JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 3 (2012)

# The Challenges in Safeguarding Financial Privacy in South Africa

**Naledi Thabang Masete**
LLB, LLM candidate
University of South Africa, South Africa
masetnt@unisa.ac.za

**Abstrac**t. *With the advancement of internet technologies, banks have adopted the use of technologies to improve the efficiency and effectiveness of banking services. These technological advancements have placed legal risks to person's financial information. The existing legislation dealing with the protection of consumer's right to privacy do not adequately protect these rights. Acts such as the National Credit Act 34 of 2005[1] makes it difficult to protect financial privacy as it enables banks to disclose their customers' information that impacts on the customers' right to financial privacy. Due to insufficient regulation of financial privacy, consumer's right to privacy may be compromised. This article will discuss the legal problems encountered in protecting financial privacy in South Africa and questions of balancing the duty of confidentiality and the duty to disclose customer's information.*


## 1. Introduction

With the fast growth of technology, the speed in which internet banking has become popular and the rise of fraudulent cases, it has become a priority for many financial service providers to strengthen their means of protecting their customers' information. Every customer expects financial privacy from their financial institutions. In South Africa, section 14 of the Constitution[2] guarantees everyone a right to privacy and it is protected by common law (law of delict) and the Constitution[3]. There is no specific legislation that deals only with the right to financial privacy.

There is a need to protect financial privacy from being misused or disclosed to wrongful people. Financial information runs a risk of being used to commit fraud and money laundering. On 24 November 2008 it was reported that credit card fraud cost South Africa R420-million in 2007 and it has increased by 146 percent between 2005/2006 and 2007/2008 according to the South African Banking Risk Information Centre (SABRIC).[4] In 2010, credit card fraud losses in South Africa amounted to R22 million, on the national level, the total banking industry's financial losses due to credit card fraud decreased by 36 percent from R409.3 million to R263.8 million.[5] Bank loan fraud is on a rise in South Africa and recently Bloemfontein was affected where fraudulent salary advices from a non-existent company were used for fraudulent bank loan applications.[6] The incidents stated above indicate how consumers' confidential information is at risk and the need to improve the measures used to safeguard financial privacy. The attack on financial privacy is not only South Africa's problem but it is a global problem.

'Traditionally, banks are required to uphold their duty of confidentiality to its customers and to protect the customers' financial information. However, the duty of confidentiality conflicts with certain provisions of the

[1] The National Credit Act 34 of 2005, (hereinafter referred to as the NCA).
[2] The Constitution of the Republic of South Africa 1996 (hereinafter referred to as the Constitution)
[3] Ibid.
[4] http:www.iol-co.za/news/south-africa/credit-card-fraud-hits-r420m, accessed on 30August 2011.
[5] *allafrica.com/stories/201012010137.html , accessed on 30 August 2011.*
[6] http://www.news24.com/SouthAfrica/News/Eight-arrested-for-bank-loan-fraud-20110214 accessed on 30 August 2011.

National Credit Act ( NCA of South Africa)[7] which places a duty on the banks to disclose their customers' information where necessary. Section 69 of the NCA provides for a national register of outstanding credit agreements in which the credit provider will report certain information either directly to the National Register or to the credit bureau regarding the customer's credit information including his/her credit history.[8] In many instances it is the institutions that are entrusted with safeguarding financial information, like bank employees, who infringe on financial privacy of the customers. In South Africa, section 36 is used when there is a conflict of rights, in determining whether the limitation on that right is justifiable.[9]

When dealing with privacy relating to financial issues, the bank has a duty of confidentiality to protect its customers' financial information. English law is also in support of the banks' duty of confidentiality.[10] In some jurisdictions such as the Swiss Law, the banks' duty of confidentiality is based in criminal law and the well-known law is Article 47 of Swiss Federal Banking Law, which was enacted in 1934[11] . In terms of Swiss Federal Banking Law, a bank breaching Article 47 is liable to imprisonment or a fine. There are many problems experienced in protecting financial information. In the course of conducting business we are required to furnish our financial information in instances such as buying a car, opening a bank account and securing a loan. The bank's duty of confidentiality plays an important role in safeguarding financial privacy and this duty is recognised by courts.[12]

The research on which this article is based focuses on the question whether legislation is failing to protect financial privacy. This article will also weigh the rights to privacy against the right to disclose information. The article is divided into four parts. Firstly it will examine the challenges experienced in protecting financial privacy. Secondly, the conflicting duties of banks are examined. Thirdly, the limitation clause is analysed. Fourthly, a conclusion is drawn and recommendations are made on how a new balance might be struck. The discussion on different crimes affecting financial privacy will not give an in-depth analysis of the following crimes, namely, money laundering, identity theft, hacking and fraud.

## 2. Contextualising the concept of financial privacy

In order to understand the concept of financial privacy in the study we examine the definitions of the following words, financial institutions, money laundering, financial privacy, right to privacy and confidential information.

The South African Banks Act defines financial institutions as any authorised financial services provider or representative, includes a bank as defined in the Banks Act,[13] a mutual bank as defined in Mutual Banks Act,[14]or a co-operative bank as defined in the Co-operative Banks Act[15]

In South Africa, the Financial Intelligence Centre Act[16] defines money laundering or money laundering activity 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 or section 4, 5 or 6 of the Prevention Act.

[7] NCA
[8] *Ibid.*
[9] See footnote 2
[10] Article 47 of Swiss Federal Banking Law 1934.
[11] http: www.proeconomics.com/Law/Banking/ Basis of the Duty, accessed on 21 August 2011.
[12] Case and Curtis v Minister of Safety and Security 1996 3 SA 617 (CC) 656-657.
[13] Section 1(1) of the Banks Act 94 of 1990.
[14] Section 1(1) of the Mutual Banks Act 124 of 1993.
[15] Section 1(1) of the Co-operative Banks Act 40 of 2007.
[16] Financial Intelligence Centre Act 38 of 2001.

Financial privacy is defined as a broad set of rights that protect consumers from unlawful access to financial accounts by the government and other bodies, and prohibit financial institutions from revealing financial data to third parties without the authorization of the affected party.[17]

According to Neethling (South African author), the right to privacy consists of all personal facts relating to a person in his condition of seclusion.[18] In South Africa the Constitution provides that "everyone has the right to privacy, which includes the right not to have their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed".[19] The right to privacy creates an obligation on financial institutions to protect the confidential information of their customers.

### *2.1 Confidential information*

It is defined as data, technology, or know - how that is known by a substantial number of persons in a particular industry.[20]

#### *2.1.1 Duty of confidentiality*

Information privacy is the creation and maintenance of rules that structure and limit access to and use of personal data.[21] The duty of confidentiality is defined as a bank's duty to protect its customers' information, to keep the financial information private and secure.[22] The status of being a fiduciary imposes burdensome obligations of good faith on a person[23]. These fiduciary obligations are imposed on trustees, directors of a companies, business partners and agents in relation to their principal. The primary legal consequence is the duty of confidentiality and it is unequivocally stated that there are fundamentally three prosaic legal consequences which ensue because of this relationship, firstly that the bank has to collect in good faith and without negligence cheques remitted to it by a customer, secondly it has a duty to obey its customer's instructions regarding the collection of cheques, effects payable to the customer and payments ordered by the customer and lastly it owes certain incidental duties to its customer.[24] The duty of confidentiality assists in protecting confidential information.

#### *2.1.2 Limitations on the Right to Financial Privacy*

The right to financial privacy is not free from limitation in South Africa, may be limited by statutory limitation or common law limitation. Section 36(1) of the Bill of Rights[25] provides for statutory limitation on the right to financial privacy. Acts of legislation such as FICA and NCA, compel banks to disclose their customers' information where necessary and they statutorily limit the customers' right to privacy. The case of Tournier[26] provides for common law limitation on privacy by laying down four instances in which limitation on the right to privacy is justified. The right to financial privacy is a right protected in the Bill of Rights in terms of section14.[27]

---

[17] http://www.businessdictionary.com/definition/financial-privacy.html, viewed on 21 August 2011.
[18] See Neethling J et el, Neethling's Law of Personality Butterworths Durban 2nd edition (2005) p 30.
[19] Section 14 of the Constitution.
[20] Robert Unikel, 'Bridging the ''Trade Secret'' Gap: Protecting ''Confidential Information'' Not Rising to the Level of Trade Secrets, Loyola University Chicago Law Journal, (1998) Vol.29, p844
[21] Edward J. Janger, Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules, The Symposium: Modern Studies in Privacy Law, Minnesota Law Review (2002), Vol.86, p1223
[22] McKelvey B, Comment: Financial Institutions' duty of confidentiality to keep customer's personal information secure from the threat of identity theft.'
[23] Alastair Hudson The law of Finance, 1st ed, Sweet and Maxwell, 2009, 93. A fiduciary obligation arises when one person has agreed to act in the affairs of another person. 96. Article 47 of Swiss Federal Banking Law of 1934, bases the banks duty of confidentiality in criminal law.
[24] Ellinger's Modern Banking Law, EP Ellinger; E Lomnicka; RJA Hooley 4th ed Oxford University Press 2006 at 117.
[25] See footnote 2.
[26] *Tournier v National Provincial and Union Bank of England (1924) 1 KB 461*
[27] Op cit.

Conditions for limiting the right to financial privacy are provided by section 36 (1)[28] of the Bill of Rights. In terms of section 36(1)[29] "the rights in the Bill of Rights may be limited only 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, taking into account all relevant factors, including:

a) the nature of the right,
b) the importance of the purpose of the limitation
c) the nature and extent of the limitation
d) the relation between the limitation and its purpose ; and
e) less restrictive means to achieve the purpose"

Section 36 (2) provides that except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.[30] When the limitation clause (section 36 of the Bill of Rights) is applied to the privacy right, the latter might be outweighed and compromised. In a situation where the right to privacy is compromised a customer's confidential information may be at risk.

### *2.2 Justification for Disclosing Confidential Information*

The case of *Tournier v National Provincial and Union Bank of England*[31] provides four instances in which limitation of privacy is justified. The qualifications as laid down in the above case can equally be applied in the Republic of South Africa.[32]
The four instances which qualify disclosure of information can be classified under the following circumstances:

- where disclosure is under compulsion by law;
- where there is a duty to the public to disclose;
- where the interests of the bank require disclosure; and
- where the disclosure is made by the express or implied consent of the customer.[33]

#### *2.2.1 Disclosure under compulsion by law*

Banks are compelled by various Acts[34] in South Africa to disclose information when called upon to do so.[35] Those instances include the following acts:

- The Receiver of Revenue is entitled to obtain whatever information he requires.[36]In terms of Section 99, the Receiver may appoint any party, including a bank, as his agent to make payment of any tax due from moneys held on behalf of a customer.[37]

- The Registrar or any person acting under his written authority, in terms of Section 3(2) may at all reasonable times enter upon any premises there to inspect and extract information from or make copies of any document relating to the finances of an affected organisation and may , if in his

[28] *Ibid*.
[29] Ibid.
[30] *Ibid*.
[31] See footnote 26
[32] A B Fourie , The Banker and the Law (1993) p 52
[33] See footnote 24.
[34] Income Tax Act No. 58 of 1962, Affected Organisations Act 31 of 1974, Drugs and Drug Trafficking Act 140 of 1992.
[35] http://www.banking.org Code of Banking Practice/ The Banking Council, accessed on 22 August 2011.
[36] Section 74 of the Income Tax Act No. 58 of 1962.
[37] *Ibid*.

opinion it is desirable for practical reasons, remove any such document to any other premises for those purposes.[38]

- An authorised officer is granted the widest powers for performing his functions, such as submission and seizure of any specified document(s) by any person in possession thereof, or under his control In terms of Section 6(2) (c).[39]

- Section 8(a) and (b) provides that the bank may be called upon to furnish confidential information in respect of his customer to the Auditor-General.[40] In terms of Section 19 (1) the Treasury, or any person authorized by the Treasury, may order any person to furnish any information at such person's disposal which the Treasury as such authorised person deems necessary for the purposes of these regulations and any person generally or specifically appointed by the Treasury for the purpose may enter the residential or business premises of a person so ordered and may inspect any books or documents belonging to, or under the control of such person.[41]

- Section (6) (a) provides that the Director may summon any person who is believed to be able to furnish any information on the subject of the inquiry or to have in his possession or under his control any book, document or other object relating to that subject, to appear before the Director at a time and place specified in the summons, to be questioned or to produce that book, document or other object.[42]

- Section 10 (2) [43] provides that if any director, manager, or executive officer of a financial institution, who has reason to suspect that any property acquired by the financial institution from any person in the ordinary course of the financial institution's business constitutes the proceeds of a drug-related crime, he should advise any commissioned officer of the South African Police assigned to the South African Narcotics Bureau thereof and, at the request of the said police official, to furnish him with such particulars as the official of the financial institution may have available regarding any such person.

- The bank must comply with court order granted against it to furnish information on its customer's account and this is enforced by the courts. A surety is legally entitled to claim information from a creditor (or bank) under Section 10 (2).[44]

### *2.2.2 Duty to disclose to the public*

In England the Criminal Justice Act permits banks to disclose confidential information based on suspicion of a customer's involvement in certain specified offences.[45] In South Africa banks do not have similar protection as in England and legislation should be introduced for banks to furnish the police with such information as the furnishing of information to the police where a customer is suspected of crime would be unwarranted.[46]

[38] Affected Organisations Act No. 31 of 1974.
[39] *Ibid*.
[40] The Auditor-General Act 52 of 1989.
[41] Exchange Control Regulations, Orders and Rules 1961.
[42] Investigation of Serious Economic Offences Act 117 of 1991.
[43] Drugs and Drug Trafficking Act 140 of 1992.
[44] Usury Act 73 of 1968.
[45] Criminal Justice Act 1988.
[46] A B Fourie , The Banker and the Law (1993) p 60.

### *2.2.3 Disclosure in the interest of the bank*

The bank could furnish confidential information to other companies in the group such as banking subsidiaries or one of its non- banking subsidiaries, such as estate agencies.[47] Banks may pass their customers' information to credit reference agencies and this information is useful to the creditors/moneylenders/credit grantors.

### *2.2.4 Disclosure made by express or implied consent of the customer*

There is implied consent of a customer when a surety obtains information on the account he guarantees from a bank and also where the bank gives bank reports to another bank acting on behalf of a customer.[48]

## 3. The importance of protecting financial privacy

In our new information-age society people, organisations, agencies and governments are confronted with threats against, and vulnerabilities of our information infrastructure and information systems. At the same time, our daily economical life and our safety rely more and more on the integrity, availability and reliability of systems and infrastructures.[49] There are indications that obtaining financial advantages by using non-ethical economical attacks is growing given the low chance of detection.[50] Fraud and (organised) financial crime is reported to take place on the information highway, where crime organisations have found their way to go after the non-virtual money.[51]

It remains a concern for customers whether their data collected by the financial institutions will be used for the purpose intended. Customers of financial institutions want to feel that their confidential information is in good hands. Trust is one of the key factors which is associated with successful banking.[52] Trust will develop when the participants to that transaction feel secure and assured that only authorised users have access to information and that the quality of the information being accessed is complete, uncorrupted and easily accessible.[53] Without legislation and common law compelling financial institutions to protect financial privacy adequately most of these financial institutions would not invest in security measures to protect their customers' financial privacy.

Some financial institutions would abuse their customers' information by providing third parties with it without their customers' consent. It would be difficult to hold someone accountable for an act that is not regarded by law as an offence. Employees of financial institutions would see no reason to exercise reasonable care when dealing with customers' information and upholding their duty of confidentiality. Without protecting financial privacy there would be a rise in fraudulent and criminal activities occurring at financial institutions.

---

[47] Suh, B. & Han, I., 2002, Effect of trust on customer acceptance of Internet banking, Electronic Commerce Research and Applications, 1(3/4), 247-263.
[48] *Ibid*.
[49] Luiijf, Eric A.M, Information Assurance and the Information Society ( EICAR proceedings 1999).
[50] Fialka J, War by other means, New York, USA, W.W North, (1997).
[51] See footnote 42.
[52] Bradley, L, Brown, I & Patel, K, 2007, 'The antecedents and consequences of trust in Internet banking', in Proceedings of the 9th annual conference on WWW applications, Johannesburg, September 5-7, 2007, pp. 1-13.
[53] McConnell, J, 1994, National training standard for information system security, accessed 14 August 2011, from http: // www.nstissc.gov/Assets/pdf/4011.pdf.

## 4. Some of the crimes affecting financial privacy

Internet banking in South Africa is estimated to have started in 1996.[54] Technology has made banking easily accessible but at the same time it has created a gap for financial privacy to be infringed. Many bank customers enjoy the convenience, ease of use and relatively low cost of online banking.[55] Internet banking has changed the way in which the business of a bank is done as there is less contact between the bank customers and the bank. In the banking sector, customers can now perform common banking transactions without being inside the bank, such as paying bills, transferring funds, printing statements, and enquiring about account balances online.[56] The nature of internet banking involves the acquiring and processing of sensitive information, such as bank card numbers, personal identification numbers and passwords.[57] It makes it vulnerable to criminal activities.

Statistics have indicated that cellphone banking is the most popular mode of doing online banking in the South Africa.[58]Security concerns are raised amongst the customers surrounding the protection of their confidential information. In South Africa one of the laws aimed at regulating the electronic environment, electronic abuse and computer – related crimes is the Electronic Communications and Transactions Act.[59]Financial privacy is attacked by crimes such as identity theft, fraud, money laundering and hacking. Money laundering is the manipulation of illegally acquired wealth in order to obscure its true source or nature.

Typically, money is laundered through a three-step process: first , the placement stage, where cash is introduced into the banking system or into the retail economy, or often smuggled out of the country, secondly, the layering stage, where money is separated from its origins by passing it through several financial transactions in order to disguise the audit trail and thirdly the integration stage where funds are aggregated with legitimately obtained money.[60] Crimes that may still be employed by investigators and prosecutors in money laundering cases include fraud, complicity (either as an accomplice or accessory after the fact) and defeating or attempting to defeat the ends of justice.[61]

The two statutes that deal with money laundering in South Africa is the Drugs and Drug Trafficking Act[62] which originally criminalized money laundering and the Proceeds of Crime Act.[63] The PCA was problematic because business undertakings that reported suspicious transactions were refusing investigating officers access to documents or records listed in their report without an order issued in terms of Criminal Procedure Act 51 of 1977, this hampered and delayed money laundering investigations.[64] There has not been any conviction for money laundering in terms of the Prevention of Organized Crime Act 121 of 1998.[65] This makes you question whether this Act is effective at all in dealing with cases of money laundering. It is difficult to provide statistics on the magnitude of money laundering in South Africa but some of the observations made about its methods

[54] Kabanda, S.K., Brown, I., Nyamakura, V. & Keshav, J., 2010, 'South African banks and their online privacy policy statements: A content analysis', SA Journal of Information Management 12(1), Art. #418, 7 pages. DOI: 10.4102 / sajim. v12i1.418.
[55] Singh, A.M., 2004, 'Trends in South African Internet banking', Aslib Proceedings: New Information Perspectives, 56(3), 187-196.
[56] Arcand, M, Arle-Dufour, M, Nantel, J. & Vincent, A, 2007, 'The impact of reading a website's privacy statement on perceived control over privacy and perceived trust', Online Information Review, 31(5), 661-681. Cazier, J.A, Shao, B. B. & St Louise, R. D. , 2003, 'Addressing e-business privacy concerns: The role of trust and value compatibility' , ACM symposium on applied computing , ACM, Melbourne, pp. 617-622.
[57] See footnote 40.
[58] *See* fn 17. http://www.worldwideworx.com/2006/11/14/cost-is-the-key-to-cellphone-banking , 'the use of mobile internet services has exploded in South Africa'. Accessed on 15 August 2011.
[59] Electronic Communications and Transactions Act No. 25 of 2002, ( herein after referred to as the ECT Act)
[60] Angela Itzikowitz, (1998) "South Africa: Prevention and Control of Money Laundering", Journal of Money Laundering Control, Vol. 2 Iss: 1, pp.74 – 81.
[61] Ronel van Wyk, 'Current situation and countermeasures against money laundering in South Africa'
[62] See footnote 36.
[63] The Proceeds of Crime Act 76 of 1996 (PCA).
[64] See footnote 23.
[65] *Ibid*.

include; cases where hot money was deposited in bank accounts or washed by buying insurance or other financial instruments and electronic wire transfers to and from South Africa.[66] It is important for financial institutions to identify circumstances in which money laundering is taking place to be able to combat it successfully.

Identity theft is another crime that is a threat to financial information. Identity as an interest of personality can be defined as a person's uniqueness or individuality which identifies or individualises him as a particular person and thus distinguishes him from others.[67] Identity theft is the theft of identity information such as a name, date of birth, Social Security number (SSN), or a credit card number.[68] Identity theft has been described by some as the crime of the new millennium.[69] Any activity in which identity information is shared or made available creates an opportunity for identity theft.[70] Identity theft can result from street theft, stealing of mail, organized crime schemes using computerized databases and bribing of employees with access to customer's personal information. It is estimated that identity theft has become the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society.[71]

Hacking continues to violate financial privacy. South African businesses are powerless to act against computer hackers who are stealing information worth billions of rand from them every year.[72] Companies that have been hit by hackers are reluctant to go public on the incidents because security that is perceived to be penetrable reflects negatively on them. There are no legal safeguards against hackers and under existing laws they are untouchable.[73] South African courts are frustrated when a hacker is caught because they are forced to allow them to get off scot- free.[74]

Cognitive hacking in the context of perception management means gaining access to or breaking into a computer information system to modify certain user behaviours in a way that violates the integrity of the entire user information system.[75] There are two kinds of cognitive hacking, it can either be covert or overt. Overt cognitive hacking is more of a nuisance and embarrassment than a serious threat, includes defacing or spoofing legitimate forms of communication to influence the user and the attacker does not disguise the attack.[76] On the other hand, convert cognitive hacking is likely to have more significant, less predictable consequences and it includes the subtle manipulation of perceptions and the blatant use of misleading information.[77] The attacker tries to disguise the attack.

More needs to be done to improve protection afforded to the user. Application of the law to cognitive hacking and Internet- related areas is volatile, the balance between privacy and security has shifted towards security.[78] Combating cognitive hacking requires either preventing unauthorized access to information assets or detecting posted misinformation before it affects user behavior and therefore countermeasures are needed to detect misinformation.[79]

---

[66] *Ibid*.
[67] See footnote 13, p 36.
[68] Hoar, Sean B, 'Identity Theft: The Crime of the New Millennium', Oregon Law Review , Vol 80, 2001, p. 1423.
[69] REG GUARD (Eugene, Or), Identity Thieves, Apr 30, 2000 at 1A.
[70] See footnote 32.
[71] Rep. John B. Shadegg, *Identity Theft: Is There Another You?: Joint hearing before the House Subcommittees. on Telecommunications, Trade and Consumer Protection, and on Finance and Hazardous Materials, of the Comm. on Commerce*, 106th Cong. 16 (1999).
[72] Gordon Greg, ' Hackers can tap into computers, steal data and get off scot-free' , www.btimes.co.za/97/0601/tech/tech6.htm accessed on 18 August 2011.
[73] See footnote 36.
[74] See footnote 65.
[75] Cybenko George, Giani Annarita, Thompson Paul, 'Cognitive Hacking: A battle for the mind ' Journal Computer Vol 35 Issue 8, August 2002. Accessed on 22 August 2011, http://dl.acm.org/citation.cfm?id=619078&picked=prox&cfid=39306023&cftoken=92565326.
[76] *Ibid*.
[77] *Ibid*.
[78] *ibid* 40.
[79] *Ibid*.

Fraud is affecting financial institutions badly. New account fraud, which involves criminals using false identity, made-up or stolen, to open a new account, typically to obtain a credit card or loan, is becoming a serious concern in our information-based economy.[80] Bank fraud takes place when a person(s) knowingly executes, or attempts to execute, a scheme or artifice to defraud a financial institution or to obtain any of the moneys, funds, credits, assets, securities or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises.[81]

## 5. Legislation that promotes the protection of financial privacy

It is a statutory requirement that banks protect and guard their customers' confidentiality. Directors of Financial Institutions, employees of the bank, officers in the Department of Finance are required to honour their duty of confidentiality to its customers except where legislation supports non-compliance. These are some of the statutes in South Africa that recognise and offer protection to the bank's duty of confidentiality.

### *5.1 South African Reserve Bank Act No. 90 of 1989[82] (SARB)*

Section 33 (1)(a)[83] deals with the preservation of secrecy on financial information and confidential information of bank customers and it prohibits disclosure of any information relating to affairs of the bank, shareholders of the bank or a client of the bank except to the Minister of Finance, Director- General, or for purpose of performing his or her duties or when required to do so before a court of law.[84] Section 33(1)(b)[85] indicates that disclosure of information of a client of the bank requires the written consent of the Minister of Finance and the Governor after consultation with the client.[86]

The bank shall be compelled to produce proof of entries in accounting records and documentation of banks only if it is ordered by the court to produce such records in terms of Section 33 (1) (a) of the SARB.[87] The above Acts govern the protection of confidential information and show that our legislation intends to protect financial privacy of bank customers.

### *5.2 Electronic Communications and Transactions (ECT) Act 25 of 2002*

The main purpose of the ECT Act is to provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.[88] The ECT Act strives to promote legal certainty and confidence in respect of electronic communications and transactions, as well as to safeguard personal information when such information is processed by public and private bodies.[89]

[80] Hartmann- Wendels Thomas et al, 'Determinants of banks' risk exposure to account fraud- Evidence', Journal of Banking & Finance 33 (2009) p 348.
[81] http:// www.fdic.gov/regulations/laws/rules/8000, accessed on 22 August 2011.
[82] South African Reserve Bank Act No. 90 of 1989 (SARB).
[83] *Ibid.*
[84] *Ibid.*
[85] *Ibid*.
[86] *Ibid.*
[87] *Ibid.*
[88] See footnote 25.
[89] Kyobe, M, 2009, 'Factors influencing SME compliance with government regulation on use of IT: The case of South Africa', Journal of Global Information Management, 17(2), 30-59.

Results and analysis of the banks compliance with the ECT Act indicated that 69% of the South African banks sampled posted a privacy statement on their website, the remaining banks lacked a privacy policy statement and the banks that had privacy policy statement, none adhered to all the prescribed by ECT Act.[90] Only 15% of the banks concerned gave customers the option of giving consent for the use of their personal information.[91]

### *5.3 Protection of Personal Information Bill[92] (PPI)*

The Protection of Personal Information Bill is proposes to give effect to the constitutional right to privacy, by safeguarding personal information subject to justifiable limitations, regulating the processing of personal information and by providing rights and remedies to protect personal information. This proposition will adequately protect financial privacy.

## 6. Overview of Legislation Impacting on Financial Privacy

### *Financial Intelligence Centre Act (FICA)[93]*

The FICA aims at governing money-laundering, outlines various measures aimed at facilitating the detection and investigation of money laundering in South Africa and ensures that the Financial Intelligence Centre (FIC) monitors compliance by accountable institutions with FICA's provisions. FICA imposes four obligations on financial institutions, namely, to identify customers, to keep a record of transactions, to report transactions and to train employees (i.e. to comply with FICA's provisions).

Section 22(1)[94] provides that whenever an accountable institution establishes a business relationship or concludes a transaction with a client, it must keep a record, among other things, of the following; the client's identity or the person on whose behalf the client is acting, the manner in which the identities were verified, the nature of the business relationship or transaction, the amount involved and the parties to a transaction, all accounts involved in transactions concluded for a client and the documents utilised to verify the client's identity.

Section 29[95] imposes an obligation on any person who carries on a business, or who manages a business, or who is employed by a business and has knowledge or suspicions about certain activities or transactions to report transactions to the Centre. The obligation to file transaction reports is imposed on three types of persons to which FICA applies: accountable institutions, reporting institutions, and business in general. Section 29(4) precludes a person who filed a report from disclosing the fact to another. Information held by the Centre could only be disclosed in the following five circumstances (s 41(a)- (e) )[96]; in terms of legislation, to further the purposes of FICA, with the permission of the Centre, for the purpose of legal proceedings and when ordered by the court.

FICA affects financial privacy being protected as it imposes obligations on accountable institutions (e.g. banks) to disclose information concerning their customer's activities and to provide records if required. Section 29 imposes a duty to disclose confidential information on accountable institutions (e.g. banks) and places banks in an occurred position as it has to choose between its obligation to protect its customers' financial privacy and its obligation to report its customers' transactions to the FIC. It is difficult for financial institutions to honour

[90] *Op cit.*
[91] *Ibid.*
[92] B9-2009.
[93] 38 of 2001.
[94] *Ibid.*
[95] *Ibid.*
[96] *Ibid.*

their duty of confidentiality towards its customers with these kinds of provisions of statute imposing obligations which impact negatively on their duty towards its customers.

## 7. The National Credit Act (NCA)[97]

The NCA was created to protect consumers from being offered reckless credit and to control the over-indebtedness in South Africa. The National Credit Regulator is responsible to regulate the consumer, credit industry by registering credit providers, credit bureau and debt counsellors in terms of section 14.[98] Section 69(1) empowers the Minister to require the National Credit Register to establish and maintain a single national register of outstanding credit agreements based on information provided to it.[99]

Prospective credit lenders need to have knowledge of the credit standing of individuals with whom they wish to do business , credit agencies fill this gap and usually unfavourable information on the credit worthiness of a person is passed on to the agency , which in turn sells the information to potential lenders.[100] Section 69 (2)[101] requires that the credit provider when entering into credit agreement with consumer must report either directly to the national register the consumer's personal information regarding their agreement, information about the debt amount and the payment agreement.

The bank as a credit provider is compelled to furnish the national register with its customers' financial information and in doing this it fails to uphold its duty of confidentiality towards its customers. The right of a customer to financial privacy is compromised to comply with the NCA. The financial position of a consumer is exposed by the NCA.

## 8. Balancing the Conflicting Duties

There two conflicting duties of a bank, on the one hand the bank is expected to uphold their duty of confidentiality towards its customers and to protect their right to financial privacy while on the other hand it is compelled by legislation to disclosure its customers' information. These two conflicting duties of a bank impact on financial privacy. The right to financial privacy is compromised in instances where legislation compels banks to disclose their customers' financial information and other confidential information it may hold. Balancing the two conflicting duties is proving to be a challenge for banks as they may fail to uphold the duty of confidentiality to its customers. This is evidenced by the failure to protect financial privacy adequately.

## 9. Recommendations and conclusion

Protecting financial information is not an easy task as there are competing interests, which have to be balanced such as providing financial security, right to confidentiality, interests of financial institutions and the task of balancing these opposite interests is a delicate one.[102] A conclusion can be reached that the right to privacy is not absolute as it may be limited in terms of general application and other rights entrenched in the Constitution.[103] Under South African law measures protecting confidential information are very scant.[104] The legislature should

[97] See footnote 9.
[98] NCA.
[99] *Ibid*.
[100] See footnote 39 ,p 61.
[101] See footnote 87.
[102] South African Law Reform Commission/ Privacy and Data Protection/ Discussion Paper 109 Project 124 October 2005.
[103] *Ibid*.
[104] See footnote 13 p 271.

find a proper balance between the fundamental right to privacy and the state's (and its organs ), as well as private persons' need to obtain information about people, based on the public interest and the fundamental rights.[105]

Consumers are protected by the ECT Act. Banks and other businesses should implement the ECT Act by posting privacy policies on their websites. A privacy policy statement is perceived as an important tool, therefore, banks should have a privacy policy statement that adheres to the requirements of the ECT Act, in order to indicate their trustworthiness.[106]

The banking sector should, provide systems which are sufficiently secure and conform to the technological standards that are acceptable. Failure to comply with the law, providing disclaimers excluding any or all liability is not in the best interest of its customers.[107]

Lack of compliance with legislation by financial institutions, should not lead to gratification of striving to protect financial privacy. The legislature needs to enforce strict penalties for non-compliance with the legislation, to ensure accountability.

To facilitate compliance with the Act, there is a need for regulatory bodies, such as the Banking Association of South Africa, which is responsible for establishing and maintaining the best possible platform on which banks can be responsible, competitive and profitable to educate their members accordingly.[108] There is a dire need for co-operation and collaboration between the government, financial institutions, ISP's and private sector for efficient protection of financial privacy. Financial institutions must commit its capital in improving web security systems. The Protection of Personal Information Bill[109] once in force will assist in protecting financial privacy and bringing South Africa in line with international standards.

* * * * *


Cite as : Naledi Thabang Masete, *The Challenges in Safeguarding Financial Privacy in South Africa*, Journal of International Commercial Law and Technology, vol.7 Issue 3 ( July, 2012 )

[105] *Ibid*. p 273.
[106] http://www.persfin.co.za/index/ Personal Finance 2006, 'Banks fail to protect online customers' accessed on 22 August 2011.
[107] See footnote 101
[108] http://www.banking.org.za/ Banking Association South Africa, n.d., The Role of the Banking Association South Africa
[109] B9-2009.