UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The Tension between Bank Secrecy and the Combatting of Financial Crime

By

Boikanyo Maloka Diremelo

(14167710)

Submitted in partial fulfilment of the requirements for the degree

Master of Laws (Mercantile Law)

In the Faculty of Law,

University of Pretoria

October 2019

Supervisor: Prof R Brits

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.
2. I declare that this thesis is my own original work. Where other people's work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.
3. I have not used work previously produced by another student or any other person to hand in as my own.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Boikanyo Maloka Diremelo
October 2019

Summary

Financial crime has resulted in serious implications for the socio-economic fabric of South Africa. As an outcome, the duty of secrecy imposed on banking institutions has become more controversial. This is because it has become increasingly difficult to balance the interests of customers, who may be perpetrators or *bona fide* victims of financial crime, against the interests of society as a whole. The common law laid the foundation for the duty of secrecy and confidentiality imposed on banks in the interests of their customers. It is, however, acknowledged by the common law that the duty of secrecy is not absolute but is indeed subjected to limitations. Consequently, the duty may be limited when such limitation is in the interests of the public or the banking institution itself, when the law requires it and when consent for the disclosure of personal information has been given. The duty of secrecy subsists in the constitutional dispensation of South Africa and the fact that it can be limited has been incorporated into South African law. In this regard, the South African legal system acknowledges the common law principle that when limiting the duty of secrecy, there ought to be a ground of justification authorising such an invasion. Therefore, the existence of a statute permitting a limitation of the duty of secrecy, is sufficient cause to compel banks to disclose information concerning a client's account in contravention of the duty of secrecy. One of the rights which are compromised when a bank voluntarily or under compulsion of law discloses private information related to a client's account is the right to privacy contained in section 14 of the Constitution. However, it is acknowledged in section 36 of the Constitution that the constitutional right to privacy can be "limited in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom". While the state guarantees an individual all of the rights contained in the Bill of Rights, the state holds a greater duty to protect the interests of the public. Therefore, a person's right to secrecy and confidentiality cannot be interpreted with such strict legalism that it compromises the interest of the community at large. As such, when a customer of a banking institution is implicated in the perpetration of financial crime, they cannot rely on the duty of secrecy to absolve their accounting records, books and other personal information held by the bank from investigation.

Acknowledgements

Firstly, I would like to thank God for granting me this opportunity, for blessing me with the courage of taking on this journey and the resilience of seeing it through.
I would also like to thank my supervisor, Prof Reghard Brits, for his valuable guidance and input through this mini-dissertation.
Lastly, I would like to thank my grandmother, Jane Matlhodi Mmampyane Diremelo, for her continuous prayers and support throughout this entire process.

Table of content

Chapter 1:
Introduction

When clients entrust their finances to a banking institution, they can reasonably expect their information to be handled with confidentiality. This is because secrecy, specifically in the bank-customer relationship, is regarded as a tacit term of the contract between the two.[1] As a country, South Africa is commonly associated with financial crime. This is largely attributable to its history of inequality and the resultant change in power post 1994.[2]

One of the greatest challenges to combating financial crime in South Africa is the disconnect between the material law as it exists in statutes and the manner in which it manifests on the ground. Our legal system contains a number of laws targeted at financial crime, but very little is done to deter criminals from actually partaking in illegal activities. The inevitable outcome of this is a limited number of perpetrators actually facing prosecution. Through the aid of initiatives like Crime Watch, media exposure and public outrage regarding the impact and implications of financial crime, the subject of financial crimes has garnered greater attention and has compelled government to take action to combat the prevalence of such criminal activity in the Republic.[3]

The internet has created a vibrant marketplace for businesses and consumers to interact but it has also provided criminals with new avenues to commit crimes.[4] Although the internet allows inexpensive, interactive and instant global communications, it does not exist in a legal vacuum. As a result, the internet poses a number of problems in a broad spectrum of legal areas such as freedom of expression, intellectual property, criminal law, contracts and jurisdiction. Moreover, the vulnerability of computer systems and networks to unauthorised users facilitates criminal activity on the Internet.[5]

---

[1] H Schulze 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review For People in Business* 125.
[2] S Powell 'Secrecy Feeds Corruption & Secures Opulence' (2016) 2 *TFM Magazine* 33.
[3] S Powell 'Secrecy Feeds Corruption & Secures Opulence' (2016) 2 *TFM Magazine* 33.
[4] R Stevenson 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1.
[5] R Stevenson 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1.

The theft of information is thus becoming easier for criminals who now have greater access to consumer information stored on databases. Cyber-attacks have increased in regularity and severity as cyber criminals have become more sophisticated and brazen. This has resulted in cyber-crime becoming the fastest growing crime in the world with resourceful crime syndicates preying on millions of unsuspecting victims.[6] Nowadays, perpetrators can use fraudulent e-mails and fake websites to scam unsuspecting victims around the globe. This form of online fraud can be distinguished from physical fraud because of the difficulty to identify and apprehend online fraudsters and the ease with which such crimes can be committed.[7] Consequently, it has become even more difficult to protect the confidentiality of personal information belonging to customers of banking institutions.

Banks play a key role in the perpetuation and the combating of financial crime because most of the money which enters or changes hands in the Republic is done through them. Furthermore, banks are first to observe any irregularities or inconsistencies in any of their client's affairs which may allude to financial crime. The high levels of financial crime in the Republic have made it difficult for banks to safeguard the personal information of their customers. The practice of bank secrecy is one of the ways in which financial crime can be enabled in South Africa. This is because secrecy may provide refuge for perpetrators of financial crime, shielding them from investigation and the possibility of prosecution. Subsequently, bank secrecy has the potential to foster an environment in which financial crime can thrive. However, the duty of secrecy is subjected to limitations which create stumbling blocks for perpetrators of financial crime.

This dissertation assesses the duty of secrecy as it is imposed on banks and the manner in which it aids in the combating of financial crime through an assessment of the duty under common law and its incorporation into South African statutes. The dissertation will also assess the impact of the constitutional right to privacy on the duty of secrecy as the right to privacy is one right which is directly affected by the limitation of the duty of secrecy. Lastly, the dissertation will consider the impact of the duty of

[6] R Stevenson 'Plugging the 1 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1.
[7] R Stevenson 'Plugging the 1 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1.

secrecy in the combating of specific financial crimes, namely, corruption, money laundering and phishing.

Chapter 2:
History of the duty of secrecy

2.1 The common law duty of secrecy

The relationship between a bank and its customers is difficult to classify and subsequently, due to its unusual nature, it has often been classified as *sui generis*.[8] As explained by Smith, the relationship between a bank and its clients is in essence one of a debtor and a creditor. Either party to the relationship can be identified as a debtor or the creditor depending on the circumstances of each case. When a client's account is in credit, the bank will be the debtor. However, when the client's account is overdrawn, it will follow that the bank is the creditor. This relationship is accompanied by certain obligations, which according to Smith, not only distinguish the relationship from the ordinary debtor-creditor relationship but elevate it to *sui generis* status.[9] It is, however, accepted at common law that the duty of secrecy imposed on banks is created by the contract of mandate (*mandatum*).[10]

According to this contract of mandate, the client gives the bank a mandate to perform *bona fide* a plethora of services in conjunction with his or her account.[11] How this ordinarily functions is that money is lent to the bank by such a customer on a current account and the bank in turn incurs the duty to repay the moneys on demand. This is done through the honouring of cheques which may be drawn on the bank by the customer.[12] The services rendered by the bank to its client, however, extend beyond the mere honouring of cheques but also include the collection of cheques, keeping and accounting of the customer's accounts with the bank as well as the payment of stop and debit orders.[13] Amongst these duties of the mandatary, being the bank in this regard, the bank may also possess the obligation to safeguard any confidential information or affairs of the mandatory, being the customer of the bank.[14]

---

[8] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 4
[9] C Smith 'The banker's duty of secrecy' 1 (1979) *Modern Business Law* 24.
[10] H Schulze 'Legislative erosion of the banker-client confidentiality relatopmship" (2007) 15 *The Quarterly Law Review for People in Business* 125.
[11] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 4
[12] H Schulze 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review for People in Business* 125.
[13] H Schulze 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review for People in Business* 125.
[14] H Schulze 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review for People in Business* 125.

This duty not only applies to a bank's current customers but also any clients they may have dealt with in the past.

The common law regards the duty of secrecy as a natural duty emanating from the contractual relationship between the bank and its clients. The duty is therefore considered to be based on a tacit term in the contract between a bank and its clients.[15] However, both parties to the bank-customer relationship may, as an alternative, expressly agree to a term unequivocally stating that the bank will have the obligation to protect the customer's right to privacy as pertaining to such a client's banking affairs.[16] This provision will effectively preclude the bank from sharing any personal information of its clients who may be accused of financial crime, should the obligation arise.

It is important to note that the common law does not regard the duty of secrecy as absolute. In the case *of Tournier v National Provincial & Union Bank of England*[17] the common law duty of confidentiality and secrecy was assessed. Not only did the court in this matter affirm the duty of secrecy imposed on banks but it also composed a list of exceptions under which the duty will not apply. When such circumstances are present, the bank has a duty or may otherwise be permitted to disclose information in conjunction with the affairs of its client.

The following headings define the exceptions which render banking institutions exempt from the duty of secrecy and confidentiality.

2.1.1 Where disclosure is under compulsion by law

This primarily refers to instances pertaining to litigation because such instances, whether expressly or implicitly, require disclosure.[18] When assessing the South African legal system, it is apparent that confidentiality in relation to banking institutions has been treated with the greatest sensitivity and awarded serious attention, particularly in conjunction with money-laundering legislation and with regard to the compulsion-of-law exception. Some statutes enacted with the intent of facilitating this duty include: the Prevention of Organised Crime Act; the Financial Intelligence Centre

[15] H Schulze 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review for People in Business* 122.
[16] H Schulze 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review for People in Business* 122.
[17] [1924] 1 KB 461.
[18] H Schulze 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review for People in Business* 122.

Act; regulations 47 and 48 of the Regulations to the Banks Act; the Financial Advisory and Intermediary Services Act and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act.[19]

2.1.2 Where there is a duty to the public to disclose

This encompasses all cases where the danger to the state or a public duty may supersede the duty of confidentiality which rests on the bank.[20] For instance, this is a valid ground of exception where a bank is aware of an account belonging to a revolutionary body or in the case where a client is suspected of treason.

2.1.3 Where the interests of the bank require disclosure

The law recognizes three instances in which this exception is valid. This includes matters relating to overdraft facilities offered by the bank. Disclosure will therefore be compulsory in the event that a client fails to make good payment on an overdraft due to the bank and the amount due has to be stated in the court documents.[21] Where a bank cedes its rights to sue a customer. According to Scott, where a bank discloses information relating to a customer's affairs when disposing of its personal rights through cession, such a disclosure would be treated as falling under this exception, as the interests of the bank would require disclosure.[22] Lastly, matters relating to suretyship. Disclosure under this heading will be permitted where a bank sues a surety and the state of the initial debtors account must be revealed.[23]

2.1.4 Where the disclosure is made with the express or implied consent of the client

This typically involves instances where a client of the bank gives authority to the bank to provide a third party with certain confidential information pertaining to the client concerned.[24] An example is where a client of the bank applies for credit facilities with a third party, and the third party is given access to the client's personal information.

---

[19] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 4.
[20] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 5.
[21] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 4.
[22] S Scott 'Can a banker cede his claims against his customer' 1 (1989) *South African Mercantile Law Journa*l 248.
[23] C Smith 'The banker's duty of secrecy' 1 (1979) *Modern Business Law* 27.
[24] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 4.

2.2 Recognition in South African law

In the past, when South African courts were faced with a matter that had not yet been decided on in South Africa, they would apply English law. This was the case in most matters related to the banking industry of South Africa as English law was considered to be identical to South African law.[25] The following paragraphs will assess early decisions on the duty of secrecy in South Africa which were influenced by English law.

2.2.1 *Abrahams v Burns*

One of the earliest cases dealing with the duty of confidentiality is *Abrahams v Burns*.[26] In this matter the plaintiff was an attorney who was acting on behalf of his client in respect of a compromise between his client and the client's creditors. The attorney and his client had made an agreement that the attorney would give his client 60 euros which would enable the client to pay his creditors.[27] The problem, however, was that the attorney did not have the money to do this and as a result, he turned to the bank for assistance. The acting banking manager, who was the defendant in the matter, agreed that the bank would advance the money required to the plaintiff on certain security that would be deposited by the plaintiff.[28] A cheque was drawn by the plaintiff and subsequently cashed by the bank. Thereafter, the plaintiff proceeded to tender to the defendant (who was also acting on behalf of the plaintiff's creditors) the full amount of the debt being 150 euros.[29] This was done in the presence of a third party. It was later alleged by the plaintiff that he had been insulted by the defendant who had also attempted to defame the plaintiff by claiming that the plaintiff had maliciously hidden information which was the plaintiff's duty to disclose to the defendant.[30] As a result of these insults, the plaintiff made a claim for damages. The plaintiff further alleged that the defendant had breached his duty of confidentiality owed by a bank to its clients because the defendant had revealed the state of the plaintiffs account to a third party without the consent of the plaintiff.[31] This third party allegedly had no right to the affairs

[25] C Smith 'The banker's duty of secrecy' 1 (1979) *Modern Business Law* 24.
[26] 1914 CPD 452 452.
[27] 453.
[28] 453.
[29] 453.
[30] 453.
[31] 453.

of the plaintiff. Therefore, by reason of this wrongful and unlawful disclosure of his account by the bank, the plaintiff had suffered damages.[32]

In his defence, the defendant argued that a banker is not bound by a duty not to disclose a client's accounting records. Furthermore, if the law recognised such a duty, his conduct would be tantamount to a breach of contract and not a claim in delict.[33] According to the defendant he was acting as an agent and therefore a claim for breach of contract cannot be brought against him personally[34]

At the time which this matter was held, there was no precedent in South African law to inform the judge's decision. Searle J thus had to consider English law in order to reach a decision. According to Searle J, the rule in English law was that a banker would be held liable if he, without sufficient reason, disclosed the customer's account to a third party and his customer suffered damages as a result.[35] It was however unnecessary to determine the legal position on this point. The more important consideration was whether the bank and not the defendant should have been sued and whether this claim could only constitute a breach of contract. It was held that when a banking manager reveals information concerning a client's account to a third party, the plaintiff will be able to sue him in delict.[36] However, according to the court, the alleged defamatory words uttered did not divulge the state of the plaintiff's account as alleged.[37]

Searle J thus says the following in respect of his decision:

> "The… rule is that 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. This seems certainly as far as one is warranted in saying that the English law goes; indeed, doubt has been cast by some judges on the principle, and it has been stated that the obligation not to disclose is a moral rather than legal one. I incline to view that the rule which would now be adopted according to authorities, in English courts, is that a banker will be liable if he, without sufficient reason, disclosed the state of a customer's account to a third party and damage resulted."[38]

[32] 453.
[33] 453.
[34] 453.
[35] 454.
[36] 454.
[37] 454.
[38] 456 – 457.

It is therefore acknowledged in *Abrahams v Burns* that a bank owes a duty of secrecy to its customers and this duty imposed on South African banking institutions, finds its origins in English law. The court's decision is echoed by Willis who states that a banker in South Africa will be liable if he or she discloses the state of a client's account to a third party without sufficient cause and the client suffered damages as a result.[39] This is consistent with English law and was rightfully held in *Abrahams v Burns*.

2.2.2 *Firstrand Bank Ltd v Chaucer Publication (Pty) Ltd*[40]

In this matter, Firstrand had applied for an interdict *pendent lite* against the first and second respondents, namely, the publisher of Noseweek Magazine and Welz, the editor. This application came as a result of a series of articles which had been published in Noseweek Magazine containing certain allegations about the banking practices of Firstrand.[41] These articles contained the names of Firstrand clients as well as the names of their local and offshore trusts. Therefore, it was alleged that the content of these articles was defamatory to both Firstrand as well as its representatives.[42] As a result, Firstrand brought an application for an interdict to preclude Noseweek Magazine from publishing such names. Firstrand further stated in a supporting affidavit that it hoped to protect itself and some of its clients from defamation, to protect the confidentiality of certain information in which it and some of its clients had a priority interest and to protect its constitutional right to privacy. According to the court papers, the application was therefore brought in the interest of the applicant and the interest of a class of persons, being the clients of Firstrand and their trusts.[43] Firstrand further alleged that it had "a real and substantial interest" in the relief sought and accordingly that it had the necessary *locus standi* in terms of the common law to bring the application.[44] The applicant relied on section 38 of the Constitution, which deals with the enforcement of rights, to prove that they have the capacity to bring forth a claim for a breach of the constitutional right to privacy. Any party listed in section 38 has the right to approach the court alleging that a right in the

[39] N Willis *Banking in South African Law* (1981) 476.
[40] 2008 (2) SA 592 (C).
[41] par 3.
[42] par 12.
[43] par14.
[44] par 15.

Bill of Rights was infringed or threatened. The applicant subsequently argued that they have a right to allege a breach of the constitutional right to privacy as they are listed under section 38(a) which permits anyone acting in their own interest and 38(c) which permits anyone acting as a member of, or in the interest of, a group or class of persons to bring forth a claim for the violation contained in the Bill or Rights.[45] In his defence, the defendant raised the defence of truth and public interest in respect of the defamation claim made by the plaintiff.[46]

It was accordingly held that "for considerations of public policy the relationship between a bank and its customer must be of a confidential nature. Equally – for considerations of public policy – this duty is subject to being overridden by a greater public interest".[47]

From the aforementioned case law it can be concluded that the duty of a bank to protect the confidentiality of its client's affairs is recognised under South African law. Furthermore, this duty is not absolute but can be limited in the interests of *inter alia* public policy.

2.3 Statutory exceptions to the duty of secrecy

When determining if an invasion of privacy has occurred at common law, it must first be established whether the invasion in question is unlawful. The presence of a ground of justification, such as a statutory provision authorising the invasion means the invasion of privacy is not wrongful. The South African legal system contains various statutes which authorise an invasion of privacy in contravention of the duty of secrecy imposed on banks. This chapter looks at statues which provide for the duty of secrecy but also limit the scope to which the duty may apply.

2.3.1 Promotion of Access to Information Act 2 of 2000

The Promotion of Access to Information Act (PAIA) was enacted with the aim of giving effect to section 32 of the Constitution which protects the right of access to information.[48] PAIA was enacted for the purpose of encouraging accountability and transparency in the private and public sectors and in so doing, giving effect to the right

[45] Constitution of the Republic of South Africa, 1996.
[46] par 14.
[47] par 20.
[48] Constitution of the Republic of South Africa, 1996.

of access to information.[49] PAIA applies to records held by both public and private bodies. However, in terms of section 7(1)(b), the provisions of PAIA do not apply to records required for criminal or civil proceedings after commencement of proceedings. Section 5 of PAIA states that it applies irrespective of other legislation that prohibits or restricts the disclosure of a public body or a private body. However, there are limits to the types of information that may be requested in terms of PAIA, in that the information requested might not be granted when it infringes a person's right to privacy as stipulated in section 9(b) of PAIA.[50]

In terms of section 34 of PAIA the information officer of a public body must protect the privacy of a third party who is a natural person. Section 34 prohibits the information officer from providing access to a record which is in the public body's possession if the disclosure of such record would involve an unreasonable disclosure of a third party's personal information.

However, PAIA states that if the information could potentially show that there has been a serious violation of the law or a threat to public safety or the environment, then the request cannot be denied. This is contained in section 7(2) of PAIA, which states that "information obtained in contravention of subsection (1) is not admissible as evidence unless the exclusion of that record by the court would, in the courts opinion, be detrimental to the interests of justice." Financial crimes by nature pose a threat to public safety and security. According to McDowell and Novis crimes such as money laundering have "a corrosive effect on a country's economy, government, and social well-being. It distorts business decisions, increases the risk of bank failures, takes control of economic policy away from the government, harms a country's reputation, and exposes its people to drug trafficking, smuggling, and other criminal activity."[51] As a result, it is submitted that the perpetrators of such crimes cannot rely on the duty of secrecy to absolve their accounting records from disclosure. However, this can only be determined taking into considerations the facts of a particular case.[52]

Section 64 of the Act deals with the protection of commercial information of a third party. It is important to establish whether this protection includes information between a bank and its customers. In terms of section 64(1) the head of a private body

[49] Act 2 of 2000.
[50] Act 2 of 2000.
[51] J McDowell and G Novis 'Consequences of money laundering and financial crime' (2001) 6 *Economic Perspectives* 7.
[52] *Bernstein v Bester* 1996 (2) SA 751 (C) par 77.

must refuse a request for access to a record of the body if the record contains trade secrets of a third party or, in terms of section 64(1)(b) financial, commercial, scientific or technical information, other than trade secrets, of a third party, the disclosure of which would be likely to cause harm to the commercial or financial interests of that third party. As stated above, the bank-customer relationship entails *inter alia* money being lent to a bank by a customer on a current account and the bank incurring the obligation to repay the money on demand. This highlights the financial or commercial aspect of the bank-customer relationship which implies that the provisions of PAIA apply thereto.

Section 65 of PAIA caters for the mandatory protection of certain confidential information of a third party. This section provides that "the head of a private body must refuse a request for access to a record of the body if its disclosure would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement".[53] The duty of secrecy is however preserved under section 67 of PAIA which protects individuals from being forced to hand over privileged records during legal proceedings. In this regard, the head of a private body may not grant access to a record of the body if the record is classified as privileged information. The submission of such records may only be permitted if the person entitled to the privilege has waived his or her privilege.

2.3.2 South African Reserve Bank Act 90 of 1989

According to its preamble, the purpose of the South African Reserve Bank Act is to consolidate the laws relating to the South African Reserve Bank and the monetary system of the Republic; and to provide for matters connected therewith.[54] The duty of secrecy owed by the Reserve Bank is governed under section 33 of the Act which states that:

> "(1) No director, officer or employee of the Bank, and no officer in the Department of Finance, shall disclose to any person, except to the Minister or the Director-General: Finance or for the purpose of the performance of his or her duties or the exercise of his or her functions or when required to do so before a court of law or under any law-
> (a) any information relating to the affairs of-

[53] Act 2 of 2000.
[54] Act 90 of 1989.

(i) the Bank;
(ii) a shareholder of the Bank; or
(iii) a client of the Bank,
acquired in the performance of his or her duties or the exercise of his or her functions; or

(b) any other information acquired by him or her in the course of his or her participation in the activities of the Bank,

except, in the case of information referred to in paragraph (a) (iii), with the written consent of the Minister and the Governor, after consultation with the client concerned."

Section 33(a)(iii) preserves the duty of secrecy owed by the Reserve Bank to clients. It is stipulated in section 33(a)(iii) that a director, officer, employee of the reserve bank or officer in the Department of Finance may only disclose to any personal information relating to the affairs of a client, with the written consent of the Minister and the Governor and only after a consultation has been conducted with the client concerned. A client of the Reserve Bank who is suspected of involvement in criminal activity is therefore afforded a degree of protection in relation to his or her banking affairs. By requiring a consultation with the client and the written consent of the Minister and the Governor, the legislature aims to ensure that a client's affairs are not handled carelessly or shared with third parties.

It is stated in section 1(1A) of the Act that "the provisions of subsection (1) do not preclude any director, officer or employee of the reserve bank who is responsible for exercising any power or performing any function or duty under the Exchange Control Regulations, 1961, issued in terms of section 9 of the Currency and Exchanges Act 9 of 1933, from disclosing to the Commissioner of the South African Revenue Service any information as may be required for purposes of exercising any power or performing any function or duty in terms of any Act administered by the Commissioner."

According to section 33(2),

"no person shall disclose to any other person any information contained in any written communication which is in any manner marked as confidential or secret and which has been addressed by the Bank to any person or which has been addressed by any person to the Bank, except

(a) for the purposes of the performance of his duties or the exercise of his powers in terms of any law or when required to do so before a court of law; or

(b) with the written consent of both the sender and the recipient of that communication".[55]

Therefore, should confidential information be shared by a client with the Reserve Bank, the Bank must ensure that the confidentiality of that information is preserved. However, when the client is involved in criminal activities and a court of law requests the books of the client from the Bank, the Bank will have to comply with the request and furnish all the information relevant to the legal proceedings. This shows that although the South African Reserve Bank Act aims to preserve the duty of secrecy in the favour of *inter alia* clients, this duty is subject to limitation.

Any person who contravenes the provisions of section 33, subject to the provisions of section 2 of the Prevention of Counterfeiting of Currency Act 16 of 1965, shall be guilty of an offence. In terms of section 34(1)(iii), this person will be liable on conviction for a fine not exceeding R4 000 or for imprisonment for a period not exceeding one year or for both a fine and imprisonment.

2.3.3 Criminal Procedure Act 51 of 1977

The Criminal Procedure Act 51 of 1977 sets out specific rules regarding a bank's obligations regarding its client's books and documents when the client has been accused of criminal activity. In terms of section 236(1), "the entries in the accounting records of a bank, and any document which is in the possession of any bank and which refers to the entries or to any business transaction of the bank, shall, upon the mere production at criminal proceedings of a document purporting to be an affidavit be *prima facie* proof at such proceedings of the matters, transactions and accounts recorded in such accounting records or document."[56] This means that information pertaining to the client's account may be presented to the court as an affidavit and will serve as proof of the client's misconduct during such criminal proceedings. The fact that the client's records are admissible as evidence without the consent of the client involved shows how the duty of secrecy is limited in terms of the Criminal Procedure Act.

However, it must be noted that when a client's accounting records are considered to be admissible as evidence in legal proceedings, the client may be permitted to make

[55] Act 90 of 1989.
[56] Act 51 of 1977.

copies of the documents in order to assist in his or her defence. This rule is contained in section 236(3) of the Criminal Procedure Act which states as follows:

> "Any party at the proceedings in question against whom evidence is adduced in terms of this section or against whom it is intended to adduce evidence in terms of this section, may, upon the order of the court before which the proceedings are pending, inspect the original of the document or entry in question and any accounting record in which such entry appears or of which such entry forms part, and such party may make copies of such document or entry, and the court shall, upon the application of the party concerned, adjourn the proceedings for the purpose of such inspection or the making of such copies."[57]

The duty of secrecy is therefore recognised by the law of criminal procedure, but it is limited. The limitation of the duty is contained in section 236(4) of the Act which states that no bank shall be compelled to produce any accounting record referred to in subsection (1) at any criminal proceedings. This is an acknowledgment of the duty of secrecy owed by the bank to its clients, but the proviso to section 236(4) is that the court concerned may compel the bank to produce such records.[58]

2.4 The Code of Banking Practice

All banks that are members to the Banking Association of South Africa have committed themselves to comply with the provisions of the Code of Banking Practice. The provisions of the code apply to personal and small business customers. "Personal customer" in terms of the code refers to "any individual who maintains an account or who receives other services from a bank" while a "small business" is one which has turnover of less than R5 million per annum. The South African Code of Banking Practice gives insight into the standards that banks have undertaken to uphold.[59] In this regard, the code recognises the duty to maintain secrecy and confidentiality in respect of their clients' confidential information. The Code provides as follows regarding the duty of secrecy:

[57] Act 51 of 1977.
[58] Act 51 of 1977.
[59] SF Du Toit 'Reflections on the South African code of banking practice' 3 (2014) *Journal of South African Law* 568.

"6.1 Confidentiality and Practice

We will treat all our personal information as private and confidential, and, as a general rule, we will not disclose any personal information about you or your accounts, including to other companies in our Group (even when you are no longer a customer) unless under the following specific circumstances:

i. When we are compelled by law to disclose the information
ii. When we have a legal duty to the public to disclose the information
iii. When we have to protect our interests by disclosing the information (for example, to prevent fraud). However, we will not use this as a reason for disclosing information about you or your accounts (including your name and address) to anyone else
iv. When you have asked us or if we have your consent to disclose the information
v. When your account is in default and you have not made satisfactory arrangements with us for the repayment of the debt; or
vi. Your cheque has been "referred to drawer", in which case the information may be placed on a cheque verification service."[60]

It is submitted that this provision ought to be legally binding on banking institutions. According to Du Toit, the Code of Banking Practice is amongst the most important influences on the relationship between a bank and its customers in South Africa.[61] As such, Du Toit argues that the 2004 code was incorrect in that it expressly provided that none of its provisions will be legally binding or may be used to influence the interpretation of the bank-customer relationship.[62] It has been admitted[63] that the influence of the code is subtler than that of legislation, however, Du Toit argues that the South African Code of Banking Practice constitutes "more than an ethical code or mere soft law".[64] This is because the 2012 code does not contain a similar provision to the 2004 code regarding the extent to which it is legally binding. As such, the courts may use provisions of the code as a basis for implying terms into the bank-customer contract.[65] According to Schulze, these provisions may then be classified as terms

[60] https://www.banking.org.za/wp-content/uploads/2019/04/Code-of-Banking-Practice-2012.pdf (accessed: 18 September 2019).
[61] SF Du Toit 'Reflections on the South African code of banking practice' 3 (2014) *Journal of South African Law* 568.
[62] SF Du Toit 'Reflections on the South African code of banking practice' 3 (2014) *Journal of South African Law* 569.
[63] SF Du Toit 'Reflections on the South African code of banking practice' 3 (2014) *Journal of South African Law* 569.
[64] SF Du Toit 'Reflections on the South African code of banking practice' 3 (2014) *Journal of South African Law* 569.
[65] WG Schulze 'The sources of South African banking law – a twenty-first century perspective (part I)' 14 (2002) *South African Mercantile Law Journal* 456.

implied by law or derived from trade usage.[66] This is because merely including a specific banking practice, such as the duty of confidentiality, in the code constitutes a strong indication that it existed as a banking practice or trade usage in its own right even before its inclusion in the code.[67] Du Toit further adds in this regard that the fact that all major banks currently subscribe to the code and subsequently aim to uphold its standards in itself points to the existence of trade usage.[68] As acknowledged in the *Alfred McAlpine* case, implied terms can derive from the common law, trade usage, custom or from legislation.[69] In this regard, it is possible that trade usage may "harden" into a rule of law.[70] As such, it is submitted that the duty of confidentiality contained in the Code of Banking practice constitutes an implied term of the contract between a bank and its customers derived from trade usage. As such, the provision ought to be legally binding on banking institutions.

[66] WG Schulze 'The sources of South African banking law – a twenty-first century perspective (part I)' 14 (2002) *South African Mercantile Law Journal* 456.
[67] WG Schulze 'The sources of South African banking law – a twenty-first century perspective (part I)' 14 (2002) *South African Mercantile Law Journal* 457.
[68] SF Du Toit 'Reflections on the South African code of banking practice' 3 (2014) *Journal of South African Law* 570.
[69] 1974 (3) SA 506 (A) par 531G.
[70] SF Du Toit 'Reflections on the South African code of banking practice' 3 (2014) *Journal of South African Law* 570.

Chapter 3:
The right to privacy

3.1 Common law right to privacy

The right to privacy is regarded as being essential for the development and maintenance of a free society and for ensuring a mature and stable personality.[71] The common law recognises the right to privacy as an independent personality right that the courts consider as part of the concept of *dignitas*.[72] Privacy can be described as an individual condition of life characterized by seclusion from the public and publicity.[73] This condition embraces all the personal facts that the person has determined to be excluded from the knowledge of outsiders and that he wishes to be kept private.[74] In terms of common law, a breach of an individual's personality right is considered an *inuria*, which can take place in two ways: firstly, where there is an unlawful intrusion of an individual's personal privacy and secondly, where there is an unlawful disclosure of an individual's private facts.[75] The unlawfulness of the disclosure is determined by assessing whether the court may find a ground of justification which authorises an invasion of the right to privacy and an enquiry into whether such disclosure was done in good faith.[76]

Since it is up to the individual to determine which information regarding his or her life must remain private, this power of self-determination is considered to be the essence of the individual's interest in privacy, and therefore also of his right to privacy.[77] In *National Media Ltd v Jooste*, Harms JA explained the right to privacy in the following manner:

> "A right to privacy encompasses the competence to determine the destiny of private facts ... The individual concerned is entitled to dictate the ambit of

[71] GE Devenish *A Commentary on the South African Constitution* (1998) 51.
[72] J Neethling 'The protection of the right to privacy against fixation of private facts' (2004) 121 *South African Law Journal* 519.
[73] J Neethling 'The protection of the right to privacy against fixation of private facts' (2004) 121 *South African Law Journal* 519.
[74] J Neethling 'The protection of the right to privacy against fixation of private facts' (2004) 121 *South African Law Journal* 519.
[75] J Neethling 'The protection of the right to privacy against fixation of private facts' (2004) 121 *South African Law Journal* 520.
[76] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) par 462F.
[77] J Neethling 'The protection of the right to privacy against fixation of private facts' (2004) 121 *South African Law Journal* 520.

> disclosure, for example to a circle of friends, a professional adviser or the public ... Hemay prescribe the purpose and method of the disclosure ... Similarly, I am of the view that a person is entitled to decide when and under what conditions private facts may be made public. A contrary view will place undue constraints upon the individual's so-called ''absolute rights of personality'' ... It will also mean that rights of personality are of a lower order than real or personal rights. These can be limited conditionally or unconditionally and irrespective of motive."[78]

The common law lists six examples in which an individual's right to privacy can be infringed. These examples are as follows:[79]

1. Entry into a person's private residence;
2. the reading of a person's private documents;
3. listening to private conversations between persons;
4. the following of a person;
5. disclosing of private facts acquired by means of wrongful act of intrusion; and
6. the disclosure of facts in breach of a confidential relationship.

The final example referring to the disclosure of private facts in breach of a confidential relationship, is applicable to the relationship between a bank and its customers and the obligation of confidentiality due to customers by a banking institution.

Shaik-Peremanov notes that while we might regard the Constitution as the supreme law of the land and by extension hold its entrenchment of the right to privacy in high esteem, notions of privacy existed prior to its inception and formed an integral part of the common law.[80] This implies that all notions of secrecy and privacy at common law subsist even in the constitutional dispensation of the Republic. What differs in this regard is merely the level of privacy a citizen can reasonably expect depending on the conduct bringing him into contact with the law.[81]

[78] 1996 (3) SA 262 (SCA) par 271 – 272.
[79] *Bernstein v Bester* 1996 (2) SA 751 (C) par 69.
[80] N Shaik-Peremanov, 'Basel II – The Right to Privacy: A South African Perspective' (2009) 21 *SA Mercantile Law Journal* 550.
[81] N Shaik-Peremanov, 'Basel II – The Right to Privacy: A South African Perspective' (2009) 21 *SA Mercantile Law Journal* 550.

3.2 Constitutional right to privacy

Section 14 of the Bill of Rights guarantees the constitutional right to privacy. This is therefore one of the most important laws governing the duty of secrecy imposed on banks. Section 14 has been strategically divided into two distinct parts: on one hand section 14 provides a general right to privacy while on the other hand, the section provides specific categories of privacy rights. In terms of section 14, 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.

Whilst section 14(d) prohibits the infringement of the private communications of an individual, Ismael maintains that it is unclear to what extent section 14(d) protects the written, oral, telephonic and electronic communications between a banking institution and its customers.[82] It therefore cannot be said that the constitutional right to privacy directly includes the duty of secrecy imposed on banks. Nevertheless, the courts have shed light on the constitutional validity of the duty of confidentiality and secrecy.

When discussing rights contained in the Bill of Rights, it is important to note that rights like those guaranteed in section 14 are not absolute and can be limited in terms of section 36. Read together with section 36 of the Constitution, the right to privacy may be "limited in terms of law of general application to the extent the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom". What the courts essentially have to do is engage in an exercise which involves the weighing up competing rights, namely the right to privacy and the right to know.[83] Any party who wishes to limit the constitutional right to privacy must thus ensure that such a limitation is brought within the ambit of section 36 of the Constitution and subsequently, that a proportionate relationship exists between the right requiring protection, the right to privacy and the importance of the objective desired by such a limitation.[84]

---

[82] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 3.
[83] OB Amao & S Dumisa 'The Utility of Moral Philosophy and Professional Ethics in the Fight against Corruption in South Africa: Any Role for Ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 125.
[84] N Shaik-Peremanov, 'Basel II – The Right to Privacy: A South African Perspective' (2009) 21 *SA Mercantile Law Journal* 550. 552-553.

In *Bernstein v Bester* the Court stated that:

> "The truism that no right is to be considered absolute implies that from the outset of interpretation that each right is always already limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person such as his or her family life, sexual preference and home environment which is shielded from erosion by conflicting rights of the community."[85]

This means that the rights of the community as a whole and those vested in its members create a corresponding obligation on a citizen and this in turn influences the perception and definition of individualism towards identifying a concrete member society.[86] This is consistent with the common law position already referred to in *Financial Mail (Pty) Ltd* case where the court held that the unlawfulness of an infringement of privacy is adjudged in light of contemporary *boni mores* and the general sense of justice of the community as perceived by the court.[87]

Therefore, there is little doubt regarding the scope and application of the section 14 right to privacy as it pertains to the personal realm of an individual's life, but one sees the nature and scope of such privacy shrink significantly as one engages in more communal affairs, such as social interactions, commercial affairs or business.[88] The relationship which exists between a bank and its customers is commercial in nature and if it is accepted that this kind of relationship limits the scope of privacy which may be enjoyed by an individual then it can be argued that a client suspected of criminal activity can expect their constitutional right to privacy to be limited in terms of section 36. It is submitted that financial crimes by their nature are harmful to the state, the economy as well as communal interests and for this reason, the invasive provisions contained in statutes enacted for purposes of combating these financial crimes would favour an outcome in support of limiting the right to privacy in terms of section 36.

3.2.1 *Bernstein v Bester*

The form of disclosure required from banks pertaining to their customers suspected of being involved in criminal activity can be likened to instances of searches and

[85] *Bernstein v Bester* 1996 (2) SA 751 (C).
[86] *Bernstein v Bester* 1996 (2) SA 751 (C) par 67.
[87] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) par 462F.
[88] *Bernstein v Bester* 1996 (2) SA 751 (C) par 67.

seizures.[89] Searches and seizures are typically conducted for purposes of obtaining evidence which is relevant to legal proceedings. However, as stated above, section 36 of the Constitution states that in order for such conduct to be regarded as lawful, the law authorising such an invasion must be a law of general application.[90] In this regard, the guidelines regarding searches and seizures offered by Chaskalson P in *S v Makwanyane and Another*[91] may offer guidelines to bankers as regards the right of privacy of their clients. According to Chaskalson P, the limitation must be justifiable in an open and democratic society based on freedom and equality, it must be both reasonable and necessary and it must not negate the essential content of the right.[92] Nevertheless, the limited scope for the privacy arguments in the context of business relations is well illustrated by the judgment of the Constitutional Court in *Bernstein v Bester.*[93] In this matter, the Constitutional Court recognised the existence and validity of the right to privacy in the personal realm and moreover, how this right morphs and becomes significantly smaller as one moves further into a commercial or business-related context.

In the *Bernstein* decision, the constitutionality of specific sections of the Companies Act were questioned.[94] Sections 417 and 418 of the Companies Act created mechanisms which vested the Master of the Supreme Court with the authority to appoint a commissioner. Such a commissioner was tasked with the duty of inquiring as to why a company had gone into liquidation. In fulfilment of these duties, the commissioner was vested with a wide range of powers including the power to subpoena and examine witnesses and more importantly, to compel such witnesses to provide any documents, books or papers relating to the company. Any witness failing to adhere to a subpoena, answer questions or furnish specific documents requested by the commissioner would subsequently be guilty of an offence. Such a failure could however be justifiable on the grounds of "sufficient cause" for failure to comply or to answer.[95]

---

[89] N Shaik-Peremanov, 'Basel II – The Right to Privacy: A South African Perspective' (2009) 21 *SA Mercantile Law Journal* 550.
[90] Constitution of the Republic of South Africa, 1996.
[91] 1995 (3) SA 391 (C).
[92] 1995 (3) SA 391 (C) par 103.
[93] 1996 (2) SA 751 (C).
[94] Act 61 of 1973.
[95] *Bernstein v Bester* 1996 (2) SA 751 (C) par 88.

In his judgment, Ackermann J acknowledged the fact that there exists certain information that a client may prefer to keep confidential and when a client is compelled to disclose such information, books or documentation, an invasion of the right to privacy occurs. Bearing this in mind, Ackermann J further stated that it is difficult to effectively pronounce on the issue of privacy without a thorough engagement with the contents of any document that has been argued to be confidential.[96] As such, pronouncement on the issue of privacy necessitates disclosure of specific information contained in any books and documents over which privacy is being claimed.[97]

Ackermann J also held that it was difficult to conclude that information which was in the possession of a particular individual and was concurrently relevant to a Companies Act inquiry was *per se* confidential.[98] This is because the primary aim of this inquiry is to ensure a proper winding-up of the company, which could only be achieved through a discovery of information in the documents that could potentially benefit the company.[99] Subsequently, information that related to the affairs of the company would solely be relevant to this inquiry, this knowledge having been acquired through the relationship with the company.[100] It would thus be incorrect to classify such information as forming part of an individual's "private information".[101]

According to Ackermann J, when business is conducted by way of a limited liability company, the parties thereto can no longer be said to be engaging in their private affairs, instead their conduct is tantamount to "participation in the public sphere".[102] Such information cannot be regarded as inhering in the person and accordingly, it does not meet the requirements of a reasonable expectation of privacy which is recognised by society as objectively reasonable.[103] These requirements are derived from the two pronged test employed by the court in *Bernstein v Bester* and the two-part test expounded by the court is as follows: The party seeking to suppress the evidence must establish that they have a subjective expectation of privacy and secondly, it must be proven that the society has recognised this expectation as

[96] par 64.
[97] par 64.
[98] par 83.
[99] par 82.
[100] par 84.
[101] par 84.
[102] par 85.
[103] par 86.

objectively reasonable.[104] Therefore, it is clear that an individual's right to privacy may only be limited in a legitimate context, pending the satisfaction of both enquiries of the test.

When viewing this in the context of financial crime, it can be argued that the limitation of the right to privacy does satisfy both legs of the test applied in *Berstein v Bester*. This is because the judge in *Bernstein v Bester* stated that "any information pertaining to participation in [the] public sphere, cannot rightly be held to be inhering in the person, and it cannot be said that in relation to such information a reasonable expectation of privacy exists. Nor would such an expectation be recognised by society as objectively reasonable."[105] It is therefore evident that one's engagement in the public sphere has the tendency to limit one's right to privacy.

It is important to note in this regard that the court in *Bernstein* considered information related to the company's (juristic person) affairs to fall within the public sphere due to the resultant implications on shareholders. The court did not mention the personal information of an individual that is in the possession of an accountable institution to fall within the scope of the public sphere. However, Ackermann J is of the opinion that any information which an individual possesses which is relevant to the purpose of an enquiry cannot said to be private.[106]

It is therefore submitted that because the financial records, accounting books and other documents of a client who may be suspected of financial crime are fundamental to the investigation process, this information qualifies as "participation in the public sphere" and subsequently satisfies both legs of the test for the limitation of the right to privacy.

3.2.2 Ubuntu and the right to privacy

Given the fact that financial crime has continued to rise[107] in the years following the inception of South Africa's democratic dispensation, it is evident that the prevailing strategies, particularly as pertaining to the right to privacy when dealing with suspects and perpetrators of financial crime, have proved to be ineffective. It is within this

[104] N Shaik-Peremanov, 'Basel II – The Right to Privacy: A South African Perspective' (2009) 21 *SA Mercantile Law Journal* 551.
[105] *Bernstein v Bester* 1996 (2) SA 751 (C) par 85.
[106] *Bernstein v Bester* 1996 (2) SA 751 (C) par 83.
[107] https://businesstech.co.za/news/government/340513/south-africa-crime-stats-2019-everything-you-need-to-know/

context that a moral appeal to the philosophy of Ubuntu surfaces as a potential antidote to criminal practices in South Africa.[108] In an attempt to describe the role of Ubuntu in this discussion, Dumisa and Amao make use of an analogy. According to them, the laws, policies and institutions that are commonly employed in the fight against corruption, can be regarded as hardware. The Professional Ethics codes, which form part of the Public Service Commission's mandate and are obtainable in section 195(1) of the Constitution[109], form part of the software of this system. Ubuntu and its values can then be regarded as the "programme" which functions in support of the professional ethics and concurrently protects the software from any potential malfunctions.[110]

In order to ascertain the efficient functioning of the system, eight principal values have been incorporated into the professional code of ethics of the Republic.[111] These values are uniformly referred to as the *Batho Pele* principles. *Batho Pele* is a Basotho term for "people first". The eight principal values are: consultation; service standards; access; courtesy; information; openness and transparency; redress; and customer satisfaction.[112]

The most relevant for this discussion are the values of openness and transparency. When assessing these values in light of the weighing up of rights outlined in section 36 of the Constitution one can see that in the interests of the *Batho Pele* principles and their focus on public interest, a bank is under an obligation to disclose certain information pertaining to a client when such client is believed to be involved in the commission of a particular financial crime. This is because Ubuntu dictates that the interests and security of the public or community must be placed above those of the individual.[113] In this regard, Mokgoro J states that "Generally, ubuntu translates as humaneness. In its most fundamental sense, it translates as personhood and morality. Metaphorically, it expresses itself in *umuntu ngumuntu*

[108] OB Amao & S Dumisa 'The Utility of Moral Philosophy and Professional Ethics in the Fight against Corruption in South Africa: Any Role for Ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 97.
[109] Constitution of the Republic of South Africa, 1996.
[110] OB Amao & S Dumisa 'The Utility of Moral Philosophy and Professional Ethics in the Fight against Corruption in South Africa: Any Role for Ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 100.
[111] White Paper on Transforming Public Service Delivery (Batho Pele White Paper) Notice 1459 of 1997.
[112] Notice 1459 of 1997.
[113] S v Makwanyane 1995 (3) SA 391 (C) par 308.

ngabantu, describing the significance of group solidarity on survival issues so central to the survival of communities."[114]

This fact is further acknowledged by Gyeke who states that the communal ethos of African culture necessarily placed a great value on solidarity, which in turn necessitated the pursuit of unanimity or consensus not only in such important decisions as those taken by the highest political authority of the town or state, but also decisions taken by lower assemblies such as those presided over by the councillors.[115]

In the *National Coalition for Gay and Lesbian Equality* case, it was stated that the courts must remove themselves from rigid and tabularized interpretations of the law and must instead interpret laws in a manner consistent with the pervasive social reality.[116] From this judgement it can be deduced that although the right to privacy is a fundamental right, it cannot be protected with such stringent legalism that it infringes on the rights of others in society or in a manner that is inconsistent with the pervasive social reality of the Republic, taking into account the plight of financial crime in South Africa.

It is thus submitted that in order to give full effect to the critical values of Ubuntu in the face of financial crime, the right to privacy cannot be used as a justifiable means upon which the values of openness and transparency can be compromised. An interpretation of the right to privacy which favours and protects suspects or perpetrators of financial crime is not welcomed as it inevitably preserves and enables criminal activity to thrive within the South African economy without fear, recourse or consequence.

[114] par 308.
[115] K Gyekye *An Essay on African Philosophical Thought* (1987) 35.
[116] *National Coalition for Gay and Lesbian Equality v Minister of Justice and Others* 1999 (1) SA 6 (C) par 112.

Chapter 4:
Specific financial crimes

4.1 Introduction

The purpose of this chapter is to look at specific financial crimes and how the duty of secrecy has been limited in order to assist in the combating of these financial crimes. There are also instances in which a customer of a specific banking institution is not the perpetrator but is instead a victim of financial crime. In this regard, the chapter also looks at how the legislature preserves the duty of secrecy in order to protect the interests and personal information of customers to banking institutions when such customers fall victim to online scams. The chapter will therefore be focusing on the duty of secrecy as it relates to the criminal activities of corruption, money laundering and the online offence of phishing which involves identity theft.

4.2 Corruption

Corruption includes any conduct which blatantly goes against the formal duties of a public official for purposes of private-pecuniary or status gains or which violates rules.[117] This is consistent with Mafunisa's definition who asserts that "corruption involves the illegal or unethical use of governmental authority for personal or political gain".[118] When this happens, there is an abuse and/or misuse of public office and authority in return for personal gain, which could be material or non-material.

Among the forms of conduct attributable to corruption are bribery, which is an example of material personal gain, where a party in a position of trust is lured into unlawful conduct by using some or other reward as incentive.[119] According to Wilson bribery occurs when a person in exchange for some private advantage acts other than

[117] OB Amao & S Dumisa 'The Utility of Moral Philosophy and Professional Ethics in the Fight against Corruption in South Africa: Any Role for Ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 89.
[118] J Mafunisa 'Enhancing Accountability and Ethics in the Public Service: the case of the Republic of South Africa' in K Frimpong & G Jaques (eds) *Corruption, Democracy and Good Governance (1999) 191.*
[119] OB Amao & S Dumisa 'The Utility of Moral Philosophy and Professional Ethics in the Fight against Corruption in South Africa: Any Role for Ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 89.

what his or her duty requires.[120] Secondly, there is nepotism, which is an example of non-material personal gain. Nepotism involves the bestowal of patronage on the basis of a familiar or close relationship with the recipient (thus favouritism) instead of merit.[121] Lastly, there is misappropriation, which refers to the illegal appropriation of public resources for private/personal use.[122]

Article 4, clause 1 of the African Union's (AU) *Convention on Preventing and Combating Corruption and Related Offences* (2003) defines corruption as:

> "(1) The solicitation or acceptance, directly or indirectly, by a public official or any other person, of any goods of monetary value, or other benefit, such as a gift, favour, promise or advantage for himself or herself or for another person or entity, in exchange for any act or omission in the performance of his or her public functions;
> (2) The offering or granting, directly or indirectly, to a public official or any other person, any goods of monetary value, or other benefit, such as a gift, favour, promise or advantage for himself or herself or for another person or entity, in exchange for any act or omission in the performance of his or her public functions, and;
> (3) The diversion by a public official or any other person, for purposes unrelated to those for which they were intended, for his or her own benefit or that of a third party, of any property belonging to the state or its agencies, to an independent agency, or to an individual, which the official has received by virtue of his or her position".[123]

The remnants and effects of corrupt activity are evident in all facets of global security, prosperity, growth and the battle to deter extreme levels of poverty experienced by many the world over.[124] Corruption plays a key role in maintaining the status quo, ensuring that the inequalities present in today's societies are heavily entrenched and many lives continue to be ruined as an outcome.[125] The 2015 Panama Papers scandal played a significant role in exposing high profile cases dealing with corrupt activities, particularly those instances that involved heads of state as well as other officials who

[120] J Wilson 'Corruption is not always Scandalous' in J Gardiner & D Olson (eds) *Theft of the City, Readings on Corruption in America* (1968) 55.
[121] OB Amao & S Dumisa 'The Utility of Moral Philosophy and Professional Ethics in the Fight against Corruption in South Africa: Any Role for Ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 89.
[122] OB Amao & S Dumisa 'The Utility of Moral Philosophy and Professional Ethics in the Fight against Corruption in South Africa: Any Role for Ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 89.
[123] Convention on Preventing and Combating Corruption and Related Offences (CPCCRO).
[124] S Powell 'Secrecy Feeds Corruption & Secures Opulence' (2016) 2 *TFM Magazine* 34.
[125] S Powell 'Secrecy Feeds Corruption & Secures Opulence' (2016) 2 *TFM Magazine* 34.

were guilty of siphoning public funds to the elite.[126] Global corruption has a direct bearing on the state of corruption in South Africa.[127] Moreover, corruption gives license to perpetrators of money laundering, often with clear links to global terrorism, creating an environment in which their criminal activities can thrive without consequence.[128]

In an effort to limit the pervasiveness of corruption in South Africa, the legislature enacted the Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA). The purpose of PRECCA is *inter alia* to provide for the strengthening of measures to prevent and combat corruption and corrupt activities.[129] PRECCA also provides for investigative measures in respect of corruption and related corrupt activities.[130] The Act places a duty on certain persons holding a position of authority to report certain corrupt transactions so as to ensure adequate governance of corrupt activity in the Republic.[131] It is submitted that these reporting obligations place a limitation on the duty of secrecy owed by banks to their clients.

The duty to report corrupt transactions is contained in section 34 of PRECCA. In terms of section 34(1) ‘’this duty vests in any person who holds a position of authority and who knows or ought reasonably to have known or suspected that any other person has committed- (a) an offence under Part 1, 2, 3 or 4, or section 20 or 21 (in so far as it relates to the aforementioned offences) of Chapter 2; or (b) the offence of theft, fraud, extortion, forgery or uttering a forged document, involving an amount of R100 000 or more, must report such knowledge or suspicion or cause such knowledge or suspicion to be reported to any police official. (2) Subject to the provisions of section 37 (2), any person who fails to comply with subsection (1), is guilty of an offence.’’[132]

Section 34(1) speaks of “any person” and does not appear to apply specifically to banks. However, in terms of section 34(4)(f) the executive manager of any bank or other financial institution holds a position of authority for purposes of subsection (1). The bank and its employees are therefore obligated to monitor the transactions of their customers and promptly report any transactions which are tantamount or potentially so, to corrupt activity. This obligation limits the duty of secrecy because it requires the bank to share confidential information related to a client’s account with the authorities.

[126] S Powell ‘Secrecy Feeds Corruption & Secures Opulence’ (2016) 2 *TFM Magazine* 33.
[127] S Powell ‘Secrecy Feeds Corruption & Secures Opulence’ (2016) 2 *TFM Magazine* 34.
[128] S Powell ‘Secrecy Feeds Corruption & Secures Opulence’ (2016) 2 *TFM Magazine* 34.
[129] Act 12 of 2004.
[130] Act 12 of 2004.
[131] Act 12 of 2004.
[132] Act 12 of 2004.

By so doing, the legislature aims to combat the prevalence of corrupt activity and to limit the amount of corruption perpetrated via banking institutions and other financial entities.

4.3 Money laundering

Money laundering refers to "the act of concealing or disguising the origin of proceeds of revenue acquired from illegal activities, in a manner whereby entities of the formal financial system are used to make proceeds appear to be clean and legitimate."[133] Money laundering emerged as a practice in the 1970s and it involves the practice of processing the proceeds of criminal conduct to make them appear legitimate.[134] The phrase is said to come from the use laundromats by American criminal organisations to hide money they obtained from criminal conduct.[135] These criminal organisations specifically used laundromats because these businesses were cash-intensive in the sense that the amount of cash they saw in a defined period of time would make it difficult to identify illegally gotten gains.[136] The term money laundering thus refers to a deliberate, complex and sophisticated procedure through which ill-gotten gains are masked or made to appear as though they were acquired by a legitimate means.[137] According to Magarura, money laundering is a three stage process which operates as follows:

> "1. the dirty money must be severed from the predicate crime generating it;
> 2. it must be characterised by a series of transactions designed to obscure or destroy the money trail in order to avoid detection; and
> 3. the criminal proceeds must be reinvested in furtherance of the objectives of the business (launderer)."[138]

Money laundering is one of the most popular ways in which organised crime syndicates the world over perpetrate financial crime and enjoy the proceeds of

[133] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 6.
[134] B Unge & D van der Linde *Research Handbook on Money Laundering* (2013) 35.
[135] B Unge & D van der Linde *Research Handbook on Money Laundering* (2013) 35
[136] N Mugarura *The Global Anti-Money Laundering Regulatory Landscape in Less Developed Countries* (2012) 1.
[137] N Mugarura *The Global Anti-Money Laundering Regulatory Landscape in Less Developed Countries* (2012) 1.
[138] N Mugarura *The Global Anti-Money Laundering Regulatory Landscape in Less Developed Countries* (2012) 1.

unlawful activity and the benefit of their crimes.[139] One of the greatest advantages to perpetrators of money laundering is that the practice provides them with a readily available and steady cash flow. This enables criminals to commit further criminal offences and may very well give an incentive to criminals because it allows such criminal acts to be profitable.[140]

FICA was enacted with the purpose of *inter alia* establishing a Financial Intelligence Centre in order to combat money laundering activities and the financing of terrorist and related activities.[141] According to the preamble, this purpose is achieved by imposing certain duties on accountable institutions and other persons who might be used for money laundering purposes and the financing of terrorist and related activities.[142]

In terms of section 1 of FICA money laundering activity is defined as "an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of section 64 of this Act or section 4, 5 or 6 of the Prevention Act."[143]

FICA applies to banks because in terms of schedule 1(6) of FICA, the term "accountable institution" includes a person who carries on the business of a bank as defined in the Banks Act 94 of 1990. Through FICA, the duty of secrecy imposed on banks has been significantly limited. This limitation is expressly provided for in section 37 of FICA which states that:

> "No duty of secrecy or confidentiality or any other restriction 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."[144]

[139] A Srivastava, M Simpson & N Moffatt *International Guide to Money Laundering Law and Practice* 4 (2013) 1179.
[140] A Srivastava, M Simpson & N Moffatt *International Guide to Money Laundering Law and Practice* 4 (2013) 1179.
[141] Financial Intelligence Centre Act 38 of 2001
[142] Act 38 of 2001.
[143] Act 38 of 2001.
[144] Act 38 of 2001.

Accordingly, in terms of Section 37 of FICA, the obligations to report and disclose information overrides any duty of confidentiality or secrecy owed to the bank's customer whether such a duty is imposed by law or is by agreement.[145]

FICA requires accountable institutions to report the following transactions:

1. Cash transactions above a prescribed limit in terms of section 28
2. Property associated with terrorist and related activities in terms of section 28A
3. The conveyance of cash in and out of the country in excess of prescribed amounts in terms of section 30
4. International electronic transfers in terms of section 31
5. Suspicious and unusual transactions in terms of section 29

In terms of section 28, an accountable institution is obligated to report to the FIC if an amount of cash in a transaction is paid to a customer or the customer's agent and the amount paid is above the prescribed amount. The accountable institution must also report to the FIC if the cash is paid to the institution by the customer or the customer's agent or a person on whose behalf the customer is acting.[146] Section 32(1) provides that a report in terms of section 28 must be made in the prescribed manner.[147] In terms of section 32(2) the FIC may request any additional information it deems necessary from the accountable institution responsible for filing the report.[148] Section 38 provides that a person who complies with these requirements will therefore be protected from criminal or civil liability provided that they acted in good faith.[149] According to De Koker, this protection is broad and would include protection against civil action that may be based on a breach of the duty of confidentiality and secrecy by a bank.[150] Such a person will furthermore be absolved of any duty of confidentiality other than attorney-client privilege as stipulated in section 37 of FICA. Section 52 states that failure to comply with the provisions of section 28 constitutes an offence which is punishable by

[145] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-40.
[146] Act 38 of 2001.
[147] Act 38 of 2001.
[148] Act 38 of 2001.
[149] Act 38 of 2001.
[150] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-40.

way of a fine not exceeding R10 million or imprisonment for a maximum period of 15 years.[151]

In terms of section 29(1) a person who carries on, manages or is in charge of a business or who is employed by a business is required to report any suspicious or unusual transactions which may come to his or her attention. Such a person is required to report the grounds for the suspicion and prescribed particulars regarding the transaction to the FIC if he or she knows or ought reasonably to have known or suspected certain facts. This party must report to the FIC within a prescribed period after he acquired the knowledge or formed the suspicion.[152]

Facts which may allude to unusual or suspicious transactions in terms of section 29 include:

> ”1. Proceeds derived from unlawful activities being acquired by the business or property obtained in connection to an offence that relates to the financing of terrorist and related activities.
> 2. A transaction or series of transactions to which the business is a party that:
> 2.1 is facilitated or is likely to facilitate the transfer of proceeds of unlawful activities or to property related to an offence in respect of the financing of terrorist and related activities;
> 2.2 does not have an apparent business or lawful purpose;
> 2.3 is conducted in such a way that it is to avoid giving rise to a duty to report under FICA;
> 2.4 may be relevant to the investigation of an attempted evasion or evasion of a duty to pay any tax, duty or levy; or
> 2.5 relates to an offence in respect of the financing of terrorist and related activities; and
> 3. The business has been used or will be used for money-laundering purposes or to facilitate the commission of an offence in respect of financing of terrorist and related activities.”[153]

Section 29(2) of FICA further requires a person who carries on, manages or is in charge of a business or who is employed by a business to report transactions where enquiries have been made regarding a specific transaction but the transaction was never actually concluded. This would be necessary where the person who must file the report knows or suspects that the transaction that was enquired about could constitute a fact which may allude to a suspicious or unusual transaction as described

[151] Act 38 of 2001.
[152] Act 38 of 2001.
[153] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-11 – 7-12.

above if the transaction had indeed been concluded. Section 52(2) of FICA provides that should a person mentioned in section 29 negligently fail to file the report as required by the Act where such a person reasonably ought to have known or suspected that a fact existed which resulted in an obligation to file a report in terms of 29, he or she will be guilty of an offence. Such a person may incur a penalty in the form of a fine not exceeding R10 million or imprisonment for a period not exceeding 15 years.

As stated above, in terms of section 29(1) a reporter is obligated to report the grounds for knowledge and suspicion as well as certain prescribed particulars relating to the transaction.[154] In this regard, in order for a suspicion to be reportable it must be based on a clearly definable ground.[155] Such ground must therefore reasonably support a suspicion. De Koker is of the opinion that knowledge in this respect encompasses both actual knowledge and wilful blindness and suspicion must be given its normal meaning.[156] Accordingly, facts which a person may reasonably be expected to have known or suspected are those facts which would have been reached by a reasonably vigilant and diligent person taking into consideration the general knowledge, experience, training and skill that may reasonably be expected from a person occupying the same position as the reporting party as well as the general knowledge, experience, training and skill the reporter in question actually has.[157]

De Koker provides the following examples of facts which may give rise to a suspicion of possible money laundering:

> "1. When a person provides information that is vague or contradictory.
> 2. A customer that has no record of employment or involvement in a business (past or present) but engages in large transactions on a frequent basis.
> 3. A customer that is reluctant to provide details about his business or funds source or those details are ill-defined.
> 4. A customer who uses a financial institution located far from his home or work.
> 5. A customer who is does not want to disclose other bank or business relationships.
> 6. A customer operating different accounts at different branches of the same financial institution.
> 7. A customer that enters into transactions that out of the ordinary for that particular customer given the portfolio of the client.

[154] Financial Intelligence Centre Act 38 of 2001.
[155] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-14.
[156] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-14.
[157] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-15.

8. The transactions entered into by the client do not appear to have a legitimate business purpose.
9. A customer that makes large or frequent deposits of cash and which do not seem appropriate when considering the profile of the client.
10. A corporate customer who makes deposits or withdrawals in cash more than in other forms.
11. A customer that makes several deposits on the same day at different branches of the same financial institution.
12. A customer who is known to be an economic criminal."[158]

Section 30 of FICA deals with the conveyancing of cash to and from South Africa. When a person wishes to conveyance cash which may be in excess of the prescribed amount across the South African boarder, that person is required in terms of section 30 to report certain particulars regarding the conveyance of such cash to a person authorised by the minister for that purpose.[159] Sections 30(1) and 32(1) of FICA respectively provide for the particulars required to be furnished and for the manner in which these particulars have to be filed.

Section 31 of FICA sets out the provisions relating to electronic transfers of money to and from the Republic. An accountable institution that in terms of this section sends money in excess of a prescribed amount out of South Africa via electronic transfer or receives such a sum from outside of South Africa on behalf of or on the instruction of another person must file a report with the FIC after such a transfer has occurred.[160] Section 32(1) provides that a report made in terms of section 31 must be made in the prescribed manner and section 30(1) sets out the required particulars to be included in the report.[161] The FIC is authorised in terms of section 32 to request additional information from the accountable institution that has furnished the report and as is the case with a section 28 and section 29 report, persons who comply with the provisions of section 31 are protected against any criminal or civil liability provided that they acted in good faith.[162] These persons are also, with the exception of the attorney-client privileged, absolved of any duty of secrecy and confidentiality which may hinder compliance with any obligations in terms of this section of the Act.[163] The

[158] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-16 – 7-17.
[159] Act 38 of 2001.
[160] Act 38 of 2001.
[161] Act 38 of 2001.
[162] Act 38 of 2001.
[163] Act 38 of 2001.

failure to file a report constitutes an offence which is punishable by a fine not exceeding R10 million or imprisonment for a period not exceeding 15 years.[164]

In terms of section 28A of FICA, accountable institutions are obligated to report property that is linked to terrorist activity. This provision was inserted into FICA by the Prevention of Constitutional Democracy against related Activities Act (POCDATARA).[165] An accountable institution must in terms of section 28A file a report with the FIC when the institution learns that it is in possession or control of property that is linked to terrorism. In this regard, section 28A states as follows:

> "(1) An accountable institution which has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of—
> (a) any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004;
> (b) a specific entity identified in a notice issued by the President, under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; or
> (c) a person or an entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1), must within the prescribed period report that fact and the prescribed particulars to the Centre."[166]

Regulation 24(1) of the Money Laundering and Terrorist Finance Control Regulations requires financial institutions to furnish the initial report to the FIC as soon as possible. However, in terms of the regulation that accountable institution has a maximum of five business days to file the report following the establishment of the fact that the institution is in possession or control of property that must be reported in respect of section 28A of FICA by a natural person who is an accountable institution or who is in charge or manages or is otherwise employed by the accountable institution. These reports must thereafter be filed in the prescribed format by the FIC and it is also possible for accountable institutions to furnish the relevant report electronically.[167] In terms of regulation 22A the particulars that must be contained in the report include the details of the reporter as well as details regarding the property involved, the details of

[164] Act 38 of 2001.
[165] Act 33 of 2004.
[166] Financial Intelligence Centre Act 38 of 2001.
[167] Regulation 22 of the Money Laundering and Terrorist Financing Control Regulations.

the controller and the details of persons who have an interest in the property.[168] It is important to note in this regard that an accountable institution is not compelled in terms of section 28A to determine whether it is in control of the relevant property nor is it required to conduct searches for links with terrorist property or names of suspected terrorists in its customer database.[169] De Koker however argues that screening a client's account against information that is publicly available for terrorist activity can reasonably be expected to form part of a well-governed business's due diligence.[170] This would ultimately help business to avoid liability in terms of POCDATARA particularly in the instance where a decision not to screen would constitute wilful blindness or negligent ignorance. It would therefore be difficult for businesses to defend allegations of wilful blindness or negligent ignorance where such screening is standard practice.[171]

Accordingly, a bank who owes a client a duty of confidentiality and secrecy will not breach that duty should it file a report in terms of FICA. The proviso to this, however, is that in order to enjoy the protection provided by FICA the bank must file the report in strict accordance therewith. FICA accordingly overrides the duty of confidentiality and secrecy in South African law. No duty of confidentiality and secrecy or any other statutory or common law restriction on the disclosure of information affects the duty of a financial institution to file a report in terms of chapter 3 (Part 3) of FICA.

The Prevention of Organised Crime Act was enacted with the purpose of *inter alia* introducing measures to combat organised crime, money laundering and criminal gang activities.[172] POCA provides for the civil forfeiture of criminal assets that have been used to commit an offence or assets that are the proceeds of unlawful activity and for the establishment of a Criminal Assets Recovery Account.[173] For purposes of this discussion, the scope of POCA will be limited to its provisions concerning money laundering as well as the provisions concerning investigative and reporting duties.

[168] Money Laundering and Terrorist Financing Control Regulations.
[169] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-44.
[170] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-45.
[171] L De Koker *South African Money Laundering and Terror Financing Law* (2013) 7-45.
[172] Prevention of Organised Crime Act 121 of 1998.
[173] Act 121 of 1998.

Money laundering is regulated in terms of section 4 of POCA which states that:

> "Any person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and—
> (a) enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether such agreement, arrangement or transaction is legally enforceable or not; or
> (b) performs any other act in connection with such property, whether it is performed independently or in concert with any other person, which has or is likely to have the effect—
> (i) of concealing or disguising the nature, source, location, disposition or movement of the said property or the ownership thereof or any interest which anyone may have in respect thereof;
> (ii) of enabling or assisting any person who has committed or commits an offence, whether in the Republic or elsewhere—
> (aa) to avoid prosecution; or
> (bb) to remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence, shall be guilty of an offence."[174]

While FICA expressly imposes reporting obligations on accountable institutions, it is important to note that POCA is a statute of general application, which implies that the commission of an offence is not exclusive to specific accountable institutions but instead, any person may commit an offence in terms of the Act.[175] It is therefore an offence for any person to engage in unlawful activities in circumstances where such a person knew or ought reasonably to have known that they were a party to an agreement, transaction or an arrangement that was materially unlawful and related to proceeds from unlawful activities. An employee of a bank who ordinarily operates with the accounts of clients can in terms of section 1(3) reasonably be expected to know that they are being requested to process a transaction that is materially unlawful if it can be proven that a reasonably vigilant and diligent person in the position of the employee would have known that the transaction in question is unlawful. This can be determined by taking into consideration the general knowledge, skill, training and experience that may be expected from a person occupying the same position as the employee as well as the general knowledge, skill, training and experience the

[174] Act 121 of 1998.
[175] R Ismail 'Legislative erosion of the banker – client confidentiality relationship" 48 (2008) *Codicillus* 3.

employee actually has.[176] A valid defence for a person accused of contravening the provisions of POCA is to prove that they have reported the conduct to the relevant authorities.

In this regard, section 7A of POCA states that:

> "(1) If a person is charged with committing an offence under section 2 (1) (a) or (b), 4, 5 or 6, that person may raise as a defence the fact that he or she had reported a knowledge or suspicion in terms of section 29 of the Financial Intelligence Centre Act, 2001.
> (2) If a person who is an employee of an accountable institution as defined in the Financial Intelligence Centre Act, 2001, is charged with committing an offence under section 2 (1) (a) or (b), 4, 5 or 6, that person may also raise as a defence that fact that he or she had—
> (a) complied with the applicable obligations in terms of the internal rules relating to the reporting of information of the accountable institution; or
> (b) reported the matter to the person charged with the responsibility of ensuring compliance by the accountable institution with its duties under that Act; or
> (c) reported a suspicion to his or her superior, if any, if—
> (i) the accountable institution had not appointed such a person or established such rules;
> (ii) the accountable institution had not complied with its obligations in section 42 (3) of that Act in respect of that person; or
> (iii) those rules were not applicable to that person".[177]

Section 8(1) of POCA states that "Any person convicted of an offence contemplated in sections 4, 5 or 6 shall be liable to a fine not exceeding R100 million, or to imprisonment for a period not exceeding 30 years.

In terms of section 71(1) of POCA:

> "the National Director may request any person employed in or associated with a government department or statutory body to furnish him or her with all information that may reasonably be required for any investigation in terms of this Act and such person shall notwithstanding anything to the contrary contained in any law which prohibits or precludes him or her—
> (a) from disclosing any information relating to the activities, affairs or business of any other person; or
> (b) from permitting any person to have access to any registers, records or other documents, or electronic data which have a bearing on the said activities, affairs or business,

[176] Act 121 of 1998.
[177] Act 121 of 1998.

furnish the National Director with such information and permit the National Director to have access to any registers, records, documents, and electronic data, which may contain such information."

The duty of secrecy is preserved under section 71(3)(a) of POCA. In terms of this subsection, "no person shall without the written permission of the National Director disclose to any other person any confidential information, registers, records, documents or electronic data which came to his or her knowledge in the performance of his or her functions in terms of this Act and relating to the activities, affairs or business of any other person, except—

(i) for the purpose of performing his or her functions in terms of this Act;
(ii) in the course of adducing evidence in any criminal proceedings or proceedings in terms of this Act; or
(iii) when required to do so by an order of a court of law.
(b) Any person who contravenes paragraph (a) shall be guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding 20 years."

4.4 Phishing

The internet has resulted in various advantages for societies across the world. Communicating across geographical boarders is much easier and conducting business transactions across differing jurisdictions is no longer as challenging.[178] These developments, however, have come with their own implications. Nowadays it has become increasingly risky to share personal information on the internet and to conduct commercial transactions because the internet is vulnerable to cyber-attacks.[179] Criminals are using cyberspace to perpetrate criminal behaviours against unsuspecting and vulnerable internet users who rely on the internet to send e-mails, purchase goods, chat on social networking sites and manage their financial accounts.[180] The speed of the internet has also made it difficult for law makers to regulate it effectively.[181]

[178] R Stevenson 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1.
[179] R Stevenson 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1.
[180] F Cassim 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 69.
[181] F Cassim 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 69.

Identity theft is one of the crimes which are committed on the internet as a result of the internet's ability to protect the anonymity of criminals.[182] Identity theft occurs when a person's personal information is wrongfully obtained and thereafter used to commit theft or fraud.[183] The internet is not the only means by which identity theft can be committed as it can also be committed through physical or traditional means, however, with the increasing use of the internet, a more technical approach to identity theft has become increasingly popular.[184] When this criminal offence takes place, the identity thief uses the information to *inter alia* open credit accounts, open bank accounts, purchase merchandise and rack up debts in the victims' names.[185] Thus, personal information is criminally obtained by identity theft, and the identity thieves use the identity-related information or data to commit unlawful activities in the victims' names.[186]

Identity theft is also considered to incorporate phishing.[187] Phishing occurs when criminals use websites and emails to trick online users into disclosing their personal or financial information.[188] According to the Anti-Phishing Working Group, phishing is a form of online identity theft that employs both social engineering and technical artifice to steal the personal identity data of customers and their financial account information.[189] How it commonly works is that an e-mail is sent by a criminal posing as a bank, company or another legitimate organisation to an online user. The criminal then coaxes the user into revealing confidential information regarding the user or such a user's affairs. Therefore, emails are the foundation of phishing schemes. These emails are sent to unsuspecting consumers by criminals falsely claiming to be a bank, government agency, internet service providers (ISP) or any other trusted entity. The e-mails typically contain links to unauthorised web pages created by criminals

[182] F Cassim 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 69.
[183] F Cassim 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 69.
[184] MW Perl 'It's not always about the money: why the state identity theft laws fail to adequately address criminal record identity theft' (2003) 94 *Journal for Criminal Law and Criminology* 170.
[185] MW Perl 'It's not always about the money: why the state identity theft laws fail to adequately address criminal record identity theft' (2003) 94 *Journal for Criminal Law and Criminology* 170.
[186] MW Perl 'It's not always about the money: why the state identity theft laws fail to adequately address criminal record identity theft' (2003) 94 *Journal for Criminal Law and Criminology* 170.
[187] http://www.antiphishing.org/hich/af37/dbch/af37/loch/f37%20.antiphishing.org/ (accessed: 02 October 2019).
[188] R Stevenson 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1.
[189] http://www.antiphishing.org/hich/af37/dbch/af37/loch/f37%20.antiphishing.org/ (accessed: 02 October 2019).

requesting personal information such as identity numbers, social security numbers or passwords.[190]

The growing popularity of online banking in South Africa has led to rising concerns regarding the safety of such transactions.[191] It has been reported that South Africa is amongst the world's most targeted regions for phishing attacks.[192] Internet penetration and broadband accessibility in recent years are cited as two reasons why South Africa has witnessed more attacks than in the past.[193] Another reason for this is the lack of a clear cyber security strategy to engage with the seriousness of online crime and how it can be remedied.[194] An example of one of the most common forms of phishing in South Africa is where criminals use cell phone SIM cards to steal money from an unsuspecting victim's bank account. Once perpetrators have successfully obtained the victim's information from a phishing attack, they fraudulently swap out a victim's SIM card from his or her phone. This is done in order to prevent a victim from receiving notifications from his or her bank informing them that certain transactions are being made in conjunction with their account, such as an added beneficiary to their internet banking profile or a cash withdrawal.[195] The South African Revenue Service (SARS) has also fallen victim to phishing attacks. Fraudulent e-mails claiming to be from SARS have been sent to unsuspecting taxpayers asking them to provide confidential information and their banking details.[196] As a result, SARS has posted alerts regards phishing attacks and related scams on its website. The e-mails were confirmed to be part of a phishing scam and the website was shut down.[197] Another incident involves Standard Bank clients who suffered claims being placed on new debit orders on their Liberty Life Insurance accounts.[198]

---

[190] F Cassim 'Addressing the spectre of phishing: are adequate measures in place to protect victims of phishing?' (2014) *Comparative and International Law Journal of Southern Africa* 412.
[191] http://www.elaw@l/hich/af37/dbch/loch/f37%20egalbrief (accessed: 02 October 2019).
[192] https://www.itnewsafrica.com/2014/04/south-africa-is-second-most-targeted-for-phishing-attacks/ (accessed: 02 October 2019).
[193] https://www.itnewsafrica.com/2014/04/south-africa-is-second-most-targeted-for-phishing-attacks/ (accessed: 02 October 2019).
[194] F Cassim 'Addressing the spectre of phishing: are adequate measures in place to protect victims of phishing?' (2014) *Comparative and International Law Journal of Southern Africa* 412.
[195] https://www.iol.co.za/personal-finance/my-money/banking/how-crooks-use-sim-swaps-to-rob-you-1507185 (accessed: 07 October 2019).
[196] https://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx?k= (accessed: 07 October 2019).
[197] https://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx?k= (accessed: 07 October 2019).
[198] https://www.fin24.com/tech/news/phishing-scam-targets-standard-bank-customers-20150814 (accesssed: 07 October 2019).

Phishing poses a serious problem for banks because it hinders a bank's ability to uphold its obligation to protect the personal information of its customers. This is particularly concerning for banks because a bank's failure to preserve the confidentiality of its client's affairs can result in some harsh consequences for a banking institution and/or its officials.[199] It is therefore important to determine the extent of the bank's duty of secrecy in the event where a customer is a victim of a phishing attack and the bank subsequently and unintentionally shares information with a criminal posing as a customer of the bank. According to Cassim,[200] the Protection of Personal Information Act (POPI)[201] provides some guidance in this regard.

POPI was enacted with the aim of giving effect to section 14 of the Constitution which provides for the right to privacy.[202] In terms of the preamble to POPI, the right to privacy includes protection against the unlawful collection, retention, dissemination and use of personal information. Furthermore, the Act promotes *inter alia* the protection of personal information processed by private and public bodies and provides for the protection of the rights of persons regarding unsolicited electronic communications.[203] POPI seeks to regulate the manner in which personal information is processed by establishing conditions prescribing minimum standards for the lawful processing of personal information.[204]

In terms of chapter 1 of POPI, personal information is defined as "information relating to an identifiable, living natural person and where applicable, an identifiable, existing juristic person". The term "data subject" refers to the "person to whom personal information relates". "Processing" refers to "any operation or activity or set of operations, whether or not it takes place by automatic means, relating to personal information, and it includes inter alia the collection, receipt, recording, storage, retrieval or use of information", whilst the term "record" refers to any recorded information regardless of the form or medium.[205]

---

[199] Protection of Personal Information Act 4 of 2013 s107 – s109.
[200] F Cassim 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 69.
[200] F Cassim 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 69.
[201] Act 4 of 2013.
[202] Constitution of the Republic of South Africa, 1996.
[203] Protection of Personal Information Act 4 of 2013.
[204] Act 4 of 2013.
[205] Act 4 of 2013.

Bearing these terms in mind, Cassim alleges that POPI may be used to address phishing which involves criminals perpetrating fraudulent activity by stealing the identity of a person and proceeding to use such a person's personal information to open bank accounts, obtain credit or to purchase goods and services in the victim's name.[206]

This is primarily because this statute places a duty on companies to respect the personal information of clients and to handle such information with the utmost care and responsibility. In this regard, POPI compels companies to secure the integrity of personal information in their possession or under their control, by taking appropriate and reasonable technical and organisational measures to prevent the loss of personal information and unlawful access to personal information. These companies will thus be forced to implement generally accepted information security practices and procedures to protect personal information in terms of section 19 of the Act which states:

> "(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
>
> (a) loss of, damage to or unauthorised destruction of personal information; and
>
> (b) unlawful access to or processing of personal information.
>
> (2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—
>
> (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
>
> (b) establish and maintain appropriate safeguards against the risks identified;
>
> (c) regularly verify that the safeguards are effectively implemented; and
>
> (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
>
> (3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations."[207]

This provision does not expressly refer to banks but a ''responsible party''. A responsible party in terms of section 1 of the Act means ''a public or private body or

[206] F Cassim 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 69.
[207] Act 4 of 2013.

any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.''[208] Therefore, banks and their employees qualify as responsible parties because they are responsible for the financial accounts of clients.

Failure to comply with the provisions of POPI may result in the issuing of a fine of up to R10 million or imprisonment for a maximum period of 10 years as stipulated in sections 107, 108 and 109 of the Act and a data subject whose personal information has been breached has recourse to civil remedies in terms of section 99 of the Act.

It is submitted that section 19 of POPI therefore reaffirms the duty of secrecy owed by banking institutions to their customers. This is because, in spite of the fact that the internet has made it easier for criminals to perpetrate financial crime and online phishing attacks are on the rise in South Africa, the bank is not by any means absolved of its duty to maintain the confidentiality of its clients accounting records and other personal information. Instead, the onus is on banking institutions and other companies alike to take measures in combating phishing attacks and protecting the confidential information of their clients.

[208] Act 4 of 2013.

Chapter 5:
Conclusion

In the final analysis, it is submitted that the duty of secrecy imposed on banks has been sufficiently limited in order to assist in the combating of financial crime. The duty of secrecy and confidentiality originated from common law, however, the common law recognised that such a duty cannot be absolute as there are other competing interests to which the duty cannot apply. As such, disclosure of a client's personal information is permitted when such a disclosure is in the interests of the banking institution, the interests of the public, where the disclosure is under compulsion by law and where consent has been given in respect of such personal information by the person to whom it relates. These exceptions have been extended by the legislature through the promulgation of legislation aimed at combatting financial crime.

This fact is specifically highlighted under the Criminal Procedure Act which in terms of section 236(1) requires a bank to comply when a court of law compels the bank to furnish information pertaining to a client's account. Although this provision does not exclusively deal with financial crime but all criminal activity which may take place in the republic, it nevertheless shows how a customer's entitlement to secrecy and confidentiality does not triumph over a bank's duty to assist in the administration of justice and by extension, the combating of financial crime. It is also stated in terms of section 37 of FICA that the duty to disclose and report information will override any duty of secrecy owed to the bank's customer whether such a duty is imposed by law or is by agreement. Therefore, although the purpose of the duty is primarily to maintain the confidence of a customer's affairs, it is also acknowledged that criminal activity requires a relaxation of the duty of secrecy in the interests of justice.

Although the duty of banking secrecy and confidentiality has been limited substantially by the anti-money-laundering and anti-terrorism legislation, it cannot be said that there is no longer such a duty in the South African legal system. In this regard, POPI requires companies to implement generally accepted information security practices and procedures to protect the personal information of their customers. Companies who therefore fail to protect the confidentiality of a customer's affairs will be guilty of an offence. While customer's to banking institutions are encouraged to take precautionary measures to protect the safety and security of their personal

details, banking institutions are equally encouraged to pay special attention to online scams and to take reasonable measures to ensure that their online banking platforms are protected from cyber-attacks.

It is further submitted that criminal activity constitutes a transgression against the community at large and as a result, the duty of secrecy ought to be interpreted in the context of the principles of Ubuntu. This is because Ubuntu holds the interests of the greater community in higher regard to those of the individual. Therefore, if a person (or group of persons) compromises the safety, security and freedom of other members of society, as is the case with financial crime, they cannot expect the law to shield them from investigation and possible punishment for their transgressions. It is acknowledged that the section 14 right to privacy includes the right of an individual not to have the privacy of their communications infringed, however, section 14 is subject to the limitation clause set out in section 36 of the Constitution. The right to privacy may therefore ‘’be limited in terms of law of general application to the extent the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom”. Bearing in mind that the court in *Bernstein v Bester* stated that the limitation of the right to privacy can only be done on a case to case basis, taking into consideration the specific facts of the matter in question, it is my submission that customer’s to banking institutions are not vested with an absolute right to privacy. When the facts of a particular matter point to a customer’s involvement in financial crime, the court may limit a customer’s right to privacy in light of section 36 of the Constitution. Furthermore, when a customer entrusts his or her money to a banking institution this constitutes participation in the public sphere and as a result, information pertaining to such a customer’s financial records cannot be absolved from investigation on the grounds of an invasion of the right to privacy when the customer is believed to be involved in the perpetration of financial crime.

-o0o-

Bibliography

Books

Currie I & De Waal J *The Bill of Rights handbook* (2005) Claremont: Juta

De Koker L *South African Money Laundering and Terror Financing Law* (2013) Pietermaritzburg: LexisNexis Butterworths

Devenish GE *A Commentary on the South African Constitution* (1998) Pietermaritzburg: LexisNexis Butterworths

Gyekye J *An Essay on African Philosophical Thought* (1987) Philadelphia: Temple University Press

Mafunisa J 'Enhancing Accountability and Ethics in the Public Service: the case of the Republic of South Africa' in K Frimpong & G Jaques (eds) (1999) *Corruption, Democracy and Good Governance* Botswana: Lightbooks

Mugarura N *The Global Anti-Money Laundering Regulatory Landscape in Less Developed Countries* (2012) United Kingdom: Ashgate

Srivastava A, Simpson M & Moffatt N *International Guide to Money Laundering Law and Practice* 4 (2013) United Kingdom: Bloomsbury Professional

Unge B & van der Linde D *Research Handbook on Money Laundering* (2013) Netherlands: Edward Elgar

Willis N *Banking in South African Law* (1981) Cape Town: Juta

Wilson J 'Corruption is not always Scandalous' in Gardiner, J and Olson, D (eds) (1968) Theft *of the City, Readings on Corruption in America* Bloomington: Indiana University Press

Case law

Abrahams v Burns 1914 CPD 452

Alfred McAlpine & Son (Pty) Ltd v Transvaal Provincial Administration 1974 (3) SA 506 (A)

Bernstein v Bester 1996 (2) SA 751 (C)

Financial Mail (Pty) Ltd & Others v Sage Holdings Ltd & Another 1993 (2) SA 451 (A)

FirstRand Bank Ltd v Chaucer Publications (Pty) Ltd & Anoter 2008 (2) SA 592 (C)

National Coalition for Gay and Lesbian Equality v Minister of Justice and Others 1999 (1) SA 6 (C)

National Media Ltd v Jooste 1996 (3) SA 262 (SCA)

S v Makwanyane 1995 (3) SA 391 (C)

Tourneir v National Provincial & Union Bank of England [1924] 1 KB 461

Journal articles

Amao OB & Dumisa S 'The utility of moral philosophy and professional ethics in the fight against corruption in South Africa: Any role for ubuntu?' (2015) 4 *Ubuntu: Journal of Conflict and Social Transformation* 85 – 111

Cassim F 'Addressing the spectre of phishing: are adequate measures in place to protect victims of phishing?' *(2014) Comparative and International Law Journal of Southern Africa* 380 – 415

Cassim F 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Law Journal* 68 – 110

Du Toit SF 'Reflections on the South African code of banking practice' (2014) 3 *Journal of South African Law* 568 – 679

Ismail R 'Legislative erosion of the banker – client confidentiality relationship' (2008) 48 *Codicillus* 3 – 14

Jackson D 'Financial crime – driven by opportunity, technology and greed…: business' (2015) *Professional Accountant* 8 – 10

McDowell J and Novis G 'Consequences of money laundering and financial crime' (2001) 6 *Economic Perspectives* 6 – 8

Neethling J 'The protection of the right to privacy against fixation of private facts' (2004) 121 *South African Law Journal* 519 – 525

Perl MW 'It's not always about the money: why the state identity theft laws fail to adequately address criminal record identity theft' (2003) 94 *Journal for Criminal Law and Criminology* 169 – 208

Powell S 'Secrecy feeds corruption & secures opulence' (2016) 2 *TFM Magazine* 32 – 36

Schulze H 'Confidentiality and secrecy in the bank-client relationship' (2007) 15 *The Quarterly Law Review For People In Business* 122 – 126

Schulze WG 'The sources of South African banking law – a twenty-first century perspective (part I)' 14 (2002) *South African Mercantile Law Journal* 438 - 462

Shaik-Peremanov N 'Basel II – the right to privacy: a South African perspective' (2009) 21 *SA Mercantile Law Journal* 546 – 554

Smith C 'The banker's duty of secrecy' (1979) 1 *Modern Business Law* 24 – 39

Scott S 'Can a banker cede his claims against his customer' (1989) 1 *South African Mercantile Law Journa*l 247 – 262

Stevenson R 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1 – 15

Legislation

Banks Act 94 of 1990

Criminal Procedure Act 51 of 1977

Companies Act 61 of 1973

Constitution of the Republic of South Africa, 1996

Convention on Preventing and Combating Corruption and Related Offences

Financial Intelligence Centre Act 38 of 2008

Prevention and Combating of Corrupt Activities Act 12 of 2004

Protection of Personal Information Act 4 of 2013

Prevention of Corruption Act 121 of 1998

Promotion of Access to Information Act 2 of 2000

South African Reserve Bank Act 90 of 1989

Prevention of Organised Crimes Act 121 of 1998

Notices and Regulations

Money Laundering and Terrorist Financing Control Regulations

White Paper on Transforming Public Service Delivery (Batho Pele White Paper) Notice 1459 of 1997

Internet sources

https://www.banking.org.za/wp-content/uploads/2019/04/Code-of-Banking-Practice-2012.pdf

http://www.antiphishing.org/hich/af37/dbch/af37/loch/f37%20.antiphishing.org/

http://www.elaw@l/hich/af37/dbch/loch/f37%20egalbrief.

https://www.itnewsafrica.com/2014/04/south-africa-is-second-most-targeted-for-phishing-attacks/
https://www.iol.co.za/personal-finance/my-money/banking/how-crooks-use-sim-swaps-to-rob-you-1507185
https://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx?k=
https://www.fin24.com/tech/news/phishing-scam-targets-standard-bank-customers-20150814