroleum Co. v Uganda Commercial Bank[54], the Supreme court held that the relationship of the banker and a customer is contractual. With existence of a contractual relationship, each party to the contract must fulfill its obligations. This research explores the one the obligations or duties of the bank to its customers which is, "the duty of Confidentiality."[55] The duty of non disclosure is a legal one arising out of contract and that the duty is not absolute, but qualified. It is not possible to frame any exhaustive definition of

---

[48] Guideline 2 of the bank of Uganda Financial Consumer Protection Guidelines, 2011
[49] Guideline 4 of the bank of Uganda Financial Consumer Protection Guidelines, 2011
[50] Guideline 6 of the bank of Uganda Financial Consumer Protection Guidelines, 2011
[51] Guideline 7 of the bank of Uganda Financial Consumer Protection Guidelines, 2011
[52] Guideline 8 of the bank of Uganda Financial Consumer Protection Guidelines, 2011
[53] Guideline 7(3) of the bank of Uganda Financial Consumer Protection Guidelines, 2011
[54] Esso Petroleum Co. v Uganda Commercial Bank Civil Appeal No. 14 of 1992
[55] That is the duty not to disclose any information concerning the affairs of the customer without his/her consent.

the duty. On principle, the qualification can be classified under four heads (a) where the disclosure is under compulsion (b) where a duty to the public to disclose (c) where the interest of the bank requires disclosure; and (d) when the disclosure is made by the express or implied consent of the customer.[56]

Conclusion

In conclusion, the exploration of Uganda's legal landscape of the research in this chapter has provided a panoramic view of the intricate tapestry of statutes that govern data protection, privacy, and cyber security in the banking sector. Whereas there is an existing legal framework, there needs for a regulatory body regulating data privacy in banks.

[56] L.J in the case of Tourner v. National Provincial and Union Bank of England (1924) 1 KB 461

CHAPTER THREE: BANK APPROACHES TO DATA PROTECTION AND DATA SECURITY INCIDENTS THAT HAVE OCCURRED.

INTRODUCTION;

Chapter Three provides the research methodology of this dissertation. I will use the qualitative research methodology designed to understand the approaches that banks have employed and legal frameworks that shape the banking sector's approach to cyber security in Uganda. This chapter focuses on understanding the 'how' and 'why' behind the effectiveness of cyber security, as influenced by data protection and privacy strategies.

Through a careful examination of current trends and policies, this research aims to provide a rich, contextual analysis of the factors that contribute to robust cyber security postures in financial institutions. By adopting a qualitative methodology, I aim to explore the implications, motivations, and outcomes of the strategies implemented by banks in Uganda.

The insights garnered from this qualitative inquiry will not only shed light on the current state of affairs but will also offer a foundation for recommendations and future enhancements in the realm of cyber security. As we navigate through this chapter, I will set the stage for a comprehensive understanding of the legal and strategic landscape that banks operate within, ultimately contributing to the broader discourse on data protection, privacy, and cyber security in the digital age.

Banks have a duty to protect customers' personal information that they manage to collect from their customers. However it should be noted that, if Banks put in place secure systems to protect unauthorized access to customers' information they are not liable for any breach that happens. This position was highlighted in the case of Aida Atiku vs Centenary Rural Development Bank Limited[57]. The case also places an obligation to the customer of preventing third party access. Customers must not share their bank details to third parties and also ensure that they do not share information that they provide to banks to other parties. Therefore each party is obligated to ensure that the information the bank keeps is safe and each party should make sure that no breach happens on the account.

[57] Aida Atiku vs Centenary Rural Development Bank Limited Civil suit No.754 of 2020

PRACTICES OF BANKS IN UGANDA ON DATA PROTECTION

Standard Bank Group

The Privacy and security statement from Standard Bank Group of Companies(a mother company of Stanbic Bank Uganda Limited)[58], entails how customer's personal data is collected, used, stored, made available, disclosed, updated, safe guarded and destroyed. It is stated in the privacy statement that, they combine customer's personal information and use it for purposes set out in the statement such as contract requirements, lawful obligations, legitimate interest and acquire consent when acquiring the data. Stanbic Bank is registered with the Personal Data Protection Office[59] hence the Data Protection and Privacy Act, 2019 applies to it.

According to the privacy and security statement, personal information of the bank's clients is processed in South Africa or in countries where they have presence. The Bank only processes information to countries that it is satisfied will provide adequate data protection and they ensure that third parties comply with the minimum data protection standards of the Standard Bank Group. The group retains the customers' personal information in line with their regulatory obligations for at least ten years from the client's last transaction.

Stanbic Bank uses the customer's personal information to market the bank's products to the customer and if you are a prospective client and the bank has no previous interaction with you or relationship, the bank seeks your express consent in compliance with the laws in Uganda.[60]

According to the privacy and security statement, the bank shares the information with third parties, auditors and advisors, with their trusted partners, with agencies and other financial institutions on credit, with data validation and trust providers and with local and foreign government and other authorities required by law.

According to the privacy and security statement, Stanbic Bank takes reasonable steps to keep the clients' personal information safe and to prevent loss, destruction, damage or unlawful access.

---

[58] Stanbic Bank Uganda limited; Privacy and security statement accessed on 2nd May 2024 https://www.stanbicbank.co.ug/uganda/personal/about-us/legal/privacy-and-security-statement

[59] Registration number PDPO-202201-0080 registered on 7th December 2023 https://www.pdpo.go.ug/search-register accessed on 7th May 2024.

[60] Stanbic Bank Uganda limited; Privacy and security statement accessed on 2nd May 2024 https://www.stanbicbank.co.ug/uganda/personal/about-us/legal/privacy-and-security-statement

The bank requires the same level of security to be implemented by the bank's service providers and third parties.

Bank of Africa Uganda Ltd

The data Privacy Statement issued by Bank of Africa[61], provides for the type of data collected, from it is collected, what it is used for, and the treatment of data collected. The bank collects, processes and controls personal data that includes information that identifies the client as a unique individual such as name, age, date of birth, address, telephone number and any other information that is necessary or desirable to the bank to offer its services and also in some cases special data may be collected. Bank of Africa is a registered data collector and controller with the Personal Data Protection Office.[62]

The bank collects personal information in writing, by email, telephone, online through their website, internet banking, mobile wallet or Whatsapp, video conferencing from clients and relevant third parties according to the privacy statement by Bank of Africa.

The clients' personal information may be shared with in the bank and with selected data processors who process the data on the bank's behalf. The clients personal information is shared with the bank's regulators even those in foreign jurisdictions should they request for it. The bank retains the clients' information in accordance with retention periods set out in applicable laws

Stanbic Bank Cyber Security Incident

In the recent events there was a breach at Stanbic bank, where a senior administrator at Stanbic bank was accused of masterminding an electronic fraud scheme that resulted in the loss of 10.4 billion shillings from the banks Online Virtual Accounts to various mobile money SIM cards[63]. Mugerwa and others allegedly gained unauthorized access to the systems of an aggregator, Pegasus Technologies leading to the transfer of money from Stanbic Bank and Bank of Africa to

---

[61] Bank of Africa Uganda Limited; Data Privacy Statement accessed on 2nd May 2024 https://boauganda.com/support/legal/data-privacy-statement/

[62] Registration number is PDPO-202111-0008 registered on 3rd October 2023 https://www.pdpo.go.ug/search-register accessed on 7th May 2024

[63] Crispus Mugisha; Stanbic Bank employee charged with manipulating mobile money system, taking Shs10b accessed on 3rd May 2024 https://nilepost.co.ug/news/92884/stanbic-bank-employee-charged-with-manipulating-mobile-money-system-taking-shs10b (Mugisha, nilepost, 2020)

various mobile money SIM cards. Pegasus is a third party financial service provider working with various banks and utilities to provide bespoke solutions[64].

In this scenario the breach happened on the side of Pegasus Technologies which is a third party financial service provider, the breach happened remains unclear but the incident emphasizes the need for enhanced data protection strategies more so with regards to sharing data to third parties to ensure cyber security effectiveness in banks. This scenario also provides a signal for the need of increased regulatory oversight and compliance requirements for third parties and banks' service providers handling sensitive customer data.

During the Annual Bankers' Conference 2023[65], a discussion on cybersecurity was conducted and the following was discussed;

Mr. John Patrick Okiring (CEO, Ifortify Uganda) said that, " the technology foot print has grown rapidly but many people are excluded from the cyber security economy for reasons such as lack of knowledge of the cost of risk. Risk is what causes complexity. The necessity to integrate new technologies emphasizes this point. The issue of trusted identities has an impact on accountability. There is an issue with verification and authentication systems. All this exposes you to a slew of security issues, increasing identity theft."[66]

Ms. Diana Majimbo (Manager for cyber and intelligence, East Africa, Mastercard), said that, Conduct a proper organization risk analysis using The inside-out strategy, such as appraising staff, sensitizing and training them about cyber security. For the outside-in strategy, companies should devise ways to defend themselves, such As knowing and screening their partners. We should educate the public about the dangers of exposure.[67]

Mr. Ronald Azairwe, (Managing Director, Pegasus Technologies (U) Ltd) said that, No! We are not doing nearly enough. We are focusing on technology and processes while overlooking

[64] ibid
[65] Uganda Bank Association; Annual Bankers Conference 2023 accessed on 2nd May 2024 https://ugandabankers.org/annual-bankers-conference-magazine/
[66] ibid
[67] ibid

people. We should do due diligence on employees during recruitment because Internal employees are heavily[68].

The conference reflected that there is a need within stalk holders in banks to come with effective strategies in order to mitigate the cyber security risks in the banking sector. But the need for efficient and strong data protection strategies that could reduce cyber security risks and protect bank clients' data was not discussed.

Application of Legal Provisions;

Section 55 of the Financial Institutions Act[69] provides for the mandate that financial institutions establish risk management procedures for example the Privacy and security statement issued by Stanbic Bank which highlights bank's written policy on customers' data protection and privacy concerns. These policies help in reducing exposure of clients personal to unlawful people hence influencing cyber security effectiveness in banks. These policies ensure that Banks have accurate information about their clients which helps in identifying and mitigating potential risks such as fraud or identity theft which are significant concerns in the banking sector.

The data protection and Privacy Act under section 3 provides for principles of data collection that banks as data collectors should follow when collecting customers' personal data. In the Stanbic bank privacy and security statement it is stated that the bank is accountable for the data it collects, it provides that the collection process is done lawfully, it provides that Stanbic bank collects information about the client's identity, address, online identifies and the clients online behavior such as cookies and IP addresses, financial information, internal reports and other derivative data based on the personal information the bank collects and other personal information including biometric details, race, ethnic personal beliefs, political beliefs and others however section 9 of the data Protection and Privacy Act prohibits collection and processing of special personal data which relates to religious belief, political opinion, sexual life, medical records among others whereas section 9(3)b provides that the information can be given freely and with the consent of the data subject, section 12 of the data protection and privacy act provides that personal data should be collected for a specific purpose which is related to the functions and activities of the data collector. Banks and their customers operate on a fiduciary

[68] ibid
[69] Financial Institutions Act, 2004

relationship specific data such as religious beliefs and political opinion is not necessary in the functions and activities of banks with or without the consent of the data subject(bank customer) such specific data should not be collected.

The privacy and security statement also provides the client's data will be retained for a time not exceeding 10 years from the time of the client's last transaction. Section 18 of the data protection and privacy act notes that a person who collects data shall not retain the personal data for a period longer than necessary to achieve the purpose for which the data was collected and processed. Therefore the stanbic bank privacy policy on retention of data is in conformity with section 18.

The privacy statement provides that the bank takes reasonable care to protect the client's information. Section 20 of the Data Protection and Privacy Act provides for the degree of reasonable care that must employed by banks when protecting data and also the measures that should be taken by the banks in order to protect data they collect from their customers.

The privacy statement by bank of Africa provides that the bank requests the client to collect the data for proper performance of the contract between the bank and its client. This ensures that the bank complies with section 13 of the Data Protection and Privacy Act. And the also the Stanbic Bank's privacy statement provide that data is collected for contractual requirements, lawful obligations, legitimate interest and that consent is required. Consent is a key aspect in data collection and by obtaining consent, banks are limited to collecting only data necessary for specified purpose which reduces the amount of risk of data and exposure.

According to the privacy statements of Stanbic and Bank of Africa both provide that the client's personal data may be submitted to a government body which may be the central bank where the law requires. Section 80 of the Financial Institutions Act requires all financial institutions to furnish all information and data of their operations this also includes clients' personal data.

Whereas Section 40 of the Bank of Uganda Act[70], The bank may publish whole or in part of the information furnished to it as the Board may determine. But the bank shall not publish or disclose any information regarding the affairs of the bank or a customer of the bank unless the

[70] Section 40 of The Bank of Uganda Act cap 51

consent of the bank or the customer has been obtained.[71] This is to the effect that the Central Bank can acquire the information provided to it by a financial institution, it should not publish the information without consent of the financial institution and the client of the bank. This affects cyber security effectiveness since disposes information or data to many entities which can lead to linkage of the data to un authorized people. This enables customers retain their trust in financial institutions and bank system which enables customers to respect the privacy regulations put up by banks.

Stanbic bank privacy statement provides that the clients' personal data is may be processed in south Africa or country where their service providers are situated, the statement also provides that countries where the data may be processed comply or have adequate measures in place similar for protection of personal data. Section 19 Data Protection and Privacy Act provides that where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that;(a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this Act; or (b) the data subject has consented. This is to ensure that the data that is processed outside Uganda is not easily accessed by unauthorized persons.

According to the privacy statement by Stanbic Bank the person has the right to, access the personal information that the bank holds, object to the processing of the information, request to delete the personal information among others. This is in conformity with section 16 of the Data Protection and Privacy Act, 2019 and also enables individuals or bank clients retain autonomy over their personal information that is collected by banks and also reduces the possibilities of exploitation of individual data which would have created an avenue for hackers to fetch the data and use it to commit cybercrimes in banks.

In conclusion, this chapter aimed at providing a comprehensive understanding of the legal comprehensive understanding, practical aspects of data protection and privacy strategies employed by banks and their influence on cybersecurity effectiveness in Uganda's banking sector.

[71] ibid

CHAPTER FOUR: SUMMARY OF FINDINGS, RECOMMRNDATIONS ON THE BEST WAY FORWARD AND CONCLUSIONS.

Introduction;

The research on "Analyzing the influence of data protection and privacy strategies on cyber security effectiveness in the banking sector" has provided a wide view on the critical role these strategies play in ensuring security in the financial industry. The comprehensive analysis has shown that data protection and privacy are not just regulatory checkboxes but are integral to the robustness of cyber security frameworks within banks.

Summary of Findings:

Data Protection and Privacy strategies are very important pillars of Cyber Security: The study has shown that effective data protection and privacy strategies in banks are foundational to cyber security. They serve as the first line of defense against data breaches and cyber threats.

Regulatory compliance drives security enhancements. Compliance with legal requirements, such as Uganda's Data Protection and Privacy Act, has been shown to significantly influence the adoption of advanced cyber security measures in banks.

Customer trust and consent are key: The assurance of data protection and privacy fosters customer trust mainly through acquiring consent which is essential for the adoption of digital banking services and the willingness of customers to engage with cyber security protocols. This is done by ensuring that customers' consent is at the heart of every step in data collection.

Risk Management and Incident Response: Proper data handling and privacy measures are key to risk management and formulating effective incident response strategies, thereby enhancing the overall cyber security posture of banks.

Best practices and areas for improvement based on the analysis of trends and legal requirements.

Adherence to Data Protection Principles: Banks should strictly adhere to the principles laid out in the Data Protection and Privacy Act, such as lawfulness, consent, data minimization, and purpose limitation. For example basing on the privacy statement issued by Stanbic, they bank can share personal data to third parties this affects data minimization since the client's data is controlled and processed by many people which creates risk of data being exposed to un lawful people.

Creation of a Data Protection Body: A Data Protection Body ensures there is a dedicated role for overseeing data protection compliance and strategy within the banks. The body can be regulated by the central bank and its major role should be ensuring that all banks in Uganda have the same data protection and privacy policies. Both Stanbic bank and bank of Africa have some differing privacy policies basing on the privacy statements of both banks for example under the privacy statement of Stanbic bank data may be processed outside Uganda but in the Bank of Africa statement it's not clear where data is processed from. Such inconsistences in bank's privacy policies create an avenue for loopholes which can be used by hackers

Regular Training and Awareness: Conducting regular training sessions for staff on data protection laws and privacy rights helps maintain a high level of awareness and compliance.

Robust Cyber security Measures: Implementing strong cyber security measures like encryption, firewalls, and intrusion detection systems to protect personal data from unauthorized access.

Transparent Data Collection Policies: Clearly communicating to customers what data is being collected, for what purpose, and how it will be used, stored, and protected.

Areas of improvement include;

Enhancing Digital Literacy: Increasing efforts to educate the public on emerging digital threats and how to protect themselves can improve the overall cyber security posture. The public should be well acquainted with their data privacy rights in order to minimize data exploitation by banks which can lead to cyber security threats like cyber stalking.

Strengthening incident response; Developing and regularly updating a detailed incident response plan to address cyber security incidents swiftly and effectively through making reporting of incidents by clients easy and providing fast response.

Improving Recovery Rates: Focusing on mechanisms to improve the recovery rate of funds lost due to cybercrimes, thereby increasing trust in digital financial systems.

Governance Framework: Establishing a more robust governance framework for cybersecurity to ensure a safe and trusted digital economy in Uganda. The chair person Uganda Bankers Association said that they are pushing for harsh regulations for cybercrimes committed in the banking sector[72].

International Cooperation: Building linkages with the global cybersecurity community for better threat intelligence and response strategies. This can be done by looking at what other banks on the international scale are doing, the data protection and privacy strategies that are put in place by major financial players on the global scale on effecting cybersecurity effectiveness.

Relevance of this research in the future

Increasing Data Regulations. Theirs is need to increase data protection and privacy regulations in banks so as to ensure that customers ' personal data is inaccessible. This topic has addressed the need to increase data regulations such as to enhance cyber security effectiveness.

Rising Cyber Threats: There is a rising cyber threat in the banking sector making it important for banks to strengthen their cyber security measures.[73]

Consumer Behavior: Data privacy policies are increasingly influencing consumer behavior, with customers favoring financial institutions that protect their personal data[74].

Competitive Advantage: Banks that prioritize data privacy and cyber security can differentiate themselves and gain a competitive advantage.

---

[72] Samuel Muhimba, Equity Bank launches investigations into fraud claims. Accessed on 3rd May 2024 https://nilepost.co.ug/sports/190944/equity-bank-launches-investigations-into-fraud-claims

(Data)[73] Retail Banker International; Data Privacy in Banking: Regulatory trends. Accessed on 5th May 2024 https://www.retailbankerinternational.com/comment/data-privacy-in-banking-regulatory-trends/

[74] Retail Banker International; Data Privacy in Banking: Regulatory trends. Accessed on 5th May 2024 https://www.retailbankerinternational.com/comment/data-privacy-in-banking-regulatory-trends/

Global Impact: As the banking sector is connected globally, effective data protection strategies can have a worldwide impact and setting standards for international banking practices.[75] Understanding the influence of data protection and privacy strategies on cyber security effectiveness in the banking sector can help in setting standards for international banking aspects.

CONCLUSION

In a nutshell, this dissertation has highlighted that data protection and privacy strategies are not just compliance obligations but are strategic measures that significantly influence the cyber security effectiveness in the banking sector. As the digital landscape continues to evolve, banks must remain vigilant in enhancing their data protection and privacy strategies to ensure the cyber security.

[75] Institute of Data; Data Science in Banking accessed on 5th May 2024 https://www.institutedata.com/nz/blog/data-science-in-banking/

Bibliography

List of statutes

The 1995 constitution of the Republic of Uganda

Access to Information Act, 2005

Bank of Uganda Act, 51

Bank of Uganda Financial Consumer Protection Guidelines 2011

Computer Misuse Act, 2011

Data Protection and Privacy Act 2019

Electronic Signatures Act, 2011

Electronic Transactions Act, 2011

Financial Institution Act, 2004

National Information Technology Act 2009

Registration of Persons Act, 2015

List of cases

Tourner v National Provincial and Union Bank of England, 461 (KB 1924).

Esso Petroleum Co. v Uganda Commercial Bank, 14 (court of appeal 1992).

Aida Atiku vs Centenary Rural Development Limited, Civil Suit No. 754 (Hgh court 2020).

List of other relevant sources.

Akankwatsa, P. (n.d.). *Independent*. visited April 23rd, 2024, from Independent web site: https://www.indepedent.co.ug/banks-strive-to-counter-cyber-threats/

Ardent . (n.d.). visited on April 23rd, 2024, from https://www.ardentprivacy.ai/data-privacy-uganda/

Bank of Africa Uganda Limited. (n.d.). *Bank of Africa*. visited on May 2nd , 2024, from Bank of Africa Web site: https://boauganda.com/support/legal/data-privacy-statement/

Boehm, J. (2020, June). *McKinsey Digital*. visited on April 22nd, 2024

Cavoukian, A. a. (2012). *Privacy by Design in the Age of Big Data.* Eurocontrol Int.

Data, I. o. (n.d.). visited on May 5th , 2024, from https://www.institutedata.com/nz/blog/data-science-in-banking/

Gorecka, A. (2023). Competition law and privacy. *extensive data acquisition as the eye of the problem*.

Graham, S. (n.d.). visited on April 22nd, 2024, from https://www.ey.com/en_gl/news/2023/01/cybersecurity-is-number-one-risk-for-global-banks-but-geopolitical-risk-tops-european-banks-concerns

IMFWorking Paper (WP/21/46). (n.d.). visited on May 2nd, 2024, from https://www.imf.org/-/media/files/publication/WP/2021/English/wpiea2021046-print-pdf.ashx

Interpol Uganda. (n.d.). visited on May 22nd, 2024, from https://www.theeastafrican.co.ke/tea/business/hackers-skim-4m-off-banks-in-uganda-359339

Konde, N. (2024). Banking Beyond the Banking Hall. *A Review of Digital Banking in Uganda*, 53.

Kshetri, N. (2019). *The Privacy-Enhancing Technologies Landscape: A Critical Review.*

Mugisha, C. (2020, December 11th). *nilepost*. visited on May 3rd, 2024, from nilepost Website: https://nilepost.co.ug/news/92884/stanbic-bank-employee-charged-with-manipulating-mobile-money-system-taking-shs10b

Mugisha, C. (2024, March 07th). *Nile Post*. visited on May 3rd, 2024, from Nilepost Web site: https://nilepost.co.ug/sports/190944/equity-bank-launches-investigations-into-fraud-claims

Muhima, S. (2024, March 07th). *NilePost*. visited on May 3rd, 2024, from Nile Post: https://nilepost.co.ug/sports/190944/equity-bank-launches-investigations-into-fraud-claims

Nabisubi, R. (n.d.). *Monitor*. visited on April 22nd, 2024, from Monitor Web site: https://www.monitor.co.ug/uganda/business/prosper/banks-themselves-for-data-protection-concerns-3717764

Retail Banker International. (n.d.). visited on May 5th, 2024, from https://www.retailbankerinternational.com/comment/data-privacy-in-banking-regulatory-trends/

Stanbic Bank. (n.d.). *Stanbic Bank*. visited on May 2nd , 2024, from Stanbic Bank web site: https://boauganda.com/support/legal/data-privacy-statement/

Uganda Bankers' Association. (n.d.). visited on May 2nd, 2024, from https://ugandabankers.org/annual-bankers-conference-magazine/

William, T. (n.d.). visited on April 22nd, 2024, from https://businessfocus.co.ug/exclusive-largest-smallest-banks-by-assets-named-as-total-industry-assets-hit-shs45-4tn-in-2022/#:~:text=Uganda’s%20banking%20industry%20total%20assets,based%20on%20their%20financial%20statements