UNIVERSITY OF KWAZULU-NATAL

College of Law and Management Studies

School of Law

The duty of bank confidentiality and the safeguarding of financial privacy

Kousar Bibi Ahmed

217037893

This mini-dissertation is submitted in pursuance of the requirements for the degree of

Masters of Law: Business Law

2024

Declaration regarding originality

I, Kousar Bibi Ahmed declare that:

A. The research reported in this dissertation, except where otherwise indicated, is my original research.
B. This dissertation has not been submitted for any degree or examination at any other university.
C. This dissertation does not contain any other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from such other persons.
D. This dissertation does not contain other persons' writing or ideas unless specifically acknowledged as being sourced from such persons. Where other written sources have been used then:
    a. Ideas from such sources have been summarised in the present author's words, but the ideas have been attributed to such sources, which have been referenced.
    b. Where exact words from these sources have been used, these words have been placed inside quotation marks, and referenced.
E. Where I have reproduced a part of a publication of which I am an author, co-author or editor, I have indicated in detail whether that part of the publication was written by myself alone, or by myself together with others and I have fully referenced such publications.
F. This dissertation does not contain text, graphics or tables copied and pasted from the internet, unless specifically acknowledged, and the sources detailed in the body and/or reference section of this dissertation.

Signed 

Date:6/2/24

ACKNOWLEDGMENTS

This thesis acknowledgement serves as a heartfelt tribute to the individuals who have made my academic journey truly worthwhile.

First and foremost, I extend my deepest gratitude to my parents, Hassan and Sheanaaz Ahmed. Your unwavering dedication and tireless efforts have profoundly shaped my character and academic pursuits. Words cannot adequately express the depth of my appreciation for everything you have done for me.

To my beloved husband, Zakir Vorajee, your boundless patience and meticulous attention to detail in proofreading have been my steadfast support throughout this journey. You are the light of my life.

To my remarkable siblings and their exceptional partners, each of you has played an integral role in my academic endeavors. Your unwavering support and encouragement have been a source of strength, and I am profoundly grateful for your presence in my life.

Jeremiah Reddy, my dear friend, your unwavering belief in my abilities have been a constant source of inspiration. Thank you for standing by me through it all.

Mr. Ramdhin, my esteemed supervisor, your guidance and patience have been invaluable throughout this process. Your wisdom and clarity have been instrumental in shaping the trajectory of my research and academic growth. I am deeply indebted to you for your mentorship and support.

DEDICATION

To my parents, your sacrifices have not gone unnoticed.

ABSTRACT

It has been widely accepted that banks owe customers a duty of confidentiality to protect their personal information. The Protection of Personal Information Act 4 Of 2013 (POPIA) was enacted for the same purpose. While there is considerable academic literature on both the duty of confidentiality and POPIA, few studies have examined their intersection within the banking realm. Understanding this intersection is crucial for comprehensively defining customers' privacy rights in banking. Through a study of the legislation, case law, journal articles, and books, the duty of confidentiality and POPIA will be explored. The duty of bank confidentiality has exceptions, including the duty to disclose to the public, disclosure in the bank's interest, and disclosure compelled by law. POPIA affects banks and data subjects through accountability, processing limits, and data security.

Banks must comply with strict rules, collect only essential data, and ensure strong security measures. They need explicit consent for processing, prompt breach notification, and cooperation with the Information Regulator to protect privacy rights. Both POPIA and bank confidentiality aim to protect customer information by setting clear rules and broadening data protection. Customers gain rights over their data, ensuring transparency. Mandatory breach notification underscores the focus on data security, highlighting their shared commitment to customer privacy. In case of breaches, customers and data subjects have legal recourse. Customers can claim damages and seek interdicts for breaches of confidentiality. Under POPIA, data subjects can sue for damages, including statutory offences leading to criminal sanctions. POPIA strengthens customer rights and aligns with banking confidentiality by granting customers more control over data while obligating banks to ensure its protection, reinforcing customer privacy within banking.

Table of Contents

CHAPTER ONE
INTRODUCTION AND OVERVIEW

I. INTRODUCTION

It is widely acknowledged that banks owe their customers a duty of confidentiality regarding the customers' banking affairs.[1] Some countries have ensured that this duty is upheld by implementing legislation.[2] In South Africa, the duty is often seen as part and parcel of the contract between a bank and its customer.[3] The English decision of *Tournier v National Provincial Union Bank of England* [4] recognised the existence of the duty and set out exceptions[5] (these exceptions will be thoroughly covered in chapter two). After that, this duty was incorporated into South African law, and it was assumed that it was an implied or tacit term of a contract.[6]

The duty of confidentiality can also be seen to be founded in the Constitution, namely section 14, which deals with the privacy of individuals, their property, their possessions, and communications.[7] Roos very succinctly stated that the right to privacy allows people to have control over their information.[8] Neethling[9] expanded on this when he said that informational privacy is described as a person's right to decide in what circumstances (when and how) their information is shared with others[10]. Therefore, in the context of a bank-customer relationship, a customer can demand privacy and confidentiality regarding personal, financial, and any related information in dealings with the bank.[11]

---

[1] H Schulze 'Confidentiality and secrecy in the bank-customer relationship' (2007) 15(3) *Juta's Business Law* 122.
[2] Ibid.
[3] Schulze (see note 1 above) 122.
[4] *Tournier v National Provincial Union Bank of England* [1924] 1 KB 461 (CA).
[5] Ibid 7.
[6] A Ramdhin 'The Bank- customer Relationship' in R Sharrock (ed) *The Law of Banking and Payment in South Africa* 110-135; see also MA Mthembu 'Marriage of convenience: Bank – Customer Relationship in the age of the internet: A South African Perspective' (2014) 9(1) *JICLT* 14-21.
[7] Section 14(d) of the Constitution of the Republic of South Africa, 1996 states "Everyone has the right to privacy, which includes the right not to have— (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed."
[8] A Roos 'Data protection: explaining the international backdrop and evaluating the current South African Position' (2007) 124(2) *SALJ* 400.
[9] J Neethling 'The concept of privacy in South African law' (2005) 122(1) *SALJ* 18; see also I Currie & J De Waal *The bill of rights handbook* 6 ed, (2013) 303-304.
[10] Ibid 20; see also Ibid 302.
[11] J Faul 'Teoretiese fundering van die bankgeheimnis in die Suid-Afrikaanse reg' (1986) *TSAR* 180.

According to the Constitution, this is considered to be part of section 14, which seeks to protect the privacy of individuals.[12] However, all constitutional rights can be limited in terms of section 36 of the Constitution if it is "reasonable and justifiable to do so in an open and democratic society based on human dignity, equality, and freedom,"[13] together with this fact, particular limitations can be applied to banks duty of confidentiality as set out in the case of *Tournier v National Provincial Union Bank of England* [14].

Apart from the Constitution, there have been arguments that the duty of confidentiality can also be rooted in legislation and custom. Legislation indirectly acknowledges the duty of confidentiality without explicit mention of banks and their confidentiality obligations[15], this is evident in statutes such as the Financial Intelligence Centre Act (FICA),[16] which recognises that certain institutions are expected to maintain secrecy but does not mention banks explicitly.[17]

Section 33(1) of the South African Bank Act provides a general prohibition on disclosing customer information.[18] Specific statutes, such as the National Credit Act (NCA), impose a duty of confidentiality on banks under certain circumstances.[19] Section 68(1) of the NCA states that "any person (such as a bank) who receives, compiles, retains, or reports any confidential information pertaining to a consumer or prospective consumer in accordance with the Act must protect that information's confidentiality."[20]

The relevant laws governing a bank's obligation to preserve the confidentiality and secrecy of its customers' affairs typically operate on the premise that the bank is obligated to uphold such confidentiality without explicitly outlining the justification for this duty.[21] There is no legislation setting out the basis of a bank's duty of confidentiality; therefore, the idea that the duty is rooted in legislation can be debatable.[22]

---

[12] S14 of the Constitution.
[13] S36 of the Constitution.
[14] *Tournier* (note 4 above).
[15] Ramdhin (note 6 above) 136.
[16] Financial Intelligence Centre Act 38 of 2001.
[17] Ramdhin (note 6 above) 135.
[18] JG Machokoto 'The duty of bank confidentiality in South Africa and other Jurisdictions such as Zimbabwe: Justifications, Judicial limitations and Legislative Inroads rising from the need to avert crimes' (2018) 1(1) *University of Zimbabwe Law Journal* 1-3.
[19] National Credit Act 34 of 2005.
[20] S68(1) of National Credit Act 34 of 2005.
[21] FR Malan, JT Pretorius & SF Du Toit *Malan on Bills of Exchange, Cheques and Promissory Notes in South African law* 5 ed (2009) 310.
[22] Ibid.

II. WHAT IS DATA PROTECTION?

While the complexities of modern data protection is trite, the historical significance of record-keeping across diverse civilizations cannot be ignored.[23] Roos stated that data protection is "an aspect of the protection of a person's right to privacy and can be considered as a fundamental right."[24] It entails the legal protection of people in relation to the personal information that a data processor processes.[25] POPIA[26] contains a definition of what personal information entails.[27] The definition is broad and can include things such as identity numbers, marital status, contact numbers, place of residence, financial history, and even bank account information.[28]

III. WHY DOES PERSONAL INFORMATION NEED TO BE PROTECTED?

California Bankers Association v Schultz[29] very eloquently postulates why personal information needs to be protected. It states, "In a sense, a person is defined by the checks he writes. By examining them, the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers, and magazines he reads, and so on ad infinitum. ... the banking transactions of an individual give a fairly accurate account of his religion, ideology, opinion, and interests… .".[30] This highlights the extensive data banks gather on their customers, emphasising the need to safeguard this information to preserve customer privacy.

The imperative to protect personal data was starkly highlighted on August 4, 2020, when Nedbank became aware of a breach involving Experian SA, a credit bureau.[31] It was discovered that Experian had inadvertently disclosed the personal information of their customers to a fraudulent third party posing as a legitimate Experian customer.[32] The compromised information encompassed a wide array of sensitive details, including customer names, identity numbers, contact numbers, email addresses, and residential addresses, putting over one million active Nedbank customers at risk.[33]

---

[23] Roos (note 8 above) 401.
[24] Roos (note 8 above) 403.
[25] Roos (note 8 above) 402-403.
[26] Protection of Personal Information Act 4 of 2013 (POPIA).
[27] Chapter 1 of POPIA.
[28] Ibid
[29] *California Bankers Association v Schultz* 416 US 1974 21.
[30] Ibid 85.
[31] A Arde', 'Nedbank data breach may leave victims open to fraudulent attacks, say experts' (Sunday Times Business Times, 8 March 2020) available at <https://www.timeslive.co.za/sunday-times/business/2020-03-08-nedbank-data-breach-may-leave-victims-open-to-fraudulent-attacks-say-experts/> accessed on 4 February 2024.
[32] Ibid.
[33] ibid.

IV. TERMINOLOGY

During this dissertation, the term “bank confidentiality” will consistently be employed to articulate the bank’s obligation of secrecy. While these expressions, “bank confidentiality” and “bank secrecy”, are frequently utilised interchangeably, the former will consistently be used to denote the same overarching concept.

V. STATEMENT OF PURPOSE

The primary objective of this dissertation is to address a notable gap in the existing literature regarding POPIA and its implications for the duty of bank confidentiality. Despite the recent introduction of POPIA, there is a distinct lack of research that explores the intersection between POPIA and the traditional duty of bank confidentiality.

The dissertation seeks to provide clarity on the evolving regulatory landscape surrounding data privacy and confidentiality in the banking sector. Through comprehensive analysis and examination of relevant legislation, the study intends to contribute valuable insights into the complex dynamics between POPIA and the duty of bank confidentiality, ultimately enhancing understanding and informing best practices in safeguarding customer information and privacy rights.

VI. RATIONALE

The evaluation of the duty of banking confidentiality and the implications POPIA hold significant importance due to their profound impact on individuals engaging with banking services. Understanding the circumstances under which personal information may be disclosed and the available remedies in case of unlawful disclosure are essential for customers navigating the intricacies of banking relationships.

Traditionally, the duty of banking secrecy has been a cornerstone principle within the banking industry. However, the enactment of POPIA has introduced novel obligations for banks and conferred more detailed rights upon customers, who are also recognised as data subjects under the legislation. Despite the considerable academic discourse surrounding POPIA, there exists a notable gap regarding the interconnectedness of banking confidentiality and the provisions of POPIA, alongside the precise nature of the new obligations it imposes on banks and its ramifications for bank customers.

Clarifying these aspects is pivotal for achieving a comprehensive understanding of customers' positions regarding privacy within the banking realm. This dissertation endeavors to contribute meaningfully to the ongoing discourse surrounding the duty of confidentiality and POPIA, aiming to illuminate previously unexplored areas and provide nuanced insights into the implications for both banks and their clientele. By elucidating these aspects, the dissertation seeks to enrich the existing

body of knowledge and foster informed discussions pertaining to privacy rights and obligations in the banking sector.

VII. RESEARCH QUESTIONS

1.1 What are the exceptions to the duty of banking confidentiality, and how do these exceptions impact customer privacy?

1.2 How does the implementation of POPIA introduce novel obligations and compliance standards for banks concerning the handling and protection of customer data?

1.3 To what extent does POPIA complement the existing banking duty of confidentiality, and how do these synergise to enhance customer privacy and data protection in the financial sector?

1.4 What legal mechanisms and remedies exist in cases of breach of the bank's duty of confidentiality and POPIA?

VIII. RESEARCH METHODOLOGY

This research will adopt a primarily doctrinal approach, intending to address the research questions by conducting a thorough analysis of legislation, case law, and scholarly literature pertaining to privacy, data protection, and the duty of confidentiality. The methodology will entail extensive desk-based research involving an exhaustive examination of pertinent statutes and secondary sources, including textbooks, articles, and journal entries sourced from esteemed legal databases such as Juta, Lexis Nexis, HeinOnline, and EBSCOhost.

The principal focus of this dissertation will revolve around the exploration of the duty of confidentiality within the banking sector and the ramifications of POPIA on the processing of personal data by banks in South Africa. By leveraging a variety of scholarly materials, including journal articles, textbooks, codes of conduct, and academic research papers, the study aims to delve into the adjustments banks have been compelled to make in response to regulatory shifts and to evaluate the augmented protections extended to customers in light of these regulatory developments.

IX. STRUCTURE OF THE STUDY

1.1 Chapter 1

This chapter provides an overview of the duty of confidentiality in banking, tracing its roots from legal precedents to constitutional provisions. It discusses the implications of data protection laws like POPIA and the need to safeguard personal information in the digital age. The purpose of the dissertation is to explore how the duty of confidentiality has evolved with the introduction of POPIA and whether it complements the banks' duty of confidentiality. The research questions focus on legal frameworks, compliance standards, the synergy between POPIA and banking confidentiality, and available legal

remedies for breaches. The research methodology involves a doctrinal approach, analysing legislation, case law, and literature to understand the evolving landscape of privacy and data protection in the banking sector.

1.2 Chapter 2

Chapter two provides an extensive exploration of the duty of confidentiality in banking relationships. It delves into the legal, contractual, and ethical dimensions of the bank-customer relationship, emphasising the significance of confidentiality in safeguarding financial privacy. The chapter navigates through the legal framework in South Africa, examining the duty of confidentiality and exploring exceptions to this duty. It also discusses the termination of the bank-customer relationship and the enduring duty of confidentiality beyond its dissolution. The chapter underscores the delicate balance between individual privacy and broader societal interests while emphasising the legal obligations of maintaining confidentiality.

1.3 Chapter 3

Chapter three offers a comprehensive examination of the obligations stipulated by POPIA concerning the processing of personal data. It delves into the far-reaching impact of POPIA on the banking sector, elucidating the rights, obligations, and regulatory oversight mechanisms inherent in this legislative framework. The chapter also scrutinises the pivotal role of the Information Regulator in ensuring privacy protection and evaluates the Code of Conduct submitted by the Banking Association of South Africa to align with POPIA standards. Moreover, the chapter navigates through the intricate dynamics between POPIA and the duty of banking confidentiality within South Africa's financial realm. It sheds light on the convergence of objectives, legal foundations, and information covered by these regulatory frameworks, thereby highlighting the evolving landscape of data protection and confidentiality in the banking sector.

1.4 Chapter 4

Chapter four delves into the repercussions faced by banks in the event of breaching the duty of banking confidentiality, drawing from legal precedents. The chapter emphasises customers' empowerment in pursuing legal remedies for breaches of the duty of confidentiality. It also lays out the recourse available under POPIA when specific provisions are not complied with. It ends with a concluding paragraph of all available remedies under the scenarios above.

1.5 Chapter 5

Chapter 5 provides a comprehensive overview of the study's findings regarding the intersection of the POPIA and the duty of banking confidentiality in South Africa. It synthesises critical insights from previous chapters, emphasising the evolving landscape of data protection laws and banking confidentiality obligations. The chapter underscores the challenges and opportunities presented by POPIA for banks, highlighting the importance of adapting to nuanced changes to ensure customer confidentiality and data security. Moreover, it outlines potential legal ramifications for breaches of banking confidentiality and elucidates customers' avenues for recourse in such scenarios. Through an analysis of legal precedents and regulatory frameworks, Chapter 5 elucidates the importance of upholding confidentiality standards while navigating the dynamic regulatory environment.

CHAPTER TWO
THE DUTY OF BANKING CONFIDENTIALITY

I. INTRODUCTION

This chapter explores the intricacies of the bank-customer relationship, focusing on the pivotal duty of confidentiality. To do this, the chapter delves into the nature of the bank-customer relationship, shedding light on its legal, contractual, and ethical dimensions as well as looking at the criteria for classifying individuals or entities as "customers" within the banking context. This classification holds substantial legal and practical implications.

This analysis is crucial for grasping the essence of the relationship itself and the nuances involved in its termination. At the heart of this exploration lies the duty of confidentiality—a linchpin of the bank-customer relationship. This chapter presents an in-depth analysis of this duty, emphasising its paramount role in safeguarding the confidential financial information entrusted to banking institutions. In the complex realm of financial data and transactions, the duty of confidentiality serves as a guardian, preserving the sanctity of financial privacy.

Chapter two will encompass the legal framework in South Africa, focusing on the bank's obligation of confidentiality. It will explore the acknowledged exceptions to this duty, shedding light on the intricate situations where legal or urgent circumstances may warrant a departure from the principle of confidentiality.

II. THE BANK-CUSTOMER RELATIONSHIP

The conventional perspective defining an individual as a "customer" of a bank is contingent upon the requirement that the person holds an account with the bank.[1] The duration in which the person keeps the account is not essential, as the mere opening of an account at the bank will create a bank-customer relationship.[2] An individual or entity becomes a "customer" when the bank assents to the opening of an account at their institution in the name of the potential customer; the agreement of the bank to do so will be considered consent to take on the individual as a customer,[3] the bank will then take on the role of the customer's agent in the course of any transactions required, and the customer will gain protection

[1] M Jones & H Schoeman *An Introduction to South African Banking and Credit Law,* (2006) 2; see also M Hapgood. … et al. *Paget's Law of Banking* 13 ed, (2007) 141.

[2] *Commissioners of Taxation v English, Scottish and Australian Bank* [1920] AC 683 687 held that a "customer signifies a relationship in which a duration is not of essence. A person whose money has been accepted by a bank on the footing that they undertake to honor cheques up to the amount standing to his credit is, in the view of their lordships, a customer of the bank in the sense of statute, irrespective of whether his connection is of short or long standing."

[3] A Ramdhin 'The Bank- customer Relationship' in R Sharrock (ed) *The Law of Banking and Payment in South Africa* 110-112.

from third parties.[4] Yet, when construed more broadly, the term 'customer' includes any person who receives services from a bank during the time of business, regardless of whether they have a bank account.[5] However, traditionally, it has been accepted that the formation of the bank-customer relationship usually occurs when an account is opened in the name of the potential customer with the bank.[6]

III. CONTRACT

The bank-customer relationship is contractual[7] in instances where the financial institution undertakes to render specific services, and the customer commits to remuneration for those services.[8] It is understood as part of the agreement between a bank and its customer that the bank won't reveal the customer's information to others (third parties),[9] the bank is not allowed to disclose details about the customer's account status, transactions, or any information obtained while managing the account, except for specific situations outlined in the *Tournier*[10] case.

The fact that the bank-customer relationship is contractual in nature is evident; however, pinpointing the specific type of contract poses challenges since it does not fall precisely into established categories under Roman or Roman-Dutch law.[11] It can vary due to the services offered by the bank and the services required by the customer. Conventionally, the relationship exhibits features of debtor and creditor[12] and of agency and mandate.[13]

At its most fundamental level, the agreement between the bank and its customer constitutes a loan.[14] Customers give the bank a loan when they deposit money into their accounts, which is then due and repayable immediately.[15] As a result, the bank's and the customer's relationship in regard to a current account has been referred to as one of debtor and creditor.[16]

---

[4] MA Mthembu 'Marriage of convenience: Bank – Customer Relationship in the age of the internet: A South African Perspective' (2014) 9(1) *JICLT* 14-16.
[5] Ramdhin (note 3 above) 112.
[6] Ibid.
[7] *Foley v Hill* (1948) 2 HL Cas 28; Hapgood (note 1 above) 145.
[8] Ramdhin (note 3 above) 109.
[9] Mthembu (note 4 above) 16.
[10] *Tournier v National Provincial Union Bank of England* [1924] 1 KB 461 (CA).
[11] Ramdhin (note 3 above) 115.
[12] Jones & Schoeman (note 1 above) 2.
[13] Ibid.
[14] Jones & Schoeman (note 1 above) 3.
[15] Jones & Schoeman (note 1 above) 2.
[16] *Foley v Hill* concluded that "money, when paid into a bank, ceases altogether to be the money of the principal; it is then the money of the banker, who is bound to return an equivalent by a similar sum to that deposited with when he is asked for it…".

3.1 Mandate

The bank-customer relationship often incorporates a mandate.[17] This was seen in *Di Giulio v First National Bank of South Africa*.[18] In this case, the court found that "the relationship between the parties emanated from a contract of mandate and that even though the rights and obligations arising from the contract may be complex in nature, the relationship remained one of mandate."[19]

The bank must adhere strictly to the customer's instructions when acting under a mandate.[20] The bank is obligated to fulfill the actions mandated by the customer.[21] The bank also must act in good faith towards its customers,[22] as the bank has cultivated a sense of trust with its customers, and customers frequently seek advice from banks.[23] Along with this duty of good faith comes the duty of confidentiality, which is owed to customers regarding their personal information, which they give to the bank during the course of the bank-customer relationship.[24]

Traditionally, the bank-customer relationship does not contain a fiduciary duty.[25] However, since the banks offer a variety of services, this duty may arise within the framework of a specific contract.[26] In a notable case, the legal relationship between a bank and its client was scrutinised, as highlighted in *First National Bank of SA Ltd v Duvenhage*.[27] When the bank was assessing what duties are owed by the bank to their customers, the court recognised a legal duty on the bank's branch manager to act in Duvenhage's best interests, emphasising a relationship of trust inherent in the bank-client association.[28] This "relationship of trust" mirrors the common-law duty of a mandatary (the bank) to act in utmost good faith and conduct affairs in the mandator's interest.[29]

---

[17] *Di Giulio v First National Bank of South Africa* 2002 (6) SA 281 (C) 17-20; *Great Karoo Eco Investments (Edms) h/a Grobbelaarskraal Boerdery v Absa Bank Bpk* 2003 (1) SA 222 (W) 33.
[18] Ibid 20.
[19] *Di Giulio* (note 17 above) 228; see also *OK Bazaars (1929) v Universal Stores Ltd* 1973 (2) SA 281 (C) 288.
[20] Jones & Schoeman (note 1 above) 4; Mthembu (note 4 above) 17.
[21] Ibid.
[22] Jones & Schoeman (note 1 above) 4.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] M Ngidi 'The termination of the bank-client relationship in South African banking law' (2020) 53(1) *De Jure* 54-69.
[27] 2006 (5) SA 369 (SCA).
[28] WG Schulze 'Delictual Liability of a Bank towards Its Client: A New Prominence Given to the Element of Causation' (2006) *TSAR* 834.
[29] Ibid 834.

Malan suggests that the contract in existence between a bank and its customer can be categorised as one of mandate, implying that a bank's duty of confidentiality and secrecy originates from the duty imposed on a mandatory to conduct the mandate in good faith.[30] Stegman J, in the *GS George Consultants*[31] case, explored the idea that the duty of confidentiality between a bank and its customer is inherently part of their contract, whether through law or as a part of an implicit agreement.[32] This view suggests that banks are obligated to maintain secrecy either by legal incorporation into their contracts or by the mutual understanding between the parties involved.[33] Additionally, the judgment emphasised the historical acknowledgment of banks' duty to preserve confidentiality, drawing from legal precedents in both English law and South African cases like *Abrahams v Burns*[34] and *Cambanis Buildings (Pty) Ltd v Gal.*[35]

3.2 Nature of the bank-customer relationship

Itzikowitz[36] argues against the idea that classifying the relationship into specific categories of contract would be beneficial.[37] Instead, the author suggests that treating the bank-customer contract as sui generis allows for more flexibility in determining aspects of the contract.[38]

The different elements of the bank-customer relationship have led to it being classified as sui generis in law,[39] as the nature of the relationship is not solely based on contract and has additional duties that have been granted through banking practice, legislation, and court decisions.[40]

[30] FR Malan, JT Pretorius & SF Du Toit *Malan on Bills of Exchange, Cheques and Promissory Notes in South African law* 5 ed (2009) 311-312.
[31] *GS George Consultants and Investments (Pty) Ltd v Datasys (Pty) Limited* 1988 3 SA 726 (W) 734 H – 736 F.
[32] Ibid.
[33] *Abrahams v Burns* 1914 CPD 452.
[34] Ibid 452.
[35] *Cambanis Buildings (Pty) Ltd v Gal* 1983 2 SA 128 (N).
[36] Lauren Immerman, 'Financial Institutions and Stock Exchanges' (2002) *Ann. Surv. S. African L* 746.
[37] Ibid 746.
[38] Immerman (note 36 above) 746; see also CJ Nagel and JT Pretorius 'Mandate and the Bank and Customer Relationship' (2016) 79 *Journal of Contemporary Roman-Dutch Law* 514-516.
[39] Jones & Schoeman (note 1 above) 4.
[40] Ibid.

3.3 Duties that arise from the bank-customer relationship

In South African banking law, banks owe various duties to their customers. The bank generally undertakes to maintain and meticulously document the customer's accounts held with the bank,[41] promptly execute withdrawals from the customer's account as per their payment instructions,[42] and accept and process payments on behalf of the customer, [43] whether in the form of cash or electronic transactions[44] and providing the customer with periodic account statements.[45] As a financial institution, one of a bank's most fundamental obligations is to uphold confidentiality.[46] For this dissertation, only the duty of confidentiality will be elaborated upon.

3.4 Incorporation of the duty of banking confidentiality into South African law

In South Africa, the legal scrutiny of whether banks are bound by a duty of confidentiality towards their customers was initially addressed in the case of *Abrahams v Burns.*[47] The court held that a bank may be held accountable to a customer if there is a loss that has resulted from the bank disclosing a customer's details to third parties.[48]A similar stance was later echoed in the case of *Cambanis Buildings (Pty) Ltd v Gal*,[49] where the court underscored the general legal principle in South Africa that imposes a duty on banks not to reveal any customer information to outside parties (third parties).[50]

In *GS George Consultants and Investments (Pty) Ltd and Others v Datasys (Pty) Ltd,*[51] the court observed that the bank's duty of confidentiality, rooted in English law, has been acknowledged in South African law.[52] In the case of *Densam (Pty) Ltd v Cywilnat (Pty) Ltd,*[53] the court refrained from deciding whether, as a matter of law, a bank must maintain confidentiality toward its customers.[54] Instead, the court took for granted the existence of such a duty.[55] It also did not delve into the legal status of the exceptions as established in the *Tournier* case.[56] The court's position was that it was

[41] Ramdhin (note 3 above) 126.
[42] Ramdhin (note 3 above) 127.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] JD Mujuzi 'Bank Secrecy: Implementing the Relevant Provisions of the United Nations Convention against Corruption in South Africa' in B Martin & R Koen *Law and justice at the dawn of the 21st century: Essays in honour of Lovell Derek Fernandez* University of Western Cape, (2012) 117-131.
[47] *Abrahams* (note 33 above) 452.
[48] Ibid 454.
[49] *Cambanis Buildings (Pty) Ltd* (see note 35 above).
[50] Ibid 137E-F.
[51] *GS George Consultants and Investments (Pty) Ltd and Others v Datasys (Pty) Ltd* [1983] 1 All SA (NC) 737F.
[52] Ibid 736.
[53] *Densam (Pty) Ltd v. Cywilnat (Pty) Ltd* 1991 (1) SA 100 (A).
[54] Ibid 21.
[55] *Densam* (note 53 above) 21.
[56] Ibid.

unnecessary to engage in an in-depth examination of the legal nature of the contractual relationship between a bank and its customer or to investigate the existence of a duty of confidentiality or secrecy owed by the bank to the customer, along with its origins and limitations.[57] For the appeal, the court assumed, without a definitive conclusion, that the bank was under a contractual obligation to the appellant to maintain secrecy and confidentiality regarding its affairs,[58] per the principles outlined in the *Tournier* case.[59]

In the case of *Firstrand Bank Limited v Chaucer Publications (Pty) Ltd & Another*,[60] it was held that the bank is obligated to refrain from disclosing information shared between itself and its customer to third parties unless compelled by a more significant public interest.[61]

South African courts have affirmed that the bank's commitment to safeguarding confidentiality has been a historical aspect of English law and has been formally embraced within South African legal doctrine.[62] It can be argued that the contract alone is not enough of a basis on which to substantiate the duty of confidentiality[63] as the duty does not cease when the customer has closed their account with the bank, nor does it cease upon the death of the customer.[64] A multitude of legal sources governs the bank's obligation to maintain confidentiality in South Africa.[65] These include common law,[66] statutes,[67] and contracts[68] of a sui generis nature[69] or mandate.[70]

Banks have a legal and ethical obligation to maintain the confidentiality of their customer's financial information.[71] Significantly, this obligation is reinforced by the constitutional

[57] *Densam* (note 53 above) 21.
[58] *Densam* (note 53 above) 19-20.
[59] *Tournier* (note 10 above) 21.
[60] *Firstrand Bank Limited v Chaucer Republications (Pty) Limited and Another* [2008] 2 All SA 544 (C); 2008 (2) SA 592 (C).
[61] Ibid PARA 20.
[62] R Ismail 'Legislative erosion of the banker - customer confidentiality relationship' (2008) 48(2) *SALJ* 3.
[63] Ramdhin (note 3 above) 135.
[64] Hapgood (note 1 above) 1; see also JG Machokoto 'The duty of bank confidentiality in South Africa and other Jurisdictions such as Zimbabwe: Justifications, Judicial limitations and Legislative Inroads rising from the need to avert crimes' (2018) 1(1) University of Zimbabwe Law Journal 1.
[65] Ramdhin (note 3 above) 136.
[66] Ismail (note 62 above) 4.
[67] Mujuzi (note 46 above) 452.
[68] Ibid.
[69] Immerman (note 36 above) 747.
[70] *Di Giulio* (note 17 above) 17-20; see also *Great Karoo Eco Investments (Edms) h/a Grobbelaarskraal Boerdery* (note 17 above) 33.
[71] Jones & Schoeman (note 1 above) 6; see also H Schulze 'Confidentiality and secrecy in the bank-customer relationship' (2007) 15(3) *Juta's Business Law* 122.

right to privacy, specifically in section 14 of the South African Constitution,[72] highlighting the bank's legal and ethical duty to protect customer's financial information in line with informational privacy.[73]

3.5 The code of banking practice[74]

The banking code is a voluntary code that members of the Banking Association of South Africa[75] undertake to abide by.[76] It outlines the minimum service and conduct standards customers can anticipate from their bank concerning the services, products, and the desired customer relationship.[77] It is important to note that the code exclusively pertains to personal and small business customers.[78]

The code of banking practice intends to encourage adherence to sound banking practices by establishing minimum standards for banks in their dealings with customers,[79] improving transparency to offer customers a clearer picture of the realistic outcomes they can anticipate from products and services. [80]

Fostering a just and transparent connection between customers and their bank builds trust in the banking system, enhancing its stability and dependability. [81] As a foundational principle, the bank commits to treating all personal information with the utmost privacy and confidentiality,[82] refraining from disclosure except in specific circumstances.[83] These include legal mandates, public duty requirements, protection of the bank's interests to prevent fraud, customer consent, default in account obligations, and check-related verification services.[84]

In cases of default, the bank may share information about personal debts and account conduct with credit risk management services and debt collection agencies under certain conditions.[85]

---

[72] Constitution of the Republic of South Africa, 1996.
[73] J Neethling 'The concept of privacy in South African law' (2005) 122(1) *SALJ* 18- 20; see also I Currie & J De Waal *The bill of rights handbook* 6 ed, (2013) 302.
[74] The Banking Association South Africa Code of Banking Practice (2012).
[75] Absa , Access Bank, African Bank , Al Baraka, Bank of China , Bank of Taiwan, Barclays Bank PLC , Bidvest Bank , BofA Securities , Communications Bank , Capitec Bank , China Construction Bank , Citibank , Deutsche Bank , Discovery Bank, FinBond Mutual Bank, FirstRand, GBS Mutual Bank, Goldman, Sachs ,Grindrod Bank ,Habib Overseas Bank, HBZ Bank, HSBC Bank, Investec, Ithala, JPMorgan Chase, Nedbank , Postbank, Sasfin Bank , Standard Bank , Standard Chartered, State Bank of India accessed via https://www.banking.org.za/about-us/member-banks/ on 10th of February 2024.
[76] Code of Banking Practice (note 74 above) clause 1.
[77] Ibid.
[78] Ibid.
[79] Code of Banking Practice (note 74 above) clause 2.
[80] Ibid.
[81] Code of Banking Practice (note 74 above) clause 4.
[82] Code of Banking Practice (note 74 above) clause 6 (i-vi).
[83] Ibid.
[84] Ibid.
[85] Code of Banking Practice (note 74 above) clause 6 (vi).

Moreover, before sharing information with third-party service providers, the bank ensures reasonable steps to verify the confidentiality and security measures in place.[86] The Code also assures customers of being informed when telephone conversations are recorded, emphasising transparency and obtaining consent in instances of electronic banking facilities.[87] These provisions within the Code exemplify the commitment to safeguarding customer information.[88]

IV. EXCEPTIONS TO THE DUTY OF CONFIDENTIALITY

Banks may encounter situations where they are either exempted from their obligation to maintain confidentiality or are required to disclose the confidential information they possess about a customer.[89] *Tournier v National Provincial and Union Bank of England*[90] outlines four essential conditions or qualifications when disclosure is warranted.

4.1 Duty to the Public to Disclose[91]

This condition arises when a situation calls for a disclosure to the public interest, which takes precedence over the private duty of confidentiality.[92] Bankes LJ highlighted the exception to the duty of confidentiality in the *Tournier* case, stating,[93] "Many instances of the second class might be given. They may be summed up in the language of *Lord Finlay in Weld-Blundell v. Stephens,* where he speaks of cases where a higher duty than the private duty is involved, as where "danger to the State or public duty may supersede the duty of the agent to his principle."

This exception emerges when there is a potential danger to the state or when a public duty overrides the bank's duty to its customer. An example of this is when a customer is using their account for fraudulent purposes.[94] Balancing the public interest and the duty of confidentiality is usually quickly resolved, as the public interest has, to a large extent, been overtaken by legislation.[95] The *Firstrand Bank Ltd v Chaucer Publication (Pty) Ltd*[96] case conforms to this exception by affirming the bank's responsibility to uphold customer confidentiality yet allowing disclosure when there is a paramount public interest.[97]

---

[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] N Willis *Banking in South African Law* (1981) 41.
[90] *Tournier* (note 10 above) 473.
[91] *Tournier* (note 10 above) 473; see also A Itzikowitz & F Malan 'Asset Securitisation in South Africa' (1996) 8 *S. Afr. Mercantile LJ* 182.
[92] Ramdhin (note 3 above) 138.
[93] *Tournier* (note 10 above) 473.
[94] *South African Revenue Service v Absa Bank Ltd* 2003 (2) SA 96 (W) PARA 46.7.
[95] Ramdhin (note 3 above) 138.
[96] *Firstrand Bank* (note 60 above).
[97] Ibid PARA 20.

4.2 The interest of the Bank Requires Disclosure[98]

The obligation of confidentiality may be loosened when the bank deems it necessary to disclose information concerning the customer or their affairs to serve its interests.[99] Additionally, banks have the prerogative to disclose under the following circumstances.

4.2.1 Where a bank sues a customer for repayment of an overdraft

Disclosure is permissible when a bank is set to initiate legal action against a customer for overdraft repayment.[100] In the *Tournier* case,[101] Bankes LJ provided an example where a bank issues legal proceedings against a customer to recover an overdraft.[102] The amount owed becomes evident in the legal documentation, such as a writ of execution.[103] This disclosure of the debt amount is crucial for the bank to pursue its legal claim effectively.[104]

4.2.2 Disclosure upon Cession of Debt

In *G S George Consultants,*[105] the court determined that there were no indications of any circumstances that might have exempted the bank from its obligation to maintain confidentiality and secrecy towards its customers. However, in *Cywilnat v Densam,*[106] it was held that there were circumstances present that justified the court in relieving the bank of its duty of confidentiality and secrecy. The court referred to *Tournier*[107] and determined that the bank had an interest in disclosing the existence of such a claim to the cessionary when disposing of its claim.[108]

4.2.3 when a guarantor is sued in relation to a guaranteed account

Disclosure will be allowed in such an instance when a guarantor is sued in relation to a guaranteed account.[109]

4.3 Express or Implied Consent of the Customer[110]

While interpreting express agreement is relatively straightforward, implicit agreement poses more challenges.[111] Express consent occurs when the customer authorises the bank to disclose personal

---

[98] Itzikowitz & Malan (note 91 above) 546-547; see also NT Masete 'The challenges in safeguarding financial privacy in South Africa (2012) 7 *J. Int'l Com. L* 253.
[99] Masete (note 98 above) 253.
[100] Ramdhin (note 3 above) 139.
[101] *Tournier* (note 10 above) 473.
[102] Ibid.
[103] Ibid.
[104] Ibid.
[105] *GS George Consultants and Investments (Pty) Ltd and Others* (note 51 above) 736H.
[106] *Densam* (note 53 above) 24.
[107] *Tournier* (note 10 above) 461.
[108] *Firstrand Bank* (note 60 above) 60A-C.
[109] Ismail (note 62 above) 6.
[110] Ramdhin (note 3 above) 138.
[111] Ismail (note 62 above) 6.

information.[112] A typical scenario is when a customer requests their bank to furnish a reference to a third party, perhaps regarding the customer's creditworthiness.[113] Even with the customer's consent, the bank must operate within the limits of that authorisation.[114] Willis emphasises that the mutual practice among banks to provide references regarding a customer's creditworthiness is essential for the effective lending of money within the economy.[115] He asserts that, ethically, such references should only be disclosed with the explicit or implied consent of the customer. Implicit consent can occur when information regarding a customer's guaranteed account is disclosed to the guarantor or potential guarantor.[116] In cases where a bank lacks the authority to provide a banker's reference, it should abstain from offering such information.[117]

4.4 Disclosure under Compulsion of the Law[118]

Specific legislation can compel banks to disclose information, such as:

4.4.1 The Prevention of Organised Crime Act[119] (POCA)

The Act imposes the duty on banks to report any knowledge or suspicion in circumstances where there are reasonable grounds to believe that someone is involved in unlawful activities.[120] The Act defines "unlawful" activities as "conduct which constitutes a crime or which contravenes any law whether such conduct occurred before or after the commencement of this Act and whether such conduct occurred in the Republic or elsewhere." [121]

4.4.2 Financial Intelligence Centre Act[122](FICA)

The Financial Intelligence Centre Act (FICA) indirectly acknowledges the duty of confidentiality. The legislation is aimed at combatting money laundering. It states that "no duty of secrecy or confidentiality or any other restrictions on the disclosure of information, whether imposed by legislation or arising from the common law or agreement, affects compliance by an accountable institution, supervisory body, reporting institution, the South African Revenue Service or any other person with a provision of this part,"[123] it acknowledges that while a bank must keep their customers' information there are exceptions

---

[112] Ramdhin (note 3 above) 139.
[113] Ramdhin (note 3 above) 139; see also Ismail (note 62 above) 6.
[114] Ramdhin (note 3 above) 139.
[115] Willis (note 89 above) 40.
[116] Ismail (note 62 above) 6.
[117] *Standard Chartered Bank of Canada v Nedperm Bank Limited* 1994 (4) SA 747 (A) 762 J – 763 A.
[118] Schulze (see note 71 above) 122 noted "Usually involves examples of litigation which expressly or impliedly authorises disclosure."
[119] The Prevention of Organized Crime Act 121 of 1998 (POCA).
[120] S5 of POCA.
[121] S1 of POCA.
[122] Financial Intelligence Centre Act 38 of 2001 (FICA).
[123] Section 37(1) of FICA.

to this rule and banks can divulge customers information under certain circumstances.[124] However, the reporting obligation does not override the common law right to legal professional privilege.[125] This privilege is maintained in the relationship between an attorney and their client for legal advice or ongoing or anticipated litigation and between a third party and an attorney for ongoing or anticipated litigation.[126] In these cases, the common law right to legal professional privilege prevails, and the duty of confidentiality is not affected by the broader provisions mentioned in s37(1).[127]

POCA and FICA work together in an effort to combat financial crime, but it can force accountable institutions such as banks to breach their duty of confidentiality.[128] When defining money laundering, FICA states that it involves hiding or disguising the profits generated from illegal activities.[129] This process typically utilises entities of the formal financial system to make these profits seem legal and legitimate.[130] The entities specified in this definition are categorised as 'accountable institutions.'[131]

Within the financial sector, accountable institutions, including banks, play a pivotal role in either facilitating or mitigating money laundering operations. It is for this reason that these institutions are expected to comply with stringent requirements placed upon them not only by the acts above but by regulations contained in the Banks Act[132] as well.[133] Under POCA, participation in transactions associated with money laundering constitutes a criminal offense.[134]

The statute broadly defines proceeds of unlawful activities, encompassing various forms of property or benefits derived from illegal conduct, including common law crimes, statutory violations, and potentially unlawful agreements.[135] An individual or accountable institution would be guilty of an offence if they know or ought reasonably to have known that they were party to transactions stemming from theses unlawful activities.[136] This has ramifications for banks as they can be guilty of an offence if they ought reasonably to have known that a customer is utilising the bank to retain funds that are the

[124] Ibid.
[125] S37(2) of FICA.
[126] Ibid.
[127] Ibid.
[128] Ismail (note 62 above) 6.
[129] S1 of FICA.
[130] Ibid; see also Ismail (note 62 above) 6.
[131] Ismail (note 62 above) 6.
[132] Regulations 47 and 48 of the Banks Act 94 of 1990.
[133] Ismail (note 62 above) 6.
[134] S5 of POCA; Ismail (note 62 above) 7.
[135] Ismail (note 62 above) 7.
[136] Ibid.

proceeds of illegal conduct.[137] The illegal conduct will include common law crimes, statutory violations, and potentially unlawful agreements.[138]

FICA imposes stringent reporting obligations on banks, mandating them to disclose any customer suspected of involvement in illicit financial activities to the Financial Intelligence Centre (FIC).[139] The significant mandates imposed on accountable entities necessitate that banks authenticate and verify the identity of all customers,[140] uphold detailed records regarding clients, business associations, and transactions,[141] furnish such records—deemed public in nature—to an authorised representative of the FIC,[142] notify the FIC upon request about the presence of a current or previous mandate,[143] disclose any cash transaction surpassing a designated threshold, report suspicious and irregular transactions to the FIC[144] (this requirement applies to any individual, not exclusively to accountable entities), and divulge the possession or control of property owned or controlled by any entity involved in an act constituting a specified offense as delineated in POCDATARA (The entity may be identified in a notice issued by the President).[145]

FIC (Financial Intelligence Center) and the National Payment System Department (NPSD) jointly released guidance on accountable institutions' management of Electronic Funds Transfers (EFTs), emphasising compliance with directive 1 of FICA.[146] This guidance note offers practical insights into FICA's operational expectations for accountable institutions, mainly focusing on Directive 1, which pertains to institutions facilitating domestic and cross-border EFTs or acting as intermediaries in such transactions.[147]

The directive mandates Customer Due Diligence (CDD) for transactions suspected of money laundering or terrorist financing, regardless of their value.[148] A "qualifying EFT" exceeding R10,000 falls within Directive 1's purview, although FICA maintains a CDD threshold of R5,000.[149] Institutions are advised to capture verified client information for all transactions above R5,000, while

[137] Ibid.
[138] Ibid.
[139] Ibid.
[140] S21 of FICA; see also Ismail (note 62 above) 7.
[141] S22 of FICA; see also Ismail (note 62 above) 7.
[142] S26 of FICA; see also Ismail (note 62 above) 7.
[143] S27 of FICA; see also Ismail (note 62 above) 7.
[144] S28 of FICA; see also Ismail (note 62 above) 7.
[145] S29 of FICA; see also Ismail (note 62 above) 7.
[146] Moonstone Information Refinery, 'FIC Issues Guidance Note on Electronic Funds Transfers' (*Moonstone*, 11 April 2023) available at <https://www.moonstone.co.za/fic-issues-guidance-note-on-electronic-funds-transfers/> accessed on 4 February 2024.
[147] Ibid.
[148] Moonstone Information Refinery (note 146 above).
[149] Ibid.

CDD procedures are obligatory for suspicious cross-border EFTs, regardless of their amount.[150] Furthermore, for outgoing cross-border EFTs below R10,000 to high-risk jurisdictions, originator verification is strongly recommended to mitigate money laundering, terrorist financing, and proliferation financing risks.[151]

4.4.3 Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA)[152]

Section 12 of POCDATARA states that if a person suspects that another person intends to commit or has committed an offense under the Act, they must promptly report this suspicion to a police official.[153]

Under POCDATARA, various actions related to terrorism and related activities are considered offenses.[154] This Act addresses the directive aimed at combating money laundering and its connection to terrorist activities.[155] Failure to comply with reporting requirements is considered an offense.[156]

Section 4 of POCDATARA outlines an offense that applies to 'any person.' According to this section, banks and their employees must be watchful and avoid aiding transactions involving property they knew or reasonably should have known or suspected to be linked to terrorist activities.[157] No duty of confidentiality or secrecy prevents compliance with the reporting requirement, except for legal professional privilege between attorneys and clients.[158] Even then, legal professional privilege applies in specific legal contexts regarding communications between attorneys and clients.[159]

4.4.4 Prevention and Combating of Corrupt Activities (PRECCA)[160]

Section 34 of PRECCA is relevant to banks.[161] It states that individuals in positions of authority are mandated to report any suspicion or knowledge of certain offenses 'including theft, fraud, extortion, forgery, or uttering a forged document, amounting to R100,000 or more' to the appropriate police official.[162] Failure to adhere to this obligation constitutes an offense under the Act.[163] The definition of

---

[150] Ibid.
[151] Ibid.
[152] Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 (POCDATARA).
[153] S12(1)(a) and (b) of POCDATARA.
[154] S1 of PODACTARA states "terrorist and related activities" means any act or activity related to or associated or connected with the commission of the offence of terrorism, or an offence associated or connected with a terrorist activity, or a Convention offence, or an offence referred to in S11 – 14.
[155] S4 of POCDATARA.
[156] S12(2) of POCDATARA.
[157] S4 of POCDATARA.
[158] S12(9) of POCDATARA.
[159] S12(10) of POCDATARA.
[160] Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA).
[161] Ismail (note 62 above) 12.
[162] Ibid.
[163] Ibid.

"position of authority" encompasses a wide range of roles, such as government officials, municipal managers, heads of institutions, executives of companies, and individuals overseeing business management.[164] This definition includes banks and bank managers.[165] The test to determine whether an executive manager has committed an offence or not is if he knew or ought reasonably to have known or suspected another person committed a specific crime.[166]

Regarding banking confidentiality, this legislation encroaches upon the duty of confidentiality traditionally upheld by banks.[167] The level of protection previously afforded to bank clients has been significantly diminished due to the introduction of such legislation.[168]

V. TERMINATION OF THE BANK-CUSTOMER RELATIONSHIP

The bank-customer relationship, founded on a contractual basis, can be terminated by either party through various means.[169] Termination by agreement involves a mutual decision to end the contract, requiring settlement of any outstanding balances.[170] In the absence of a contrary agreement, either the customer or the bank possesses the authority to promptly terminate the contract by notifying the other party.[171]

Termination by law may occur due to the customer's death, sequestration, or the dissolution of the bank.[172] Upon termination, the credit balance becomes repayable, and if in debit, the bank can pursue legal action.[173] While the bank-customer relationship may be terminated, the duty of confidentiality endures, emphasising the importance of maintaining confidentiality beyond the existence of the bank-customer relationship.[174]

VI. CONCLUSION

The exceptions to the duty of confidentiality highlight a delicate balance between safeguarding individual privacy and addressing broader public interests.[175] Situations may arise where the public interest takes precedence over the private duty of confidentiality.[176]

---

[164] Ibid.
[165] Ibid.
[166] Ibid
[167] Ibid.
[168] Ibid.
[169] Ramdhin (note 3 above) 163.
[170] Ramdhin (note 3 above) 166.
[171] Ramdhin (note 3 above) 163.
[172] Ramdhin (note 3 above) 165.
[173] Ramdhin (note 3 above) 166.
[174] Ibid; see also *Tournier* (note 10 above) 473.
[175] *Firstrand Bank* (note 60 above) 20.
[176] Ramdhin (note 3 above) 138.

Banks operate within a legal framework that compels them to disclose information under specific circumstances.[177] Express or implied consent from customers plays a role in certain exceptions.[178] Customers may authorise the bank to disclose information for specific purposes.[179] Additionally, the bank has prerogatives to share information within its corporate group and with credit reference agencies, aligning with legal and business necessities.[180]

Disclosure under compulsion of the law is a significant exception, particularly in the context of combating money laundering and terrorist activities.[181] Legislation such as POCA and FICA compels banks to report suspicious transactions and entities involved in unlawful activities, emphasising the legal obligations placed on financial institutions.[182] Specific exceptions, like those outlined in POCDATARA,[183] aim to protect constitutional democracy against terrorist and related activities.[184] Section 34 of PRECCA is particularly relevant, mandating individuals in positions of authority, including banks, to report suspicions of specific offenses, emphasising the broader societal role of banks.[185]

The voluntary Code of Banking Practice reinforces confidentiality standards and outlines circumstances under which information may be disclosed.[186] The code underscores ethical considerations and the importance of protecting customer information while adhering to legal requirements.[187]

[177] Schulze (see note 71 above) 122.
[178] Ramdhin (note 3 above) 138.
[179] Ramdhin (note 3 above) 139.
[180] Masete (note 98 above) 253.
[181] Schulze (note 71 above) noted "Usually involves examples of litigation which expressly or impliedly authorises disclosure."
[182] S5 of POCA; Section 37(1) of FICA.
[183] Act 33 of 2004.
[184] S4 of POCDATARA
[185] S34 of PRECCA.
[186] Code Of Banking Practice (note 74 above) 6.
[187] Code Of Banking Practice (note 74 above) 6.

CHAPTER THREE
POPIA AND THE DUTY OF CONFIDENTIALITY

I. INTRODUCTION

Chapter 3 delves into the intricate dynamics of the intersection between POPIA and the longstanding duty of banking confidentiality in South Africa's financial landscape. As a comprehensive data protection legislation, POPIA focuses on safeguarding individuals' privacy, albeit within a legal framework different from the traditional duty of confidentiality imposed on banks. The chapter underscores the importance of understanding this intersection to comprehend how POPIA influences the conventional duty of confidentiality within the banking sector. While both frameworks share a commitment to protecting customer information, the chapter highlights their distinctions. POPIA introduces a more explicit and organised strategy for data protection, outlining precise principles and obligations for responsible parties. The subsequent sections of the chapter meticulously explore the impact of POPIA on the banking industry, covering crucial aspects such as consent and transparency, data security measures, data breach notification, processing limitation, and accountability. A comparative analysis is drawn between the obligations imposed by the duty of banking confidentiality and POPIA, emphasising differences in scope, legal foundation, and the nature of information covered.

The chapter also sheds light on the Code of Conduct submitted by the Banking Association of South Africa to the Information Regulator[1] providing specific processing practices to align with POPIA.[2] The Code underscores measures to secure customer information,[3] illustrating the evolving landscape of banking duties under the influence of POPIA. In navigating both frameworks, banks are challenged to adapt to nuanced changes to ensure the confidentiality and integrity of customer information.[4]

II. THE IMPACTS OF POPIA ON THE BANKING INDUSTRY, INCLUDING THE RIGHTS AND OBLIGATIONS OF BANKS, DATA SUBJECTS (CUSTOMERS), AND REGULATORY AUTHORITIES.

2.1 Accountability[5]

[1] The Banking Association South Africa Code of Conduct (2021).
[2] Ibid 1.5.
[3] Code of Conduct (note 1 above) 8.3.1.
[4] Ibid.
[5] S8 of POPIA.

Section 8 of POPIA places a significant burden on responsible parties to ensure compliance with the conditions outlined in the Act.[6] The responsible party is the entity responsible for defining both the purpose and methods used in processing personal information.[7] In simpler terms, they are the entities requiring personal information for specific purposes.[8] A data subject refers to any individual to whom the personal information relates.[9] Rationally, this would include customers and employees or any other person whose personal information is processed by an organisation.

Specifically, this section requires that banks (as responsible parties) meticulously adhere to the conditions set forth in POPIA, including all measures designed to enforce these conditions, both when determining the purpose and means of processing personal information and throughout the processing itself.[10]

Section 105 of POPIA deals specifically with unlawful acts by responsible parties in connection with account numbers. It is read with section 8 of POPIA. Section 105 emphasises that the accountable party must ensure compliance with all provisions of POPIA and handle personal information, including account numbers, appropriately.[11] Failure to do so constitutes an offense.[12] However, this offense only applies if the accountable party significantly and persistently violates section 8,[13] causing distress to the data subject,[14] with awareness of the wrongdoing[15] and its potential consequences.[16] Moreover, they must fail to take reasonable measures to prevent the violation.[17] In such cases, they can be charged with an offense under POPIA.[18]

Section 106 of POPIA outlines unlawful acts related to the disclosure and procurement of a data subject's account number without consent.[19] Third parties who knowingly or recklessly obtain or disclose a data subject's account number or procure its disclosure to another person are deemed to commit an offense under subsection (1) of POPIA.[20] However, certain defenses can be raised against such charges.[21] These include asserting that the action was necessary for preventing, detecting,

---

[6] Ibid.
[7] S1 of POPIA.
[8] E De Stadler & P Esselaar *A guide to the Protection of Personal Information Act* (2015) 15.
[9] S1 of POPIA.
[10] S8 of POPIA.
[11] S105(1) of POPIA.
[12] Ibid.
[13] S105(2)(a) of POPIA.
[14] S105(2)(b) of POPIA.
[15] S105(3)(a)(i) of POPIA.
[16] S105(3)(a) (i-ii) of POPIA.
[17] S105(3)(b) of POPIA.
[18] S105(1) of POPIA.
[19] S106 of POPIA.
[20] S106(1) of POPIA.
[21] S106(2) of POPIA.

investigating, or proving an offense or that it was required by law or court order.[22] Moreover, a person may argue that they reasonably believed they were legally entitled to obtain or disclose the account number[23]or that they would have obtained consent if the responsible party had been aware of the circumstances.[24] Additionally, if the action was in the public interest, it may serve as a defense.[25] Notably, any advertisement indicating the sale of a data subject's account number is regarded as an offer to sell the information, as stipulated in subsection (5) of the section.[26]

Section 55 of POPIA specifies that a responsible party must designate an Information Officer.[27] The responsibilities of the Information Officer include ensuring compliance with the conditions for the lawful processing of personal information, dealing with requests made to the responsible party, working with the Information Regulator, and ensuring overall compliance with POPIA.[28]

2.2 Processing limitation

Section 9 requires that personal information must be processed lawfully and in a manner that is not excessive, infringing on the privacy of the data subject.[29] In the context of POPIA, the processing means "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information."[30]

Banks must adhere to the principle of processing limitation, ensuring that personal information collected is adequate, relevant, and not excessive for the purposes for which it is processed.[31] This section is referred to as the minimality requirement.[32] This condition cannot be met if

[22] S106(2)(a)(i-ii) of POPIA.
[23] S106(2)(b) of POPIA.
[24] S106(2)(c) of POPIA.
[25] S106(2)(d) of POPIA.
[26] S106(5) of POPIA.
[27] S55 of POPIA.
[28] S55 of POPIA; see also 'Protection Of Personal Information' (*Standard Bank*) available at available at <https://www.standardbank.co.za/southafrica/personal/about-us/regulatory/popia/protection-of-personal-information-act> accessed on 4 February 2024; Standard Bank has stated that they have appointed an Information Officer and Deputy Information Officer and established the Data Privacy Office to keep them accountable.
[29] S9 of POPIA.
[30] S1 of POPIA.
[31] S10 of POPIA.
[32] De Stadler & Esselaar (note 8 above) 15.

the purpose for which the personal information is collected is not adequately defined.[33] Personal information may only be processed for specific, explicitly defined purposes compatible with the original reason for its collection.[34] Personal information may not be further processed in a manner incompatible with the initial purpose of collection unless the data subject consents or unless permitted by law.[35] This limitation prevents unauthorised disclosures or uses of personal information, maintaining confidentiality standards.[36] Organisations must be transparent about their data processing practices and be accountable for ensuring compliance with confidentiality requirements and other provisions of POPIA.[37]

2.3 Retention and restriction of records

Section 14 of POPIA sets rules for handling personal information records.[38] It says that records should not be kept longer than needed unless required by law[39] or with the person's consent.[40] If information is used to make decisions about someone, it must be kept for a reasonable time for them to ask for it.[41] Records must be destroyed securely when no longer needed.[42] Processing of personal information can be restricted if accuracy is challenged or if the data subject asks for it.[43] During restriction, information can only be used for specific reasons, like proof or protecting rights.[44] The responsible party must tell the person before lifting any restrictions.[45]

2.4 Data subject participation

Under the POPIA, data subjects possess the right to request adjustments or deletions[46] of personal data that are inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or unlawfully acquired.[47] Upon receiving such a request, the responsible party must promptly take suitable actions, such as

[33] ibid.
[34] S5 of POPIA
[35] S5 of POPIA states that "personal information may only be processed for specific, explicitly defined purposes compatible with the original reason for its collection."
[36] S19 of POPIA requires responsible parties (entities processing personal information) to secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage, or unauthorised access.
[37] S9 of POPIA.
[38] S14 of POPIA.
[39] S14(1)(a) of POPIA.
[40] S14(1)(d) of POPIA.
[41] S14(3)(b) of POPIA.
[42] S14(4) of POPIA.
[43] S14(6)(a) of POPIA.
[44] S14(7) of POPIA.
[45] S14(8) of POPIA.
[46] S24(1)(a) of POPIA.
[47] Ibid.

rectifying the information,[48] expunging it,[49] providing evidence to corroborate the information,[50] or appending an indication of the requested correction if agreement cannot be achieved.[51] If the rectification affects decisions made about the data subject, the responsible party should inform pertinent parties who have received the personal information about the modifications made.[52] Furthermore, the responsible party is obligated to communicate the measures undertaken in response to the data subject's request, ensuring transparency and accountability under the POPIA.[53]

2.5 Consent and Transparency

The bank has an implicit consent[54] requirement. In order for consent to be considered valid, transparency must be a central theme.[55] In order to adhere to the transparency requirement and ensure valid consent, the bank must obtain voluntary, specific, and informed consent from the data subject.[56] This involves clearly communicating the purposes for data processing and obtaining consent for each specific purpose.[57] The determination derived from section 18(1)(c) unequivocally states that broad consent for utilising personal information will not legitimise the processing of such information.[58] While the duty of confidentiality traditionally mandated confidentiality, POPIA introduces a more explicit consent-driven model.[59]

Section 11 of POPIA imposes several requirements on banks regarding the processing of personal information.[60] Consent must first be given by a data subject or a competent person (if the data subject is a child) before personal information can begin to be processed.[61] The onus is upon banks to get consent from data subjects and to ensure that it is explicit consent for the processing of their personal information.[62] Banks must ensure that they are complying with the legal requirements being imposed on them by legislation.[63]

---

[48] S24(2)(a) of POPIA.
[49] S24(2)(b) of POPIA.
[50] S24(2)(c) of POPIA.
[51] S24(2)(d) of POPIA.
[52] S24(3) of POPIA.
[53] S24(4) of POPIA.
[54] S1 of POPIA defines consent as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information."
[55] De Stadler & Esselaar (see note 8 above) 15.
[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] S11 of POPIA contains provisions on consent, justification and objection.
[60] Ibid.
[61] S11(1)(a) of POPIA.
[62] Ibid.
[63] S11(1)(c) of POPIA.

Personal information processing is permissible if it safeguards a genuine concern of the data subject, is vital for the effective fulfillment of a public legal duty by a public body or is essential for advancing the legitimate concerns of the responsible entity or another party.[64] Banks have the prerogative to manage personal information based on legitimate interests but must carefully assess and harmonise these interests with the entitlements and liberties of data subjects.[65]

Data subjects retain the right to revoke their consent at any given moment.[66] However, withdrawing consent does not impact the lawfulness of processing carried out before or under other lawful reasons.[67] In addition, data subjects can object to the processing of personal information if it is based on legitimate interests, public law duty, or the legitimate interests pursued by the responsible party or a third party.[68] Should such an objection arise, the responsible party, including banks, is no longer authorised to process the contested personal information.[69] Essentially, Section 11 of POPIA sets forth the criteria for how banks can handle personal information, emphasising the importance of consent, contractual necessity, legal obligations, and legitimate interests while safeguarding the rights of data subjects.[70]

Litigation naturally involves revealing information.[71] In law, this is a common occurrence, but when information is brought up in court, it needs to be directly relevant to the case.[72] The introduction of POPIA has granted data subjects the right to grant consent in order for their information to be processed and shared.[73] Undoubtedly, this right will be utilised as a legal defense to prevent the disclosure of a data subject's information.[74] One such instance occurred in the case of *Divine Inspiration Trading 205 (Pty) Ltd and Another v Gordon and others.*[75] This case deals with medical records but is relevant to this dissertation as it deals with instances when the data subjects' rights to consent to the disclosure of information are limited.[76]

---

[64] S11(1)(d-f) of POPIA.
[65] S11(1)(f) of POPIA.
[66] S11(2)(b) of POPIA.
[67] Ibid.
[68] Ibid.
[69] S11(4) of POPIA.
[70] S11 of POPIA.
[71] R Bhoora & A Hinckemann-Dlamini , 'POPIA: Litigants, is your personal information protected?' (Fasken, 25 February 2022) available at <https://www.fasken.com/en/knowledge/2022/02/25-popia-litigants-is-your-personal-information-protected> accessed on 4 February 2024.
[72] Ibid.
[73] S14 of POPIA.
[74] Bhoora & Hinckemann-Dlamini (note 71 above).
[75] 2021 (4) SA 206 (WCC).
[76] Bhoora & Hinckemann-Dlamini (note 71 above).

At the core of the case was an application seeking an order compelling medical practitioners to furnish the medical records of the first respondent to both the applicants and the court.[77] The application revolved around a subpoena duces tecum, a form of subpoena under Rule 38(1) of the Uniform Rules of Court, requiring witnesses to produce relevant documents for the proceedings.[78] The medical records were sought under this rule.[79] However, the medical practitioners declined disclosure. They based this on provisions of the National Health Act[80] and Ethical Rules of Conduct,[81] which do not allow disclosure without a patient's consent.[82] Disclosure was further barred due to the patient invoking their rights under section 11 of POPIA, which would require the patients' consent (in their capacity as a data subject) before personal information can be processed.[83]

The court ruled that relevant health legislation and ethical codes allowed disclosure if mandated by law, and the subpoena constituted 'law' under Rule 38.[84] Furthermore, the court emphasised the significance of the information that was being sought as it would constitute vital evidence.[85] The court also referenced sections of POPIA, including section 12(2)(d)(iii) permitting data collection from sources other than the data subject for court proceedings, and section 15(3)(c)(iii) allowing further processing of collected personal information if essential for court proceedings.[86] Ultimately, the court held that POPIA was not intended to conflict with discovery rules or evidence procurement via subpoenas under Rule 38, indicating that court rules may override protective provisions, offering data subjects limited safeguarding.[87] The case demonstrates that courts may disregard the rights raised under POPIA if the personal information needed is indeed materially relevant to the court proceedings.[88]

2.6 Data Security Measures[89]

Banks are required to implement suitable technical and organisational measures to uphold the integrity and confidentiality of personal information.[90] These measures aim to prevent the loss, damage, or unauthorised destruction of personal information, as well as unlawful access to or processing of such

[77] *Divine Inspiration Trading 205 (PTY) LTD and Another v Gordon and others* 2021 (4) SA 206 (WCC) 206.
[78] Ibid.
[79] *Divine Inspiration Trading 205 (PTY) LTD* (note 77 above) 215.
[80] National Health Act 61 of 2003 (NHA).
[81] Ethical Rules of Conduct for Practitioners Registered under the Health Professions Act 56 of 1974.
[82] *Divine Inspiration Trading 205 (PTY) LTD* (note 77 above) 211.
[83] *Divine Inspiration Trading 205 (PTY) LTD* (note 77 above) 207.
[84] *Divine Inspiration Trading 205 (PTY) LTD* (note 77 above) 213.
[85] *Divine Inspiration Trading 205 (PTY) LTD* (note 77 above) 217.
[86] *Divine Inspiration Trading 205 ((PTY) LTD* note 77 above) 215.
[87] Ibid.
[88] Bhoora & Hinckemann-Dlamini (note 71 above).
[89] S19 of POPIA.
[90] Ibid.

information.[91] The responsible party must take reasonable actions to meet this obligation.[92] These actions include identifying foreseeable internal and external risks, establishing and maintaining appropriate safeguards against these risks, regularly verifying the effectiveness of these safeguards, and ensuring continuous updates to address new risks or deficiencies.[93]

Additionally, the responsible party should adhere to generally accepted information security practices and procedures, whether applicable at a broad level or mandated by specific industry or professional regulations.[94]

2.7 Data breach notification[95]

Section 22 of POPIA mandates the responsible party to promptly notify both the Regulator and the data subject when there are reasonable grounds to suspect unauthorised access to personal information.[96] This notification must be made as soon as possible after the compromise discovery.[97] Delay in notifying the data subject is permitted only under certain circumstances.[98] The written notification to the data subject can be communicated via mail, email, website, or news media[99] and must provide sufficient information for protective measures, including potential consequences, actions taken, recommendations, and, if known, the identity of the unauthorised person.[100]The Regulator holds the authority to instruct responsible parties to publicise any compromise if it believes such publicity would protect affected data subjects.[101]

III. POPIA AND THE ROLE OF THE INFORMATION REGULATOR IN SAFEGUARDING PRIVACY

POPIA and the banking duty of confidentiality are intertwined in their focus on safeguarding individuals' privacy,[102] but they operate within different legal frameworks. POPIA is a comprehensive data protection legislation that establishes conditions for the lawful and

---

[91] Ibid.
[92] Ibid.
[93] S19(2)(a-d) of POPIA.
[94] S19 of POPIA.
[95] S22 of POPIA.
[96] S22(1)(a)(b) of POPIA.
[97] S22(2) of POPIA.
[98] S22(3) of POPIA states "The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned."
[99] S22(4) of POPIA.
[100] S22(5) of POPIA.
[101] Ibid.
[102] Preamble of POPIA; see also JD Mujuzi 'Bank Secrecy: Implementing the Relevant Provisions of the United Nations Convention against Corruption in South Africa' in B Martin & R Koen *Law and justice at the dawn of the 21st century: Essays in honour of Lovell Derek Fernandez* University of Western Cape, (2012) 117- 118.

responsible processing of personal information.[103]Although it does not specifically target the banking duty of confidentiality, POPIA's primary objective is to safeguard individuals' privacy by overseeing the management of their personal information.[104] One of the ways POPIA does this is through the establishment of the information regulator.[105] The creation of the Information Regulator is authorised under section 39 of POPIA.[106]

This section establishes the Information Regulator as an independent body with the authority to exercise its functions and powers independently and without fear, favor, or prejudice.[107] The purpose behind the creation of the Information Regulator is multifold. Firstly, it seeks to ensure that the processing of personal information is done lawfully and responsibly, safeguarding individuals' privacy rights.[108] This involves monitoring how organisations collect, use, store, and share personal data, ensuring that they adhere to the principles of POPIA.[109] Secondly, the Information Regulator is tasked with promoting access to information,[110] which is vital for transparency and accountability within both public and private sectors.[111] Thirdly, the regulator serves as a regulatory authority with investigative and enforcement powers.[112] It has the authority to receive complaints[113] and conduct investigations.[114] The information regulator is allowed to resolve disputes through mediation and conciliation.[115]

IV. REGULATIONS RELATING TO POPIA

In December 2018, the Information Regulator released the 'Regulations Relating to the Protection of Personal Information'[116] pursuant to section 112(2) of POPIA.[117] The regulations provide various standardised forms that individuals and organisations can utilise when carrying out specific actions in accordance with POPIA. Among the key provisions, the regulations outline procedures for objecting to

[103] POPIA Chapter 3: Conditions of Lawful Processing outlines eight key conditions that must be met for the processing of personal information to be considered lawful. These conditions aim to ensure that personal information is handled responsibly, ethically, and with due regard for data subjects' rights.
[104] Preamble of POPIA.
[105] S39 of POPIA.
[106] Ibid.
[107] S39(b) of POPIA.
[108] S40(1)(a)(i) of POPIA.
[109] S40(b) of POPIA.
[110] S40(1)(a)(ii) of POPIA.
[111] S40(1)(a)(v) of POPIA.
[112] S40(1)(d)(i) of POPIA.
[113] Ibid.
[114] Ibid.
[115] Section 40(d)(iii) of POPIA.
[116] Department of Justice and Constitutional Development (2018, December 14) Regulations Relating to the Protection of Personal Information. Government Gazette No. 42110.
[117] S112(2) of POPIA.

personal information processing[118] and requesting corrections or deletions of records.[119] They delineate the duties of information officers, stressing the importance of impact assessments.[120] Moreover, the regulations establish guidelines for the issuance of industry codes of conduct [121] and obtaining consent for electronic direct marketing.[122] They also detail protocols for lodging complaints and the Regulator's role as a conciliator during investigations.[123] Additionally, the regulations mandate the Regulator to notify affected parties during complaints or investigations[124] and to inform them of assessments[125] or requests from third parties,[126] ensuring transparency and accountability throughout the process.

V. CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL INFORMATION BY THE BANKING INDUSTRY

Section 60 of POPIA grants authority to the Information Regulator to issue codes of conduct,[127] ensuring compliance with the lawful processing of personal information. These codes must encompass or functionally equate to all conditions stipulated in POPIA, prescribing their application within specific sectors.[128] The scope of the application can target specified information, bodies, activities, or industries.[129] The codes should outline measures for information matching programs and the protection of data subjects' legitimate interests, especially in automated decision-making.[130] In essence, section 60 enables customised and evolving frameworks for lawful data processing across diverse sectors, with regulatory oversight and a commitment to personal information protection.[131]

The Banking Association of South Africa submitted its code of conduct to the information regulator in 2022.[132] The code deals explicitly with how banks will now handle the processing of personal information in order to comply with the obligations placed on it by POPIA.[133] The code establishes clear guidelines for the lawful processing of personal information, aligning with

---

[118] Regulations Relating to the Protection of Personal Information (see note 116 above) S2.
[119] Regulations Relating to the Protection of Personal Information (see note 116 above) S3.
[120] Regulations Relating to the Protection of Personal Information (see note 116 above) S4.
[121] Regulations Relating to the Protection of Personal Information (see note 116 above) S5.
[122] Regulations Relating to the Protection of Personal Information (see note 116 above) S6.
[123] Regulations Relating to the Protection of Personal Information (see note 116 above) S7.
[124] Regulations Relating to the Protection of Personal Information (see note 116 above) S12.
[125] Regulations Relating to the Protection of Personal Information (see note 116 above) S8.
[126] Regulations Relating to the Protection of Personal Information (see note 116 above) S11.
[127] S60(1) of POPIA.
[128] S60(2)(a)(b) of POPIA.
[129] S60(3)(a)(b)(c)(d) of POPIA.
[130] S60(4)(a)(i)(ii) of POPIA; see also S60(4)(b)(c); The provision for periodic review by the Regulator emphasises adaptability, acknowledging the dynamic nature of data protection, while the requirement for code expiration ensures ongoing relevance and updates.
[131] S60 of POPIA.
[132] Department of Justice and Constitutional Development, "Notice is hereby given of the issuing of the Code of Conduct for the Banking Sector in terms of section 62(1) of the Protection of Personal Information Act, 2013 (1 of 2013)," Government Gazette No. 47257, General Notice 1030 of 2022, 7 October 2022.
[133] Code of Conduct (note 1 above)

the conditions specified in Chapter 3 of POPIA. The codes provide specific obligations of the member banks since a bank can act in many capacities, such as a responsible party,[134] an operator,[135] or a jointly responsible party[136] when processing personal information.[137] A bank acts as an operator or as a jointly responsible party when they form part of group companies that offer services that does not fall within the financial scope of banks, namely insurance, roadside assistance, and telecommunication.[138]

Member banks operate compliance functions governed by compliance frameworks.[139] These frameworks are designed to identify, manage, monitor, and report compliance risks, including those related to POPIA.[140] Regulatory risk universes are compiled, and risk management plans are established to address any compliance gaps.[141]

The code includes information officer oversight in accordance with POPIA. The information officer role helps in embedding POPIA compliance within the organisational structure of the bank.[142] Member banks must undertake to create a governance structure that ensures acceptable leadership, where the corporation operates responsibly and generates sustainable results that align with the conditions stipulated in POPIA.[143] The code explicitly outlines principles for processing limitation, facilitating processing in a lawful manner that is in compliance with POPIA.[144] It highlights the importance of "processing personal information that is adequate, relevant, and not excessive for the stated purpose".[145]

Member banks commit to having a lawful reasons for processing personal information, including "obtaining consent, fulfilling contractual obligations, complying with legal requirements, protecting legitimate interests, and performing public law duties".[146] The code provides specific guidance on obtaining "voluntary, specific, and informed consent".[147] The code provides a list of

---

[134] S1, Part A of POPIA defines a "responsible party" as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information."
[135] S1, Part A of POPIA defines "operator" as "a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party."
[136] Code of Banking Practice (note 1 above)
above) clause 2.3.22 defines "responsible party"/"we"/"us", for purposes of this Code, a bank which is a member of BASA and which, alone or in conjunction with others (as joint responsible parties), determines the purpose of and means for processing personal information.
[137] Code of Conduct (note 1 above) Clause 1.3.
[138] Ibid.
[139] Code of Conduct (note 1 above) Clause 4.2.3.
[140] Code of Conduct (note 1 above) Clause 17.2.
[141] Ibid.
[142] Ibid.
[143] Ibid.
[144] Code of Conduct (note 1 above) Clause 3.
[145] Code of Conduct (note 1 above) Clause 4.
[146] Code of Conduct (note 1 above) Clause 4.2.3-4.2.6
[147] Code of Conduct (note 1 above) Clause 4.2.1.

legitimate interests, demonstrating how the banks must balance their interests with the protection of personal information.[148]

The code provides specific examples of how the processing of personal information is required in the context of financial services, such as risk management, credit assessment, and compliance with financial laws.[149] Member banks must implement risk management plans to mitigate compliance risks.[150] The compliance function monitors the adequacy and effectiveness of controls relevant to POPIA, ensuring continuous improvement.[151]

In case of control gaps, agreed-upon actions are documented to target areas that are inadequate in complying address with POPIA.[152] The code of conduct serves as a practical and strategic framework for member banks to implement measures that align with the principles of POPIA.[153] The Code does not specifically mention the duty of confidentiality, but it does mention how the bank will secure the confidentiality of the customers' information by taking measures to prevent the "loss, damage, and unauthorised access to customers' information".[154] This code of conduct actively demonstrates how the bank's duties and processes have had to change to comply with POPIA.

VI. BANKING OBLIGATIONS UNDER THE DUTY OF BANKING CONFIDENTIALITY AND POPIA

The obligations imposed on banks vary in scope, emphasis, and legal prerequisites between the duty of banking confidentiality and POPIA. This section provides a comparative examination of the duties assigned to banks within these two frameworks.

The duty of banking confidentiality primarily focuses on safeguarding a customer's financial information and maintaining the confidentiality of transactions and account details.[155] The case of *Tournier*[156] clarified the scope to which the duty of confidentiality applies. According to Atkin LJ, the bank secrecy rule not only encompasses the customer's account but also extends to include the balance of the account.[157] Furthermore, Atkin LJ emphasised that this rule applies not only to the account itself but also covers transactions processed through the account and any associated securities and persists even after the account is closed or the customer ceases to be active with the bank.[158]

---

[148] Code of Conduct (note 1 above) Clause 4.2.4
[149] Code of Conduct (note 1 above) Clause 4.2.3 (iii-vi)
[150] Code of Conduct (note 1 above) Clause 4.2.3 (vi)
[151] Code of Conduct (note 1 above) ibid.
[152] Code of Conduct (note 1 above) Clause 4.2.3.
[153] Code of Conduct (note 1 above) Clause 1.5
[154] Code of Conduct (note 1 above) Clause 8.3.1.1
[155] *Tournier v National Provincial Union Bank of England* [1924] 1 KB 461 (CA) 470.
[156] Ibid.
[157] CH Smith 'The Bankers Duty to Secrecy' (1979) 1 *Modern Business Law* 24.
[158] Ibid 26.

Additionally, Atkin LJ clarified that the bank confidentiality rule encompasses information obtained not only from the customer's account but also from external sources, encompassing details provided by the customer and information relayed to the bank from other sources regarding the customer.[159]

Atkin LJ emphasised that disclosure of a bank customer's information to other banks or third parties is permissible only if there is a justifiable reason, either implied or express consent from the customer.[160] The duty of confidentiality is generally considered ongoing, persisting even after the termination of the banking relationship,[161] with exceptions allowing disclosure in certain instances.[162]

On the other hand, POPIA, as a modern data protection framework, encompasses a broader range of information. It aims to protect the privacy and personal information of individuals when their information is being processed.[163] The focus of POPIA is on the lawful and responsible processing of personal information, ensuring transparency, and giving individuals control over their data.[164] The regulation under POPIA is statutory, with specific provisions outlining the lawful processing of personal information.[165] POPIA governs the entire lifecycle of personal information, from collection[166] to processing[167] and, if necessary, deletion.[168]

While both the duty of banking confidentiality and POPIA share common principles of ensuring the confidentiality and security of sensitive information, as demonstrated above, each differs in its scope, legal basis, and the nature of the information covered. The duty of banking confidentiality is not typically governed by a single statutory law like the POPIA but is instead a combination of common law,[169] legislation,[170] and contracts.[171] Banks will be required to navigate and comply with both frameworks to ensure the confidentiality and security of customer information.

In the bank-customer relationship, the definition of the term "customer" typically refers to individuals or entities who have an account or engage in transactions with the bank.[172] These individuals entrust their personal and financial information to the bank during their banking activities.

---

[159] Smith (note 157 above) 24.
[160] *Tournier* (note 155 above) 473.
[161] *Tournier* (note 155 above) 485.
[162] *Tournier* (note 155 above) 461.
[163] S2 of POPIA.
[164] POPIA Chapter 3 (note 103 above).
[165] S8 - 12 of POPIA outlines conditions for the lawful processing of personal information.
[166] S12 - 18 of POPIA address the conditions for the lawful collection of personal information.
[167] S8 - 11 of POPIA specify conditions for the lawful processing and further processing of personal information.
[168] S24(2)(b) of POPIA.
[169]R Ismail 'Legislative erosion of the banker - customer confidentiality relationship' (2008) 48(2) *SALJ* 3-4.
[170] Mujuzi (note 102 above) 126.
[171] Ibid 117.
[172] M Jones & H Schoeman *An Introduction to South African Banking and Credit Law,* (2006) 2; see also M Hapgood. … et al. *Paget's Law of Banking* 13 ed, (2007) 141.

The reconciliation between the definition of a "data subject" (any person whose personal information is being processed)[173] in POPIA and the concept of a customer in the bank-customer relationship lies in the recognition that customers are a subset of data subjects. While not all data subjects may be customers of a bank, all customers are data subjects whose personal information is subject to protection under POPIA.

VII. HOW DOES POPIA RECONCILE WITH THE DUTY OF CONFIDENTIALITY?

POPIA and the banking duty of confidentiality converge in their dedication to protecting customer information.[174] POPIA is advantageous to customers as it provides greater protection by establishing conditions outlining precise principles and obligations that responsible parties must adhere to.[175]

While the duty of confidentiality primarily restricts banks from disclosing customer information, POPIA extends its scope to cover a broader range of personal data activities.[176] A customer of the bank becomes a data subject when their personal information is collected, stored, or processed by the bank.[177] This transformation underscores the interconnectedness between the duty of confidentiality owed by banks.

Banks must adhere to principles such as lawfulness, fairness, and transparency when processing personal data.[178] Moreover, POPIA empowers data subjects by granting them rights over their personal information, including the right to access, rectify, or delete their data held by banks.[179] This provision enhances transparency and accountability within the banking sector.[180]

Additionally, POPIA introduces mechanisms for data breach notification and enforcement, compelling banks to promptly report breaches[181] and take appropriate measures to mitigate risks and protect customer data.[182] By imposing these requirements, POPIA reinforces the duty of confidentiality and underscores the importance of maintaining the security and integrity of customer information.[183]

---

[173] S1 of POPIA.
[174] Preamble of POPIA ; see also Mujuzi (note 102 above) 118.
[175] S2(2) of POPIA.
[176] S1 of POPIA.
[177] Ibid.
[178] S5 of POPIA.
[179] Ibid.
[180] The Protection of Personal Information Act No. 4 of 2013, Chapter 3: Conditions for Lawful Processing.
[181] S22 of POPIA.
[182] S19(1) (a-b) of POPIA.
[183] S19 of POPIA.

Under POPIA, failure of the responsible party to ensure processing complies with all conditions set out in POPIA constitutes a statutory offense.[184] Section 105 explicitly ensures the protection of account numbers. Section 8 of POPIA sets forth the obligations placed on entities handling personal information, including banks, to ensure the lawful and responsible processing of data. These requirements encompass principles of transparency, accountability, and data minimisation, all critical for upholding customer confidentiality and privacy.

Section 105 delineates unlawful acts by responsible parties concerning the processing of account numbers, imposing strict criteria for evaluating the seriousness of contraventions.[185] It underscores the vital role of responsible parties, such as banks, in safeguarding the sensitive information of account holders and underscores the legal ramifications for breaches of confidentiality and data protection standards.[186] The statutory nature of offenses under POPIA highlights the legislative intent to enforce robust standards for data processing and protection.[187]

VIII. CONCLUSION

This chapter illuminates the intricate relationship between POPIA and the duty of banking confidentiality in South Africa's financial landscape. POPIA is a comprehensive data protection legislation, and as demonstrated above, it complements the longstanding duty of confidentiality imposed on banks.

POPIA introduces explicit conditions for responsible parties to adhere too.[188] The principles and obligations are explicitly defined, and banks have had to make significant changes. This was illustrated in the new code of conduct put forth by BASA to the information regulator.[189] In navigating both frameworks, banks are challenged to adapt to the nuanced changes to ensure the confidentiality and security of customer information in this dynamic regulatory environment.

[184] S8 of POPIA.
[185] S105 of POPIA.
[186] Ibid.
[187] Ibid.
[188] S2(2) of POPIA
[189] Code of Conduct (note 1 above).

CHAPTER 4
RECOURSE AVAILABLE FOR THE BREACH OF BANKING CONFIDENTIALITY

I. INTRODUCTION

This chapter will deal with the duty of confidentiality.

The bedrock of a bankers contractual duty to uphold confidentiality is firmly established in the seminal case of *Tournier*[1]. This pivotal legal precedent unequivocally affirmed a customer's rightful claim to maintain the confidentiality of their financial affairs.[2] However, this entitlement is nuanced, arising either explicitly through a contractual agreement or implicitly from the enduring relationship between a banker and a customer.[3] The duty of confidentiality continues even after the bank-customer relationship has terminated.[4]

This chapter will delve into the potential ramifications for banks when confronted with a breach of the duty of confidentiality. Moreover, it will illuminate the avenues open to customers seeking redress in the aftermath of such breaches. The chapter will also address the recourse available to customers in their capacity as data subjects when POPIA is breached.

II. RECOURSE AVAILABLE

When the duty of confidentiality is breached, avenues for recourse become available.[5] Remedies may include damages for breach of contract,[6] a claim in delict for damages,[7] or obtaining an interdict. These remedies are exemplified through the analysis of case law. Customers can seek damages for breach of contract,[8] as illustrated in the *Turner v Royal Bank of Scotland* case.[9] Additionally, customers may pursue a delictual claim for damages[10] if a bank discloses account details without sufficient justification, as seen in the *Abraham v. Burns*[11] case. However, compensation is granted only if the customer incurs damages due to the disclosure.[12] Alternatively, customers may seek an interdict to prevent unwarranted

---

[1] *Tournier v National Provincial Union Bank of England* [1924] 1 KB 461 (CA) 461.
[2] Ibid.
[3] Ibid.
[4] A Ramdhin 'The Bank- customer Relationship' in R Sharrock (ed) *The Law of Banking and Payment in South Africa* 166; see also Tournier (note 1 above) 473.
[5] R Hooley 'Bankers' references and the bank's duty of confidentiality: when practice does not make perfect' (2000) 59(1) *Cambridge Law Journal* 21.
[6] *Turner v Royal Bank of Scotland Plc* [1999] 2 All E.R. (Comm) 664 (24 March 1999)
[7] *Abrahams v Burns* 1914 CPD 452.
[8] *Turner* (note 6 above).
[9] Ibid.
[10] *Abrahams* (note 7 above) 454.
[11] Ibid.
[12] Ibid.

disclosures,[13] as demonstrated in the *Firstrand v. Chaucer* case[14] and *Stevens and Others v Investec Bank Ltd and Others*.[15] Notably, the application for an interdict must be made in the customer's capacity, according to Schulze, who emphasises their exclusive right to seek relief for such disclosures.[16]

2.1 Breach of contract

Seeking damages for a breach of contract was exemplified in the *Turner v Royal Bank*[17] case. In this case, the circumstances revolved around Mr. Turner, who held accounts at the Royal Bank of Scotland ("the Bank").[18] During the course of Mr. Turner being a customer to the Bank, the Bank responded unfavorably to several status inquiries which were instituted by a third party (another bank) regarding Mr. Turner's "creditworthiness".[19] The Bank based their unfavourable response on the state of Mr. Turner's accounts.[20] Mr. Turner eventually instituted legal proceedings against the Bank, seeking "damages for the breach of its implied contractual duty of confidentiality".[21] Although the Bank acknowledged owing Mr. Turner a duty of confidentiality concerning his accounts, it argued that this duty did not apply when disclosure was made with the "customer's express or implied consent".[22] The Bank argued that "every customer opening an account implicitly agreed to the practice of responding to status inquiries from other banks".[23] Ultimately, Turner lost the case because he couldn't demonstrate any financial loss as a result of the bank's disclosure; therefore, the court did not grant him damages.[24] The court ruled that clients typically understand the general practices of banking, including the right to share information with other banks.[25]

2.2 Delict

An early illustration of a legal case addressing the duty of confidentiality in South Africa is *Abrahams v Burns*.[26] In this case, the plaintiff, an attorney representing a customer in a compromise with creditors,

---

[13] *Firstrand Bank Limited v Chaucer Republications (Pty) Limited and Another* [2008] 2 All SA 544 (C) 13.
[14] Ibid.
[15] *Stevens and Others v Investec Bank Ltd and* Others (2012/32900) [2012] ZAGPJHC 226 (25 October 2012).
[16] H Schulze 'Confidentiality and secrecy in the bank-customer relationship' (2007) 15(3) *Juta's Business Law* 124.
[17] *Abrahams* (note 7 above).
[18] Hooley (note 5 above) 21.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] 'The Legal Consequences of the Unlawful Transfer of Personal Client Data to Third Parties: UK Case Study' (*ELTOMA*, 14 May 2018) available at <https://www.eltoma-global.com/knowledge-base/the-legal-consequences-of-the-unlawful-transfer-of-personal-client-data-to-third-parties-uk-case-study> accessed on 4 February 2024.
[25] Ibid.
[26] *Abrahams* (note 7 above) 452.

faced financial constraints to fulfill an agreed-upon payment of 60 euros to the customer's creditors.[27] Seeking assistance, the plaintiff approached the bank, and the acting banking manager, the defendant, agreed to advance the necessary funds based on specified security.[28] Subsequently, the plaintiff, in the presence of a third party, tendered the total debt amount of 150 euros to the defendant, who also represented the plaintiff's creditors.[29] The plaintiff later claimed damages,[30] alleging that the defendant insulted and defamed him by disclosing his account's state to an unauthorised third party, leading to unwarranted damages.[31]

The defendant contended that a banker is not obligated to maintain confidentiality regarding a customer's accounting records, asserting that such a duty, if recognised, would constitute a breach of contract rather than a delictual claim.[32] The defendant justified his actions as an agent, seeking immunity from personal breach of contract claims.[33] Given the absence of a South African precedent, the court, guided by English law, held that a banker could be held liable for damages if, without sufficient reason, they disclosed a customer's account details to a third party, resulting in harm to the customer.[34] The court clarified that a banking manager revealing customer account information to a third party could be sued in delict, contrary to the defendant's argument.[35]

Searle J, the presiding judge, articulated the principle in the following obiter dictum:

> "The rule … is that a banker will be liable for any actual damage sustained by his customer in consequence of an unreasonable disclosure to a third party of the state of his account... I incline to the view that the rule which would now be adopted according to the authorities in English Courts is that a banker would be liable if he, without sufficient reason, disclosed the state of a customer's account to a third party and damage resulted." [36]

Based on this statement, it can be understood that a banker would be liable for actual damages suffered by a customer due to an unreasonable disclosure of their account to a third party.[37] Despite acknowledging doubt and moral considerations surrounding the duty not to disclose, the court

[27] *Abrahams* (note 7 above) 453.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] *Abrahams* (note 7 above) 454.
[36] Ibid.
[37] Ibid.

aligned with English law, emphasising a banker's liability when unwarranted disclosure leads to customer damages.[38]

Abrahams v Burns[39] underscores the recognition of a bank's duty of confidentiality to its customers, derived from English law, forming the basis for similar obligations imposed on South African banking institutions. Based on this decision, it can be concluded that a South African banker may be held liable for disclosing a customer's account details without sufficient cause. If a customer suffers damages from the disclosure, they will be able to sue the bank in delict.[40]

Willis[41] echoes the court's decision, asserting that a South African banker may be held liable if they disclose a customer's account details to a third party without adequate justification, resulting in damages for the customer.[42] The duty of confidentiality was reaffirmed in *GS George Consultants and Investments (Pty) Ltd and Others v Datasys (Pty) Ltd*.[43]As per the court's explanation, the bank is accountable for any damages incurred by its customers as a result of an unjustified disclosure of the customer's personal information to a third party.[44]

2.3 Interdict

In cases when a customer wishes to restrain a bank from disclosing their personal information, they can seek an interdict,[45] and an interdict can be sought if the disclosure has yet to occur.[46]

Firstrand Bank Ltd v Chaucer Publication (Pty) Ltd[47] sought an interdict against Noseweek Magazine's publisher and editor, Welz.[48] The application arose from articles in Noseweek Magazine alleging certain unsavory banking practices by Firstrand.[49] The published articles included information about Firstrand customers and their local and offshore trusts, leading to allegations of defamation against Firstrand and its representatives.[50]

Firstrand sought a petition for an interdict to prevent Noseweek Magazine from disclosing specific names.[51] In a supporting affidavit, Firstrand expressed its intention to protect itself

[38] *Abrahams* (note 7 above) 456 - 457.
[39] *Abrahams* (note 7 above).
[40] *Abrahams* (note 7 above) 454.
[41] N Willis *Banking in South African Law* (1981) 476.
[42] Ibid.
[43] *GS George Consultants and Investments (Pty) Ltd v Datasys (Pty) Limited* 1988 3 SA 726 (W).
[44] Ibid.
[45] *Stevens and Others v Investec Bank Ltd and Others* (2012/32900) [2012] ZAGPJHC 4.
[46] *Firstrand Bank Ltd* (note 13 above) (An interdict was sought thus preventing the disclosure of information).
[47] Ibid.
[48] *Firstrand Bank Ltd* (note 13 above) 13.
[49] *Firstrand Bank Ltd* (note 13 above) 4.
[50] *Firstrand Bank Ltd* (note 13 above) 13.
[51] Ibid.

and its customers from defamation, protect the secrecy of confidential information in which both Firstrand and its customers held vested interests, and uphold its constitutional privacy rights.[52] The application was presented in the interest of Firstrand as the applicant and a class of individuals comprising Firstrand's customers and their trusts, as outlined in the court documents.[53]

Firstrand stated that it had "real and substantial interest" and the "necessary locus standi" to apply for an interdict in its interests and those of a class of persons (those persons being Firstrand customers and their trusts, which were listed in the article).[54] The court did not grant the interdict because it did not believe that Firstrand had the necessary locus standi and substantial interests in the matter.[55] One of the reasons the application was rejected is because Firstrand based its real and substantive interests on the duty of confidentiality that arises from the banks' contractual relationship with the customer.[56] However, it was determined that while the responsibility to maintain confidentiality lies with the bank, the privilege of preventing the disclosure of its transactions with the bank rests with the customer.[57] Traverso DJP held "that the privilege not to have the details of its dealings with the bank disclosed belonged to the client, and only the client could invoke this privilege and insist that the bank maintain confidentiality".[58]

The right to privacy was a private right, and each individual named could have applied for an interdict to stop the defamatory matter.[59] This means that the bank did not need to apply for the interdict for itself and its customers.[60] The court also stated that publishing the fact that someone is a customer of a bank does not amount to an attack on *Firstrand's* right to privacy, and common law did not recognise class actions, therefore, the bank did not have the necessary locus standi to bring the application to the court, and the interdict could not be granted.[61]

In *Stevens and Others v Investec Bank Ltd and Others,*[62] the applicants sought an interdict against the respondents. The interdict served to preserve bank confidentiality pending the finalisation of the review proceedings initiated by the applicants.[63]

---

[52] *Firstrand Bank Ltd* (note 13 above) 14.
[53] Ibid.
[54] Schulze (note 16 above) 122.
[55] Schulze (note 16 above) 124.
[56] Ibid.
[57] Schulze (note 16 above) 124.
[58] *Firstrand Bank Ltd* (note 13 above) 12-13.
[59] *Schulze* (note 16 above) 124.
[60] Ibid.
[61] Ibid.
[62] *Stevens* (note 15 above).
[63] Ibid 4.

In simple terms, the case involves a group of individuals and entities (applicants) who were concerned about their privacy and banking information. Members of the South African Police Services (SAPS) sought and obtained subpoenas under section 205 of the Criminal Procedure Act to gather information,[64] including loan applications, financial statements, and property valuations, from three banks (respondents).[65]

The applicants believed that the subpoenas were obtained as part of a smear campaign against them orchestrated by their competitors.[66] They argued that certain members of SAPS were working inappropriately with private investigators, abusing their authority, and violating the law.[67] The applicants filed a court application to review and set aside the decision to issue the subpoenas.[68] In the meantime, they sought an interim order (interdict) to protect their privacy.[69] The court granted the interdict,[70] which means the documentation (which contains confidential banking details) obtained through the subpoenas is sealed and kept safe by the court registrar.[71] Neither the respondents nor the applicants can access these documents during the review process.[72] The respondents (the three banks) were interdicted from disclosing any information or document requested under the subpoenas to other parties.[73]

III. RECOURSE AVAILABLE UNDER POPIA

3.1 Instituting a claim

Section 99 of POPIA stipulates that a data subject or the Regulator (upon the data subject's request), can file a lawsuit for damages in court against a responsible party if they violate a provision contained in section 73.[74] Legal action can be instituted regardless of whether the violation of section 73 occurred intentionally or negligently. Section 73 establishes the grounds for a claim regarding interference with the protection of a data subject's personal information.[75] This includes any violation of the conditions required for the lawful processing of personal information,[76] "non-compliance with sections 22, 54, 69, 70, 71, or 72 of the Act",[77] and "breach of a code of conduct that is rightfully issued under section

[64] *Stevens* (note 15 above) 1.
[65] *Stevens* (note 15 above) 2.
[66] *Stevens* (note 15 above) 5.
[67] *Stevens* (note 15 above) 5 – 6.
[68] *Stevens* (note 15 above) 3.
[69] *Stevens* (note 15 above) 4.
[70] *Stevens* (note 15 above) 10-11.
[71] *Stevens* (note 15 above) 10.
[72] *Stevens* (note 15 above) 11.
[73] ibid.
[74] S99(1) of POPIA.
[75] S73 of POPIA.
[76] S73(a) of POPIA.
[77] S73(b) of POPIA.

60 of POPIA."[78]

This provision works hand in hand with section 99, as it defines what will be considered interference, and section 99 explains what remedies are available should interference occur.[79] It offers a pathway for a data subject to pursue legal recourse against a responsible party for neglecting to safeguard personal information.[80] It also delineates the circumstances that lead to a legitimate claim against a responsible party under the Act.

3.2 Compensation

> A court hearing proceeding in terms of subsection (1) may award an amount that is
>
> just and equitable, including—
>
> (a) "payment of damages as compensation for patrimonial and non-patrimonial loss
>
> suffered by a data subject as a result of the breach of the provisions of this Act;
>
> (b) "aggravated damages, in a sum determined in the discretion of the Court;
>
> (c) interest; and
>
> (d) costs of suit on such scale as may be determined by the Court.[81]

When the regulator is the one who starts proceedings (for the data subject) the regulator will be entitled to whatever sum of money was used to institute the claim at court and this can include administration cost.[82]

3.3 Penalties

Violating specific provisions of POPIA may amount to a statutory offense and attract criminal sanctions.[83]Acts such as impeding, obstructing, or unlawfully influencing the Regulator, disregarding an enforcement notice, providing false testimony, or violating lawful conditions for processing personal information pertaining to an account number may result in a fine, imprisonment for up to 10 years or both.[84]

3.4 Administrative fines

Section 109 of the Act deals with administrative fines. It outlines the process by which the Regulator can issue an infringement notice to a responsible party (referred to as the infringer) alleged to have

[78] S73(c) of POPIA.
[79] S73 and s99(1) of POPIA.
[80] S73 of POPIA.
[81] S99(3) of POPIA.
[82] S99 (4) of POPIA.
[83] S107 of POPIA.
[84] Ibid.

committed an offense under the Act.[85] The notice contains specific details such as the name and address of the infringer,[86] particulars of the alleged offense,[87] and the amount of the administrative fine payable,[88] which may not exceed R10 million.[89] The infringer has the option to pay the fine,[90] arrange installment payments with the Regulator,[91] or elect to be tried in court.[92]

The Regulator considers various factors when determining the appropriate fine,[93] including the "nature of the personal information involved",[94] the "duration and extent of the contravention",[95] the "number of data subjects affected",[96] whether the breach raises issues of public importance,[97] the likelihood of significant harm or distress to data subjects,[98] the preventive measures that could have been taken by the responsible party or a third party,[99] any deficiencies in risk assessment or in implementing effective policies and procedures to protect personal information,[100] and the responsible party's history of previous violations under the Act.[101] The Regulator cannot impose an administrative fine if the responsible party has been charged with an offense for the same facts under the Act,[102]and no prosecution can be initiated if the fine has been paid.[103]

IV. CONCLUSION

In conclusion, the breach of the duty of confidentiality can have significant legal consequences for banks, as exemplified by the case of *Abrahams v Burns.*[104] This legal precedent establishes that a banker may be held liable for damages if the disclosure of a customer's account details to a third party, without sufficient justification, results in harm to the customer.[105] This principle is consistently upheld in subsequent cases, such as *GS George Consultants and Investments (Pty) Ltd and Others v Datasys (Pty) Ltd.*[106]

---

[85] S109(1) of POPIA.
[86] S109(2)(a) of POPIA.
[87] S109(2)(b) of POPIA.
[88] Ibid.
[89] S109(2)(c) of POPIA.
[90] S109(2)(d)(i) of POPIA.
[91] S109(2)(d)(ii) of POPIA.
[92] Ibid.
[93] S109(3) of POPIA.
[94] S109(3)(a) of POPIA.
[95] S109(3)(b) of POPIA.
[96] S109(3)(c) of POPIA.
[97] S109(3)(d) of POPIA.
[98] S109(3)(e) of POPIA.
[99] S109(3)(f) of POPIA.
[100] S109(3)(g) of POPIA.
[101] S109(3)(h) of POPIA.
[102] S109(6) of POPIA.
[103] S109(7) of POPIA.
[104] *Abrahams* (note 7 above).
[105] Ibid 456 – 457.
[106] *GS George Consultants and Investments (Pty) Ltd (*note 43 above*).*

Customers, on the other hand, possess avenues for recourse in the face of confidentiality breaches. They are empowered to pursue delictual claims, as well as damages for breach of contract, when their account details are disclosed without adequate justification, causing harm.[107] Furthermore, customers can seek an interdict to prevent unwarranted disclosures, as evidenced in cases like *Firstrand Bank Ltd v Chaucer Publication (Pty) Ltd*[108] and *Stevens and Others v Investec Bank Ltd and Others*.[109]

In terms of POPIA, data subjects (which can include bank customers)[110] can receive payment of damages if there is a breach of the provisions of POPIA, they can also receive aggravated damages but this amount will have to be decided by the Court.[111] Furthermore, violating specific provisions of POPIA may amount to a statutory offense and attract criminal sanctions.[112]

[107] *Abrahams* (note 7 above) 456 – 457.
[108] *Firstrand Bank Ltd* (note 13 above).
[109] Stevens (note 15 above).
[110] S99(1) of POPIA.
[111] S73 of POPIA.
[112] S107 of POPIA.

Chapter 5
CONCLUSION AND RECOMMENDATIONS

This chapter deals with conclusionary statements and recommendations .

The duty of confidentiality was adopted into South African law and recognised through a number of decisions.[1] POPIA impacts the banking industry, including the rights and obligations of banks, data subjects , customers , and regulatory authorities, by creating conditions that provide conditions for the lawful processing of personal information.[2] This dissertation aimed to fill the gap in the existing literature about the duty of confidentiality and its intersection with POPIA. It aimed to do this by answering the following questions:

I. WHAT ARE THE EXCEPTIONS TO THE DUTY OF BANK CONFIDENTIALITY, AND HOW DO THESE EXCEPTIONS IMPACT CUSTOMER PRIVACY AND INFORMATION SECURITY?

Exceptions to the duty of confidentiality within the bank-customer relationship highlight the delicate balance between safeguarding individual privacy and addressing broader public interests.[3] Situations may arise where the public interest takes precedence over the private duty of confidentiality[4] as such, one of the exceptions to the duty of confidentiality is the duty to the public to disclose.[5] This exception is supported by the case of *Firstrand Bank Ltd v Chaucer Publication (Pty) Ltd,*[6] where the bank's responsibility to uphold customer confidentiality was affirmed, yet disclosure was permitted when there was a paramount public interest.[7]

Another exception, the interest of the bank, requires disclosure,[8] which grants banks the authority to disclose confidential information under specific circumstances. For instance, disclosure is permissible when a bank is initiating legal action against a customer for overdraft repayment[9] or upon cession of debt,[10] as illustrated by *Tournier*[11] case and *GS George Consultants*.[12]

---

[1] *Abrahams v Burns* 1914 CPD 452; *Cambanis Buildings (Pty) Ltd v Gal* 1983 2 SA 128 (N)*; GS George Consultants and Investments (Pty) Ltd v Datasys (Pty) Limited* 1988 3 SA 726 (W); Densam (Pty) Ltd v. Cywilnat (Pty) Ltd 1991 (1) SA 100 (A); *Firstrand Bank Ltd v Chaucer Publication (Pty) Ltd 2008 (2) SA 592 (C).*

[2] S2(2) of POPIA.

[3] A Ramdhin 'The Bank- customer Relationship' in R Sharrock (ed) *The Law of Banking and Payment in South Africa* 138.

[4] Ibid.

[5] *Tournier v National Provincial Union Bank of England* [1924] 1 KB 461 (CA) 73; A Itzikowitz & F Malan 'Asset Securitisation in South Africa' (1996) 8 *S. Afr. Mercantile LJ* 182.

[6] *Firstrand Bank Ltd* (note 1 above).

[7] *Firstrand Bank Ltd* (note 1 above) PARA 20.

[8] Itzikowitz (note 5 above) 546 – 547; Ramdhin (note 3 above) 138.

[9] Ramdhin (note 3 above) 139.

[10] *Firstrand Bank* (note 1 above) 60.

[11] *Tournier* (note 5 above).

[12] *GS George Consultants and Investments (Pty) Ltd and Others* (note 1 above).

Express or implied consent of the customer[13] represents another facet of exceptions to confidentiality, wherein customers authorise the bank to disclose personal information for specific purposes.[14] This consent may be explicit or implied, and it plays a crucial role in facilitating banking operations.[15]

The exception of disclosure under compulsion of the law includes legislation such as POCA,[16] FICA,[17] POCDATARA,[18] and PRECCA,[19] which compel banks to disclose information under certain circumstances, primarily aimed at thwarting money laundering, terrorist financing, and corrupt activities.[20] Regarding banking confidentiality, this legislation encroaches upon the duty of confidentiality traditionally upheld by banks.[21] The level of protection previously afforded to bank clients has been significantly diminished due to the introduction of such legislation.[22]

II. HOW DOES THE IMPLEMENTATION OF POPIA INTRODUCE NOVEL OBLIGATIONS AND COMPLIANCE STANDARDS FOR BANKS CONCERNING THE HANDLING AND PROTECTION OF CUSTOMER DATA?

The implementation of POPIA introduces novel obligations and compliance standards for banks concerning the handling and protection of customer data.[23] POPIA impacts the banking industry by delineating the rights and obligations of banks, data subjects (customers), and regulatory authorities.

Under POPIA, the lawfulness of processing personal information is paramount.[24] Section 9 mandates that personal information must be processed lawfully, ensuring it is not excessive and does not infringe on the privacy of the data subject.[25] Banks must adhere to specific, explicitly defined purposes for processing personal information, ensuring transparency and accountability in data processing practices.[26]

Accountability is another crucial aspect outlined in section 8 of POPIA.[27] Banks, as responsible parties, bear the burden of ensuring compliance with the conditions set forth in the Act.[28]

---

[13] Ramdhin (note 3 above) 138.
[14] R Ismail 'Legislative erosion of the banker - customer confidentiality relationship' (2008) 48(2) *SALJ* 6.
[15] N Willis *Banking in South African Law* (1981) 40.
[16] Act 121 of 1998.
[17] Act 38 of 2001.
[18] Act 33 of 2004.
[19] Act 12 of 2004.
[20] Section 37(1) of FICA.
[21] Ismail (note 14 above) 12.
[22] Ibid.
[23] S8 of POPIA.
[24] S9 of POPIA.
[25] Ibid.
[26] S5 of POPIA.
[27] S8 of POPIA.
[28] Ibid.

This includes meticulous adherence to processing conditions and measures to enforce compliance, as well as appointing Information Officers to oversee compliance efforts.[29]

Processing limitation requires banks to assess data collection practices to ensure that personal information collected is adequate, relevant, and not excessive for the intended purposes.[30] Retention and restriction of records, as outlined in section 14, mandate that records should not be kept longer than necessary and must be securely destroyed when no longer needed.[31] Data subject participation grants individuals the right to inquire about, rectify, and erase their data, emphasising transparency and accountability in data processing practices.[32] Consent and transparency requirements necessitate that banks obtain voluntary, specific, and informed consent from data subjects before processing their personal information.[33]

Data security measures require banks to implement suitable technical and organisational measures to uphold the integrity and confidentiality of personal information, preventing unauthorised access or processing.[34] Data breach notification mandates prompt notification to both the Regulator and data subjects in the event of unauthorised access to personal information.[35] The role of the Information Regulator is pivotal in safeguarding privacy rights and overseeing compliance with POPIA.[36] The regulator ensures lawful and responsible processing of personal information, promotes access to information, and serves as a regulatory authority with investigative and enforcement powers.[37]

The Code of Conduct for the processing of personal information by the banking industry provides clear guidelines for banks to comply with POPIA obligations.[38] It emphasises lawful processing, consent, data security, and transparency, ensuring that banks align their practices with the principles of POPIA while safeguarding customer confidentiality.[39] In conclusion, POPIA introduces comprehensive regulations that reshape how banks handle and protect customer data, emphasising transparency, accountability, and data privacy.[40]

---

[29] S40(b) of POPIA.
[30] E De Stadler & P Esselaar *A guide to the Protection of Personal Information Act* (2015) 23.
[31] S40 of POPIA.
[32] S5 of POPIA.
[33] De Stadler & Esselaar (note 30 above) 15.
[34] S19 of POPIA.
[35] S22(1)(a)(b) of POPIA.
[36] S40(1)(a)(i); S40(b); S40(1)(a)(ii) of POPIA
[37] S40(1)(a)(i); S40(b); S40(1)(a)(ii); S40(1)(a)(v) ; S40(1)(d)(i) of POPIA
[38] The Banking Association South Africa Code of Conduct (2021) Clause 1.6.
[39] Code Of Conduct (note 38 above) Clauses 3.4; 4.1 – 4.1.3.
[40] Code Of Conduct (note 38 above) Clause 1.11.

III. TO WHAT EXTENT DOES POPIA COMPLEMENT THE EXISTING BANKING DUTY OF CONFIDENTIALITY, AND HOW DO THESE SYNERGISE TO ENHANCE CUSTOMER PRIVACY AND DATA PROTECTION IN THE FINANCIAL SECTOR?

POPIA and the duty of confidentiality in banking intersect in their shared commitment to safeguarding customer information.[41] POPIA enhances customer protection by establishing clear principles and obligations for responsible parties, including banks, to follow in managing personal data.[42]

While the duty of confidentiality traditionally limits banks from disclosing customer information, POPIA broadens its scope to encompass a broader range of personal data activities.[43] Customers become data subjects under POPIA when their personal information is collected, stored, or processed by banks, highlighting the interconnectedness between banking confidentiality and data protection.[44]

Banks must adhere to POPIA's principles of lawfulness, fairness, and transparency when processing personal data.[45] Furthermore, POPIA empowers data subjects by granting them rights over their personal information, including the right to access, rectify, or delete their data held by banks.[46] This provision enhances transparency and accountability in the banking sector.[47]

Moreover, POPIA introduces mechanisms for data breach notification and enforcement, compelling banks to promptly report breaches and take necessary measures to mitigate risks and protect customer data.[48] By imposing these requirements, POPIA reinforces the duty of confidentiality and emphasises the importance of maintaining the security and integrity of customer information. Failure to ensure compliance with POPIA constitutes a statutory offense under section 105, emphasising the seriousness of maintaining confidentiality, particularly regarding account numbers.[49] Section 8 of POPIA outlines the obligations of entities handling personal information, including banks, to ensure lawful and responsible data processing practices.[50] These requirements, including transparency, accountability, and data minimisation, are crucial for upholding customer confidentiality and privacy.

---

[41] Preamble of POPIA ; see also JD Mujuzi 'Bank Secrecy: Implementing the Relevant Provisions of the United Nations Convention against Corruption in South Africa' in B Martin & R Koen *Law and justice at the dawn of the 21st century: Essays in honour of Lovell Derek Fernandez* University of Western Cape, (2012) 118.
[42] S2(2) of POPIA.
[43] S1 of POPIA.
[44] Ibid.
[45] S5 of POPIA.
[46] Ibid.
[47] S40(1)(a)(v) of POPIA.
[48] Code Of Conduct (note 38 above) Clause 4.2.1.
[49] S105 of POPIA.
[50] S8 of POPIA.

In essence, POPIA and the duty of confidentiality in banking converge to establish robust standards for data processing and protection, ensuring that customer information remains secure and that banks fulfill their obligations to safeguard privacy and confidentiality.[51]

IV. WHAT LEGAL MECHANISMS AND REMEDIES EXIST IN CASES OF BREACH OF THE BANK'S DUTY OF CONFIDENTIALITY AND POPIA?

The legal mechanisms and remedies available for individuals and institutions in cases of breach of a bank's duty of confidentiality are multifaceted and often rely on contractual obligations and the relationship between a banker and a customer.[52]

Fundamentally, the obligation of a banker to maintain confidentiality stems from established legal precedents like the *Tournier* case, which solidified a customer's right to expect privacy regarding their financial affairs.[53] This duty is intrinsic to the banker-customer relationship, whether explicitly outlined in a contractual agreement or implied through the nature of their interaction.[54] Importantly, this duty persists even after the termination of the bank-customer relationship.[55]

Instances of breach of confidentiality can result in legal repercussions, as seen in cases like *Turner v Royal Bank*[56] and *Abrahams v Burns*[57]. In *Turner v Royal Bank,*[58] the courts upheld the rights of customers to confidentiality even in the face of implied consent arguments by the bank.[59] Similarly, *Abrahams v Burns* highlighted the liability of banks for disclosing customer account details without sufficient cause, affirming the duty of confidentiality recognised under English law and applied in South Africa.[60]

Moreover, legal remedies such as delictual claims for damages,[61] interdicts,[62] and damages for breach of contract[63] are available to aggrieved parties. Customers may seek damages if a bank's unwarranted disclosure of account details results in harm,[64] as demonstrated in *Abrahams v Burns* and supported by subsequent legal opinions. Interdicts, as exemplified in *Firstrand v Chaucer*

---

[51] Preamble of POPIA(note 41 above) ; Mujuzi (note 41 above).
[52] *Tournier* (note 5 above) 461.
[53] Ibid.
[54] Ramdhin (note 3 above) 135 – 136.
[55] M Hapgood. … et al. *Paget's Law of Banking* 13 ed, (2007) 158.
[56] *Turner v Royal Bank of Scotland Plc* [1999] 2 All E.R. (Comm) 664 (24 March 1999)
[57] *Abrahams* (note 1 above).
[58] *Turner* (note 56 above).
[59] R Hooley 'Bankers' references and the bank's duty of confidentiality: when practice does not make perfect' (2000) 59(1) *Cambridge Law Journal*.
[60] *Abrahams* (note 1 above) 454.
[61] Ibid.
[62] Ramdhin (note 3 above) 164.
[63] *Turner* (note 56 above) 454.
[64] Ramdhin (note 3 above) 164.

and *Stevens and Others v Investec Bank Ltd*, can be pursued to prevent banks from making unwarranted disclosures, albeit customers must do so in their capacity.[65]

Under POPIA, individuals have further avenues for recourse. Section 99(1) empowers data subjects or the Regulator to institute civil actions for damages against responsible parties for breaches of the Act, including non-compliance with specified sections or breach of codes of conduct.[66] Courts may award compensation, including damages and interest, to data subjects for losses suffered due to breaches of POPIA.[67] Moreover, penalties under POPIA can be imposed on parties impeding regulatory processes or violating processing conditions, reinforcing the importance of compliance with data protection standards.[68]

In conclusion, the legal landscape surrounding breaches of a bank's duty of confidentiality is comprehensive, incorporating contractual[69] and delictual remedies.[70] These mechanisms aim to uphold the integrity of banking relationships and ensure the protection of personal information in an increasingly digitised world.

V. CONTRIBUTIONS OF THIS DISSERTATION

This dissertation offers significant insights into the intricate dynamics of confidentiality within the banking sector, particularly within the framework of South African law and its intersection with POPIA. With a primary focus on analysing the duty of confidentiality alongside POPIA, this dissertation delves into how case law has addressed banking confidentiality and personal data protection, as well as the perspectives provided by South African scholars.

Over the years, the duty of banking confidentiality has been instrumental in safeguarding personal information imposing crucial obligations on financial institutions. However, the advent of POPIA has reshaped these duties, underscoring a shared objective of protecting personal data. This dissertation offers clarity on the boundaries of confidentiality obligations by elucidating exceptions to this duty and examining their implications for customer privacy. Moreover, it navigates the intricate interplay between the duty of confidentiality and POPIA, shedding light on how breaches of these standards are addressed.

Central to the findings of this dissertation is the assertion that POPIA complements the duty of confidentiality, enriching the protective landscape for customers and offering viable avenues

---

[65] *Firstrand Bank ltd* (note 1 above) 13*;* see also H Schulze 'Confidentiality and secrecy in the bank-customer relationship' (2007) 15(3) *Juta's Business Law* 122-124.
[66] S99(1) of POPIA.
[67] S99(3); S99 (4) of POPIA.
[68] S107 of POPIA.
[69] Hooley (note 59 above) 21.
[70] *Abrahams* (note 1 above) 454.

for recourse in the event of breaches. By elucidating these intersections and clarifying the evolving legal landscape, this study contributes to a deeper understanding of privacy rights and regulatory compliance within the banking realm.

BIBLIOGRAPHY

Secondary sources

Code of Banking Practice (2012) by the Banking Association of South Africa.

Code Of Conduct For The Processing Of Personal Information By The Banking Industry (2021) by the Banking Association of South Africa.

Currie, I., De Waal, J. and Law Society of South Africa *The bill of rights handbook* 6 ed Cape Town: Juta ,(2013).

De Stadler, E and Paul E *A guide to the Protection of Personal Information Act* Cape Town: Legal Ease Essence Juta, (2015).

Faul, W 'Teoretiese fundering van die bankgeheimnis in die Suid-Afrikaanse reg' (1986) *TSAR* 180.

'FIC ISSUES GUIDANCE NOTE ON ELECTRONIC FUNDS TRANSFERS' (11 April 2023), *Moonstone Information Refinery* at https://www.moonstone.co.za/fic-issues-guidance-note-on-electronic-funds-transfers/, accessed on 5 February 2024.

Hooley, R 'Bankers' References and the Bank's Duty of Confidentiality: When Practice Does Not Make Perfect' (2000) 59(1) *The Cambridge Law Journal* 21–23.

Ismail, R 'Legislative erosion of the banker - customer confidentiality relationship' (2008) 48(2) *South African Law Journal* 3-14.

Itzikowitz, A 'Banker and Customer: The banker's duty of secrecy' (1989) 18 *Businessman's Law* 255.

Jones, M., Schoeman, H. and Schoeman, H *An introduction to South African banking and credit law* Durban: LexisNexis Butterworths, (2009).

Jones, Mariëtte and H. Schoeman. *An Introduction to South African Banking and Credit law*. Durban, South Africa: LexisNexis Butterworths, (2006).

Machokoto, J.G 'The duty of bank confidentiality in South Africa and other jurisdictions such as Zimbabwe: Justifications, judicial limitations and legislative inroads rising from the need to avert crimes' (2018) 1(1) *University of Zimbabwe law Journal* 1-10.

Malan, F. R., Pretorius, J.T, & Du Toit, S. F *Malan on bills of exchange, cheques and promissory notes in South African law* 5 ed Durban: LexisNexis, (2013).

Martin, B & Koen, R (2016). *Law and justice at the dawn of the 21st century: Essays in honour of Lovell Derek Fernandez* University of the Western Cape.

Masete N.T 'The Challenges in Safeguarding Financial Privacy in South Africa' (2012) 7(3) *Journal of International Commercial Law and Technology* 248–259.

Mthembu, M.A 'Marriage of Convenience: Bank-Customer Relationship in the Age of the Internet: A South African Perspective' (2014) 9(1) *Journal of International Commercial Law and Technology* 14-23.

Mujuzi, J.D 'Bank Secrecy: Implementing the Relevant Provisions of the United Nations Convention against Corruption in South Africa' (2016) 1(1) *University of the Western Cape*, 118-139.

Neethling, J ‘The concept of privacy in South African law’ (2005) 122 (1) *South African Law Journal* 18–28.

Ngidi, M ‘The Termination of the Bank-Client Relationship in South African Banking Law’ (2020) 53(1) *De Jure* 54–69.

Paget, J. R Hapgood, M and Slade, R *Law of banking* 13 ed London: LexisNexis, (2007).

Ramdhin, A ‘The Bank-customer Relationship’ in R Sharrock *The law of banking and Payment in South Africa* Claremont: Juta and Company [Pty] Ltd, (2016). 110-166

Roos, A ‘Data protection: explaining the international backdrop and evaluating the current South African Position’ (2007) 124 (2) *South African Law Journal* 400- 437.

Schulze, H ‘Confidentiality and secrecy in the bank-customer relationship’ (2007) 15(3) *Juta’s Business Law* 122-126.

Schulze, W.G ‘Delictual liability of a bank towards its client: a new prominence given to the element of causation: regspraak’ 2006 (4) *Journal of South African Law/Tydskrif vir die Suid-Afrikaanse Reg* 834-839.

Smith, C ‘The banker’s duty of secrecy’ (1979) 1 *Modern Business Law* 24.

'The Legal Consequences of the Unlawful Transfer of Personal Client Data to Third Parties: UK Case Study' (14 May 2018), *Eltoma* at https://www.eltoma-global.com/knowledge-base/the-legal-consequences-of-the-unlawful-transfer-of-personal-client-data-to-third-parties-uk-case-study, accessed on 4 February 2024.

Willis, N *Banking in South African law* Cape Town: Juta, (1981).

Table of Cases:

South African Cases:

Abrahams v Burns 1914 CPD 452

Cambanis Buildings (Pty) Ltd v Gal 1983 (2) SA 128 (N)

Cywilnat v Densam 1989 (3) SA 59 (W)

Densam (Pty) Ltd v. Cywilnat (Pty) Ltd 1991 (1) SA 100 (A)

Di Giulio v First National Bank of South Africa 2002 (6) SA 281 (C).

Divine Inspiration Trading 205 (pty) ltd and Another v Gordon and others 2021 (4) SA 206 (WCC).

First National Bank of SA Ltd v Duvenhage 2006 (5) SA 369 (SCA).

Great Karoo Eco Investments (Edms) h/a Grobbelaarskraal Boerdery v Absa Bank Bpk 2003 (1) SA 222 (W).

GS George Consultants and Investments (Pty) Ltd v Datasys (Pty) Limited 1988 (3) SA 726 (W).

Standard Chartered Bank of Canada v Nedperm Bank Limited 1994 (4) SA 747 (A).

Stevens and Others v Investec Bank Ltd and Others (2012/32900) [2012] ZAGPJHC 226.

Foreign Cases:

California Bankers Association v Schultz 416 US 1974 21

Commissioners of Taxation v English, Scottish and Australian Bank [1920] AC 683

Tournier v National Provincial Union Bank of England [1924] 1 KB 461 (CA)

Turner v Royal Bank of Scotland Plc [1999] 2 All E.R. (Comm) 664 (24 March 1999)

Table of Statutes:

Constitution of the Republic of South Africa, 1996.

Ethical Rules of Conduct for Practitioners Registered under the Health Professions Act 56 of 1974

Financial Intelligence Centre Act 38 of 2001

National Health Act 61 of 2003

Prevention and Combating of Corrupt Activities Act 12 of 2004

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

Protection of Personal Information Act 4 of 2013

Regulations of POPIA

UNIVERSITY OF
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

Miss Kousar Bibi Ahmed (217037893)
School Of Law
Pietermaritzburg

Dear Miss Kousar Bibi Ahmed,

Protocol reference number: 00013755
Project title: The duty of bank confidentiality and the safeguarding of financial privacy.

Exemption from Ethics Review

In response to your application received on 19 August 2021 , your school has indicated that the protocol has been granted **EXEMPTION FROM ETHICS REVIEW.**

Any alteration/s to the exempted research protocol, e.g., Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through an amendment/modification prior to its implementation. The original exemption number must be cited.

For any changes that could result in potential risk, an ethics application including the proposed amendments must be submitted to the relevant UKZN Research Ethics Committee. The original exemption number must be cited.

In case you have further queries, please quote the above reference number.

PLEASE NOTE:
Research data should be securely stored in the discipline/department for a period of 5 years.

I take this opportunity of wishing you everything of the best with your study.

Yours sincerely,

[redacted]----------

Mr Simphiwe Peaceful Phungula
obo Academic Leader Research
School Of Law