A LEGAL PERSPECTIVE ON THE RISKS RELATING TO INTERNET BANKING

By

Frans Christoffel Booyens

A Dissertation submitted in partial fulfilment for the Degree

MAGISTER LEGUM IN BANKING LAW (BL29XDC2)

UNIVERSITY OF JOHANNESBURG

Supervisor: Prof Charl Hugo

2014

TABLE OF CONTENTS

1 INTRODUCTION

During the last ten years technology evolved to such an extent that it was inevitable that banks would have to adapt their traditional understanding and methods of banking. This led to banks introducing various products and services such as internet banking, mobile banking and e-money.

The advantages of these products are being able to access your bank account on the go, within minutes, without having to go into the bank and having face-to-face interaction. These products are automated and computerised. This decreases the bank's need for human capital and therefore the banks offer these services at lower charges than normal banking as we are accustomed to. Prima facie these new products seem like the ultimate banking experience, being able to effect payment to a creditor outside of banking hours from the comfort of your home with the push of a button and even at lower rates.

This ease of use without face-to-face interaction, however, inevitably led to fraudsters entering the arena with easier methods at their disposal to defraud unsuspecting victims through various trojan horses and man-in-the-mirror techniques which do not require the fraudsters to alter the victim's identity document in order to present it to the bank's teller to withdraw the victim's money. These attacks are highly advanced and the victim will normally not even know that an attack has been launched on his account.

With these new methods of committing fraud, the legislature had to implement certain standards the banks have to adhere to in order to protect sufficiently the bank's customer against these attacks and to avoid the customer suffering losses.

Banks regularly send out e-mails to warn their customers about the risk of fraud being committed on their online accounts. The trends of doing things easier, quicker and with less human interaction, however, clearly bring about new risks that should be investigated.

This paper will investigate the phenomenon of electronic money and what obligations or responsibilities, if any, the bank has in respect of the protection of their customers in an always-evolving world. The conclusion will seek to answer the question as to who bears what risks in this context and the impact this may have on a customer's decision to make use of these services or not.

2 CONCEPT OF ELECTRONIC MONEY AND ITS FUNCTIONS AS LEGAL TENDER

Before examining what constitutes electronic money, one first has to look at the requirements of money as legal tender. Money acts a method to make the economy more efficient. Should you be in possession of a cell phone which you do not need anymore and you are on the lookout for a laptop it would not be an easy endeavour to locate someone with whom to trade. A far easier method will be to sell the cell phone and utilise the money to buy a laptop from your nearest computer shop. Without money this will not be possible.

A lengthy definition of what constitutes money was handed down in *Moss v Hancock*[1] where money was defined as "that which passes freely from hand to hand throughout the community in final discharge of debts and full payment of commodities, being accepted equally without reference to the character or credit of the person who offers it and without the intention of the person who receives it to consume it or apply it to any other use than in turn to tender it to others in discharge of debts or payment of commodities".[2]

What we can gather from this definition is that money must be able to pass freely and by delivery in final discharge of a debt. It must also be accepted as a medium of exchange and must not be any other goods. Further the credit of the person tendering the cash must be irrelevant. And finally the transferee must take it free from claims of the previous owner.

With the electronic era blooming since 1994 in the Republic of South Africa, it was inevitable for the banking industry to develop their services and to offer the general public services such as cell-phone banking, internet banking and accompanying these revolutions, the main attraction, EFT's.[3] This made it possible for the bank's customers with enabled "internet banking" services to pay their creditors without having to go into a bank. At first it was not a common service and the general public took a while to warm up to the idea. The general belief in society was that it was unsecure and risky.

So what constitutes electronic money? A layperson would prefer to refer to "having money in the bank". If someone would analyse the abovementioned saying it would mean leaving your money with a bank and thereafter receiving that same money on demand. However, due to

[1] *Moss v Hancock* [1899]2 QB 111 116.
[2] *ibid*.
[3] Electronic Fund Transfers.

commixtio, the money you deposited becomes the property of the bank and at that time the bank gives you a personal right to request the value displayed on the credit side on demand.

These days most of the population of South Africa uses internet banking. The question which arises is whether we can regard electronic money as legal tender. According to the ECB[4], "electronic money is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer."[5] "The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions."[6]

The European Parliament issued a new Directive on 16 September 2009 in which they set out the legal basis for electronic money. Article 2(1) of the Directive defines an electronic money institution as "a legal person granted authorisation to issue e-money".[7] Furthermore, according to Article 2(2) of the Directive, electronic money means "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer".[8]

On the South African side, the Reserve Bank issued a position paper in 2009 defining electronic money as "monetary value represented by a claim on the issuer. Electronic money is stored electronically and issued on receipt of funds, is generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand."[9]

Electronic money does not qualify as money in the true sense of the word as someone with a bank account only has a personal right against the bank to claim the amount given to it plus the applicable interest generated on that sum.

EFT's do not only entail transferring funds by accessing the bank's secured web-enabled services but also includes automated teller machines, point-of-sales systems and automated

[4] European Central Bank.
[5] ECB Blue Book available at https://www.ecb.europa.eu/stats/money/aggregates/emon/html/index.en.html (26-10-2014).
[6] *ibid*.
[7] *ibid*.
[8] *ibid*.
[9] South African Reserve Bank Position Paper on Electronic Money 1 3 available at https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf(26-10-2014).

clearing houses. An EFT involves the bank's customer giving the bank an instruction to "transfer" funds from his account to the account of the beneficiary. Should the payee and the beneficiary not be at the same bank there will be two banks involved. What will happen in legal terms will be the cancellation of a personal right the payor has against his bank and the creation of a new personal right in the name of the beneficiary against its bank.

The payor bank will then "pay" the beneficiary bank the sum credited to the beneficiary's account. The payee bank doesn't transfer the funds to the beneficiary's bank. It is done through automated clearing houses which settle the sums due between banks. Their role will not be discussed further for purposes of this paper.

Another way an EFT can be effected is through the use of an automated teller machine by inserting your bank card which is nowadays embedded with the new technology known as chip cards, and which is more secure than the traditional cards which only needed to be swiped. Cloning of these cards was of the order of the day. This card acts as a physical token for authentication and enables the customer to transfer money to another account holder or to withdraw cash on demand. The well-known speed points at most retailers are also under the category of EFT's. This facility enables the retailer to receive payment of goods by inserting the card into the machine provided by its bank and the customer then enters his pin whereafter the money is "transferred" to the retailer as described above.

Electronic money can be analysed by the requirements of money to be accepted as legal tender. Firstly it must pass freely and by mere delivery. Electronic money can pass freely and by mere delivery through the clearing process. However, for electronic money to be "transferred" from the payee to the beneficiary, both parties must have a bank account recognised by the other's bank. In respect of the fact that it must pass freely by mere delivery, electronic money passes the test of ownership passing by mere delivery. As soon as the credit is cleared through the clearing houses the beneficiary of the account number receives a personal right to claim the sum displayed to its credit side on demand from its bank.

Secondly it must be accepted in final discharge and full payment of debt. Should the creditor accept to receive payment by means of electronic fund transfer, an electronic funds transfer has the ability to extinguish a debt owed to another party in terms of the underlying agreement. "Upon clearing and reflection in the beneficiary's account, the electronic fund transfer cannot

be reversed legally."[10] The writer is of the opinion that the only exception would be in the situation where fraud was committed. Decisions have gone against banks in South Africa, the best known being the *Take and Save Trading* case[11] wherein the court said: "One may even assume there is no interbank agreement preventing the reversal of electronic transfers... all that being assumed, how can a bank retransfer an amount transferred by A into the account of B back into the account of A without the concurrence of B?"[12] It is suggested that this conclusion of Harms J is correct and that it would be safe to say that an electronic transfer may not be reversed except in the instance of fraud where the beneficiary acted *mala fide*, as there is no ground for reversing it without the beneficiary's consent, and, accordingly, it will be a final discharge of a debt if this is the chosen way of making payment.

The third requirement of money according to the *Moss case*[13] is that it should "be accepted equally without reference to the character or credit of the person who offers it".[14] This seems problematic to start off with as banks issue different cards for different levels of clients and the general understanding is that depending on your financial status you are permitted access to the bank's private-bank services. According to Mann[15] the general idea behind this requirement is that when payment by means of electronic fund transfer has been made, the debtor makes the payment in final settlement of the debt and the beneficiary accepts it as such. Electronic money as described above fulfils this requirement.

Fourthly it should fulfil the requirement of "without the intention of the person who receives it to consume it or apply it to any other use than in turn to tender it to others in discharge of debts or payment of commodities".[16] Electronic money constitutes the client's personal right against its bank to claim the sum displayed on its credit side as mentioned earlier. It is unthinkable to imagine a bank providing goods in repayment of credit to the client and accordingly the beneficiary of an electronic funds transfer will utilise the credit to acquire goods and to discharge the debt owed to his creditors.

---

[10] Schultze "Countermanding an Electronic Funds Transfer: The Supreme Court of Appeal takes a Second Bite at the Cherry" (2004) *SA Merc LJ* 667 675.
[11] *Take and Save Trading CC & others v The Standard Bank of South Africa Ltd* [2004] 1 All SA 597 (SCA) 608.
[12] *ibid*.
[13] *Moss v Hancock* [1899]2 QB 111 116.
[14] *ibid*.
[15] Mann FA *The Legal Aspects of Money* 5 Ed (1992) 1 12.
[16] *Moss v Hancock* [1899]2 QB 111 116.

The South African Reserve Bank's position paper sets out a definition of electronic money and from this we can gather the following characteristics of electronic money:[17]

1) Electronic money is a monetary value represented by a claim on the issuer. This characteristic is discussed above as the personal right a person has against his bank.
2) Money is stored electronically.
3) Electronic money is issued on receipt of funds.
4) Electronic money is generally accepted as payment by persons other than the issuer.
5) Electronic money is redeemable for physical cash or as a deposit into a bank account on demand.

Lawack–Davids[18] takes the view that this Position Paper of 2009 differs from previous versions. The definition now includes that in order to be seen as electronic money, it must be redeemable for physical cash or a deposit into an account on demand. Without this characteristic it would not be seen as electronic money. This would exclude loyalty cards issued by shops on which points are stored which are only redeemable as a discount on your next purchase at selected retailers. This type of credit is thus not electronic money.

Schultze[19] list a few issues in regard to electronic fund transfers, the most important of which includes the "absence of legislation". He points out that "there is at present no legislation in South Africa dealing directly with either payment cards or e–money."[20] The ECT Act[21] only provides a wide and general framework for the facilitation of electronic communications and that it doesn't deal directly with electronic banking services. Schultze is further of the opinion that due to the rapid development of electronic banking, in time, it will disclose more gaps in the ECT Act. South Africa did not, like the USA and several other countries, develop an act designed specifically to deal with electronic banking. Such an act will clear up the current confusion as to whether electronic money is legal tender and same will be properly regulated.

Schultze[22] also mentions that the unilateral conduct by banks since 2002 no longer to accept cheques for more than R5 million indicates that banks are trying to limit their liability. In the

---

[17] Lawack – Davids VA "The Legal and Regulatory framework of Mobile Banking and mobile Payments in South Africa" (2012) *JICLT* 318 322.
[18] *ibid*.
[19] Schultze "E Money and Electronic Fund Transfer. A Shortlist of Some of the Unresolved Issues" (2004) 16 *SA Merc LJ* 50 57.
[20] *Ibid.*
[21] Electronic Communications and Transactions Act 25 of 2002.
[22] Schultze (n 19) 59.

case of a cheque the bank has the obligation to verify the account number as well as the name of the beneficiary while in the case of an EFT the bank only has to verify that the money is paid to the correct bank account number. This might also be a way in which banks are pressurising their clients into switching to the new services they offer via secured websites. "In the absence of dedicated legislation" banks can "unilaterally determine the rules and procedures by which cards and e–money are to be used"[23] says Schultze.

The question accordingly arises whether electronic money can be seen as legal tender. The absence of legislation causes one to wonder whether electronic money in South Africa can be regarded as legal tender. It is submitted that Schultze is correct in his view that South Africa is in need of "dedicated legislation" dealing specifically with electronic money.[24] It is further submitted that South Africa should follow Europe in defining electronic money as per the directive issued on 16 September 2009.[25] Even though we don't have "dedicated legislation" dealing exclusively with electronic money, it can still be seen as legal tender in so far as it fulfils the modern requirements of money. Electronic money fulfils the requirements to be seen as legal tender as it passes freely and by mere delivery when cleared through the clearing houses as mentioned earlier. Payment by means of electronic money can further be regarded as discharging the debt finally as soon as it "reflects" in the beneficiary's bank.

Thomas Greco in his e–book says that the money we use daily is merely a token of the money that was first created as bank credit. The use of cheques and debit cards are merely ways to transfer bank credit from your account to that of someone else. He further states that no credit card is money but that the card allows you to create money by borrowing from the bank. "[I]n order for money to come into circulation, someone must go into debt", says Greco.[26]

Money is merely a way to keep score in the economy. So if money is seen as merely a token of bank credit, we can come to the conclusion that electronic money is legal tender. Hence, as stated by Greco, "money is created by debts owed to the bank and should there be no debt owed to a bank, there would be virtually no money in circulation".[27] Due to the evolution of electronic money and the credit cards accompanying it, it is easier than ever before to borrow

---

[23] *ibid*.
[24] Schultze (n 19) 57.
[25] ECB, Blue Book available at https://www.ecb.europa.eu/stats/money/aggregates/emon/html/index.en.html (26-10-2014).
[26] Greco TH Jnr *Understanding and creating alternatives to legal tender* (2001) 18 available at https://www.community-exchange.org/docs/Greco%20MoneyEbook.pdf(18/11/2014).
[27] *ibid*.

money from the bank. Electronic money and money as we are accustomed to are thus interlinked and both fulfil the requirements to be seen as money.

To quote Greco: "[w]e can see then that the essence of money is an agreement (a consensus) to accept something that in itself may have no fundamental utility to us, but that we are assured can be exchanged in the market for something that does".[28] Electronic money, it is submitted, meets the essence of money and should accordingly function as legal tender.

[28] Greco TH Jnr (n 26) 29.

3 METHODS OF SECURING ONLINE BANKING AND METHODS OF AUTHENTICATION OF CLIENTS

With electronic money making its appearance, inevitably fraudsters entered the arena with their tricks to defraud unsuspecting clients. The bank had to ensure that these new services they offered were safe and secure, and that the possibility of an unknown third party pretending to be a certain customer was eliminated. Although internet banking has developed since it was first introduced to the general public, there are still cases where people are defrauded out of "money" in their account. The most important requirement relating to internet banking is the need for identifying the customer. The customer will nowadays only visit the branch if it relates to services which cannot be executed over the electronic platforms, for example getting a new chip card. Prasad[29] says that "the most important aspect which is checked by banks is the account number and the name of the account holder. Once this identification process is completed, the bank will then check whether the person claiming to be the account holder, is indeed the account holder".

This authentication is essential as whoever logs into an account has full access to whoever's account is logged in. This enables whoever is logged in to access the account holder's funds. As more and "more banks began to offer access to these services, the risks involved came to light such as mala fide access to accounts, fraudulent withdrawal of accounts, phishing and scamming".[30] The general users of internet banking expect banks to provide them with safe and secure access while not making it cumbersome to make use of these services.

Prasad and Kumar[31] set out the various options used under three authentication systems. They are as follows:

[29] Prasad and Kumar "Authentication factors for Internet Banking" (2012) *IDRBT* Working Paper No 11 2 available at http://www.idrbt.ac.in/publications/workingpapers/Working%20Paper%20No.%2011.pdf (13/11/2014).
[30] *ibid*.
[31] *ibid*.

User knows	User possesses	User is
Username	USB Token	Fingerprint
Password	Smart Card	Palm print
PIN	OTP[32]	IRIS
Card No.	SMS/ token	Voice
CVV 2	Swipe Cards	Vein Pattern
3D Secure / VbV	Mobile signature	
Identifiable picture		

The first type of authentication set out by Prasad and Kumar is single factor authentication. This is the most basic authentication method and uses any one of the factors above. This method is the basic method and not secure as it can be easily intercepted.

Secondly, two-factor authentication utilizes a combination of two factors and Prasad and Kumar say that it is the method most used by banks. This entails using two factors, for example using your tablet or smart phone and by entering your password and, secondly, a sms sent to your device. Your device then answers with the correct response, and the two-factor authentication is complete. The initial thought of banks was to implement the two-factor authentication if transactions exceeded a certain threshold. Due to the need that arose in the general public this first notion was reconsidered. These days the two-factor authentication system is even provided for student accounts held at banks.

Thirdly a multi-factor authentication mechanism can be utilised. This entails two or more of the factors set out in the table, of which one needs to be authorised by the "user is".[33] This method will usually be used in large value transfers to ensure the maximum security for both the user and the bank. The bank will do a risk assessment and decide what method to use depending on its risk assessment process. According to the Federal Financial Institutions Examinations Council "this risk assessment should identify all the transactions and levels of access associated with internet based customer products and services".[34] Secondly it should "identify and assess the risk mitigation techniques, including authentication techniques, including authentication

[32] one time password.
[33] The "user is" entails such products as fingerprint and palm readers.
[34] available at http://www.federalreserve.gov/boarddocs/srletters/2005/sr0519a1.pdf (13/11/2014).

methodologies, and authorisation for employees for each transaction type and level of access".[35] Thirdly "it should include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access".[36]

Prasad further states that mutual authentication is often used by banks. "This involves mutual authentication from both parties…This method causes the bank on its website to ask questions after entering the account details but before entering the password."[37] These are answers only the user will know. Upon answering the questions correctly the bank will display a pre–chosen image which will enable the user to determine whether he is in fact on the bank's legitimate website. These images can be stored in three different manners. They are stored either at the bank's side, the client's side or a combination of both the client and the bank's server.

In order to protect these numbers sent via the internet against unwanted interception, a variety of numerical formulas or codes are used to encrypt this information. The developers will try to increase the difficulty in decrypting the information sent by using huge varieties of code and calculations that cannot just be figured out. There are numerous encryption methods: usually they substitute a letter and/or number for another and knowing what false key to change with a real one will enable the receiver to decrypt the information. "For the private sector, the stronger the encryption, the smaller the cause for concern."[38] The US Department of Treasury quoted James Barksdale, the CEO of Netscape, who once said that "security is to the internet what safety is to the airlines".[39] This statement is very important as a lack of security can compromise the whole integrity of electronic money and regular money as money is merely a token of value. Should it be possible to decrypt freely messages sent by banks the whole financial system could collapse, financial loss would occur, unenforceable agreements would be the order of the day and, most importantly, customers' private information would be disclosed.

According to the US Department of Treasury in preparation for the United States Department of the Treasury Conference in 1996, "informal surveys conducted indicated consumers' lack of

[35] *ibid*.
[36] *ibid*.
[37] Prasad and Kumar (n 29) 4.
[38] United States Department of the Treasury Conference prepared for The United States Department of the Treasury Conference (1996) 28 available at http://www.occ.gov/topics/bank-operations/bit/intro-to-electronic-money-issues.pdf (13/11/2014).
[39] *ibid.*

confidence in purchasing goods and services online".[40] Its survey revealed that customers will much rather send their credit card details over the post and furnish same to unknown clerks at shops than to enter their credit card details over the internet. This indicates that there is a real need to educate the general public about the risks involved in entering your details over the internet. Consumers must have trust in their banks that they will ensure that their clients' information sent over the internet is not intercepted. Consumers are also still sceptic about how secure this encrypted information is. The US Department of Treasury realised already in 1996 that consumers are demanding that a trusted third party verify both parties. This brings us back to Prasad's[41] discussion about mutual authentication which leaves consumers feeling protected as the general idea is that they will not enter their details on a fraudulent website.

After looking at the ways banks and other institutions use to secure online banking and other transactions related to electronic money and purchases, we need to look at how these fraudsters try to defraud unsuspecting victims.

The first method and most commonly used is the social phishing method. This method entails the fraudster sending an e-mail to the customer pretending to be someone it would trust like its bank manager. The "bank manager" then requests the customer to enter the website address provided in the e-mail to verify details on its account. You can just click on the link and it will redirect you to a website looking exactly like the real thing. The customer then enters its account details and password and these details are sent to the phisher on the other side. He or she then simply logs in to the bank's real website and transfers money from the customer's account to his or her own. The best way to prevent these attacks is to remember the golden rule of which banks always inform their customers: you will never get an e-mail from the bank requesting you to verify your account details and password. The other way would be not to open any such links in e-mails and merely to enter the normal bank's website address into your browser.

A second manner in which conmen defraud the customer is a more advanced method and requires someone with an advanced knowledge of computer systems and programming. This method is known as "man-in-the-browser" attacks or "man-in-the-mirror" attacks. This method first entails the fraudster installing a computer virus known as a trojan horse onto the

[40] United States Department of the Treasury Conference prepared for The United States Department of the Treasury Conference (1996) 28 available at http://www.occ.gov/topics/bank-operations/bit/intro-to-electronic-money-issues.pdf (13/11/2014)..
[41] Prasad and Kumar (n 29) 4.

customer's computer. A trojan horse infects the customer's computer and the attacker is from that moment "inside the victim's computer". This causes the trojan horse to execute certain pre–set demands in order to fulfil its function. Zhe[42] is of the opinion that "the new trojan horses are technically more advanced by using browser–helper–objects, browser extensions and by using direct browser manipulation techniques".[43] In simpler terms it means that it's a small program that is installed onto the victim's computer which modifies transactions or redirects the victim to bogus websites. There is virtually no need for human interaction and the virus starts doing what it was designed to do. For once the victim opens his browser on the next occasion and types in the bank's website or a secured website where online purchases are to be made, the virus checks the URL[44] from the list of target sites and is activated if it matches one. As soon as a match is found it registers a "button event handler"[45] in the current page and once the button is pressed all the data filled in will be stored. Zhe[46] says that it can even record and modify the value and make the browser continue submitting it. The trojan horse will be in the middle and transfers its certificate to the consumer and encrypts the consumer's message together with its certificate to the bank as the consumer. "The server receives the form and trusts its value and doesn't know whether it was modified or not."[47] The server trusting its validity issues the receipt and forwards it back to the consumer. The trojan horse will intercept the receipt and receives it before the victim. The browser then receives and alters the receipt back to the victim's original request and displays it without the victim knowing what the trojan horse did. The trojan horse is pre-programmed to transfer money from the victim's account to the fraudster's account and the victim is satisfied after his transaction that the transaction went as was instructed by the consumer.

"Thirdly high profile security breaches also pose a huge problem as some of these breaches causethe loss of banking data and credit card data".[48] These high security breaches occur when fraudsters hack into bank and other card companies and steal a database containing clients' confidential information which may cause widespread damages. The bank or other card

[42] Sun Z "Using Two – Factor Authentication Systems to Prevent Social Phishing & man-in-the- mirror attacks for Internet Banking" Dissertation in the Department of Computer Science, University of AucklandPark 1 3 available at https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/zsun.pdf (23/11/2014).
[43] *ibid*.
[44] Uniform Resource Locator.
[45] Sun Z (n 42) 4.
[46] *Ibid.*
[47] *ibid*.
[48] Rutledge GP *Law & Regulation of Electronic Finance & Internet Banking* (2014) 7–8.

companies will carry the losses incurred. These attacks are launched by using a SQL[49] injection to find out where a website's vulnerabilities are. This tactic shows hackers the error messages on the pages and this usually enables them to exploit this vulnerability by inserting a malicious code into the SQL database. SQL injections can also be used to get a website to throw the whole database contents such as account details and passwords to the "hacker". Banks pay large sums of money to prevent such unauthorised entry to the client's account details. Although not unknown this type of hacking is not as common as an attack on a specific individual accountholder.

The banks employ companies to ensure that their clients' account details are secured since insecurity in this regard can cause catastrophic consequences to the economy and to the integrity of electronic money and/or money as we know in paper and coins. There will always be some or other individual with the intellectual capacity to outsmart the common consumer by utilising tactics such as "hacking" in order to gain access to their clients' records. Banks are at present sufficiently protected against these attacks and informed customers can help prevent these unauthorised attacks. As far as high-profile security breaches are concerned, the customer of a bank will merely have some inconvenience as banks are liable for these losses.

[49] An SQL is a special purpose programming language designed to manage data held in a relational database management system. Most databases are based on the relational database model.

4 OBLIGATIONS AND/OR RESPONSIBILITIES IMPOSED ON BANKS AND THEIR CUSTOMERS

As electronic money came with the technology revolution we have experienced since 1994 in South Africa, there has been no specific act promulgated by the South African parliament. This is due to the rapid development of technology. It is therefore necessary to look at other rules which can be applied to transactions relating to electronic money.

The main concerns regarding internet banking are the main obligations banks owe their clients. According to Mthembu,[50] the three points of departure would be to "protect the privacy of the consumer, the bank's duty of confidentiality and safety of the payment". First in regards to the privacy of the consumer: Mthembu is of the opinion that the Bill[51] prior to the Protection of Personal Information Act[52] that is supposed to protect the customer does not offer adequate protection. For purposes of this paper the writer refers to the promulgated Act.[53] According to Section 12 of the Act[54] personal information must be collected directly from the data subject except if the information is contained in a public record or if the information has been deliberately made public by the data subject. "[I]nternet banking undermines the fundamental right of protection of personal information as Banks are allowed to disclose confidential information without consent to other companies in their group".[55]

This is a bold statement which carries weight and is worth discussing. The Constitution came in place to protect people's fundamental rights and each and every person is bound by it. There should be no reason why banks don't fall thereunder. The fact of the matter is that the banks owe their customers the duty to protect their information, thereby also protecting them from loss. The bank won't cause the customer to suffer any damages by disclosing information to other companies in their group. If damages are incurred by the customer, the bank disclosing personal information would carry the costs thereof. Banks will do everything they can to protect this information as their reputation can suffer irreparable damage if their disclosure to other companies in their group causes damages to the customer.

---

[50] Mthembu MA "Electronic Funds Transfer: Exploring the Difficulties of Security" (2010) *JICLT* 201 202–203.
[51] The Protection of Personal Information Bill B9 – 2009.
[52] The Protection of Personal Information Act 4 of 2013.
[53] *ibid*.
[54] *ibid*.
[55] Mthembu MA (n 50) 202.

Secondly, in regard to the duty of confidentiality, in the *FirstRand Bank*[56] judgment handed down in the Cape of Good Hope Provincial Division, the court described the duty of confidentiality imposed on banks. The court also referred to the well know case of *Tournier*[57] wherein the court held that the customer has the right (is entitled) to confidentiality regarding his private affairs. This right arises *ex contracto* or is an implied term of the client and bank agreement. In the judgment handed down by Traverso DJP[58] she held that "the confidential nature of the relationship between a bank and its client has been recognised by several authors and there are also a number of statutory provisions that are based on the assumption that bankers owe a duty of confidentiality to its (sic) clients for example Section 87(2) of the Banks Act".[59]

The only times a bank can disclose personal information is when disclosure is under compulsion by law, where there is a duty to disclose, where the interest of the bank require disclosure and, lastly, where the disclosure is made by expressed and/or implied consent by the consumer.[60]

Thirdly, banks are obliged to ensure the safety of the payment. This obligation is an implied obligation and customers expect the bank to ensure their money isn't stolen from them when utilising internet banking. Customers of the bank do not always have the knowledge to understand internet banking security and "internet banking crime is often difficult to detect because funds can be removed or manipulated by instructions hidden in complex software".[61] With the revolution of the electronic era, only a select few possess the intellectual capacity really to know and understand technology to the extent that they are able to manipulate electronic servers and to use it to their advantage. Mtembu[62] is also of the opinion that these individuals might be committing internet banking crimes "as it offers a sporting element or intellectual challenge which is perhaps as enticing as the opportunity for financial gain".

These individuals may have the superiority complex of being able to outsmart the developers employed by banks. The banks thus have the duty to protect their clients against these select

[56] *First Rand Bank Ltd v Chaucer Publications (Pty) Ltd and another* case no.12645/07 (CPD) (Unreported) 1 Par 19.
[57] *Tournier v. National Provincial & Union Bank of England* (1924) 1 KB 461 483.
[58] *First Rand Bank Ltd v Chaucer Publications (Pty) Ltd and another* case no.12645/07 (CPD) (Unreported) 1 Par 19.
[59] The Banks Act 94 of 1990.
[60] Mthembu MA (n 50) 202.
[61] Mthembu MA (n 50) 202
[62] *ibid*.

few individuals as this is a basic expectation customers have. "The amount of internet banking security violations is difficult to assess at present because there is under reporting of internet banking crime, a lack of information about internet banking security and a lack of informed public discussion... ."[63] This brings us back to having a dedicated act dealing specifically with electronic money and internet banking regulation which can address the disclosure of statistics relating to internet banking crimes as well as force banking institutions to educate the general public to the extent that they are fully aware of all risks that they may face when utilising these services. Currently the obligation is contained in the duty of care owed by the bank to the customer. This, however, causes difficulties as negligence claims can be problematic and difficult to prove.

As mentioned earlier, in South Africa there is no dedicated act dealing directly with electronic fund transfers. This, however, doesn't mean that there aren't binding rules and regulations when it comes to the responsibilities of banks to ensure that the payment system in South Africa isn't compromised. This may very well happen if the integrity of electronic money is compromised. This may have the same effect as an illegal printing press flooding the market with counterfeit notes.

The Basel Committee on Banking Supervision laid down certain principles in July 2003, the so-called "Risk Management Principles for Electronic Banking".[64] Even though the Basel Committee's guidelines aren't binding, they provide a supervisory standard and framework that South African banks follow as non-compliance of a member country will cause other members not to do business with the non-compliant bank.

For purposes of this paper only Principle 4 to 14 will be discussed. They are as follows:

"Principle 4: A bank should take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the internet."[65] The Basel Committee acknowledges that ensuring the authentication of an individual to access to banking systems "in a purely electronic open network environment can be a difficult task."[66] The Committee also sets out that banks must determine which authentication methods they will use based on an assessment of the risks relating to electronic banking. They further stress the

[63] *ibid*.
[64] The Basel Committee on Banking Supervision "Risk Management Principles for Electronic Banking" (2013) available at http://www.bis.org/publ/bcbs98.pdf (23/11/2014).
[65] *ibid.*
[66] *ibid*.

importance of customer identification in transactions involving cross border electronic banking. This is due to the additional difficulties that may arise from doing business over country borders. They further encourage sound industry practise in respect of authentication of their clients. This means:

1) Authentication databases should be tamperproof and protected against corruption, and methods should be in place to record such instances of fraud;
2) Any changes made to an individual bank account should be authorised by the source;
3) Measures should be in place to protect customers from third parties taking the role of the customer;
4) An authenticated session must remain secure for the entire duration of the transaction and if the connection is lost, re-authentication is required.

"Principle 5: Banks should use transaction authentication methods to promote non repudiation and establish accountability for e-banking transactions."[67] The main concern in addressing this situation is the problem that arises when "proof of the origin or delivery of the information isn't recorded. This protects the sender against a false denial by the recipient that the data was received".[68] The Committee lists 2 well-known problems which occur should the accountability of transactions not be properly protected. "They are the potential of hijacking electronic transactions and customers claiming that transactions were fraudulently altered".[69] It is further recommended that:

1) E-banking systems must reduce the likelihood that authorised users will initiate transactions without knowing about them and they must ensure that customers are fully informed;
2) The parties to the connection must be fully authenticated and the connection must remain connected over the authenticated channel for the entire session;
3) All transactions must be protected from changes and all changes must be recorded.

"Principle 6: Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications."[70] It is mentioned that segregation of duties is an internal control measurement. This entails shifting the duties between several employees to prevent one individual internally from defrauding clients or the

[67] *Ibid.*
[68] The Basel Committee on Banking Supervision (n 64) 14 – 15.
[69] The Basel Committee on Banking Supervision (n 64)15.
[70] *ibid.*

bank itself. Employees would have to collude in order to commit fraud if the correct measures are in place internally. "Segregation of duties is critical to ensuring the accuracy and integrity of data."[71] The committee sets out the following guidelines in this respect:

1) The systems should ensure that not one single employee and/or contractor could enter, authorise and complete a transaction;
2) "Segregation should be maintained between the contractors initiating 'static data'[72] and those verifying the integrity";[73]
3) These systems should be tested to ensure that measures can't be bypassed;
4) Segregation should also be between the developers and the contractors administering the systems.

"Principle 7: Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications."[74] This involves maintaining strict control over authorisation and access privileges. This further involves protection of the databases and should the bank realise the system has been tampered with, it should not be further used until replaced with the correct records. It is further sound practise to prevent any changes to the authorisation levels during an e-banking transaction and any changes to authorisation should be brought to the attention of management.

"Principle 8: Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information."[75] The committee[76] stresses the importance of preventing the editing of information in transit and/or databases without authorisation. This aspect addresses the concern of man-in-the-mirror attacks. The Basel Committee[77] sets out the following sound practises to ensure the data integrity:

1) Transactions through internet banking should be resistant to tampering;
2) "Records should be stored, accessed and modified in such a way that they are tamper resistant";[78]

---

[71] *ibid*.
[72] Data that does not change.
[73] The Basel Committee on Banking Supervision (n 64) 16.
[74] *ibid*.
[75] *ibid*.
[76] The Basel Committee on Banking Supervision (n 64).
[77] *ibid*.
[78] The Basel Committee on Banking Supervision (n 64) 17.

3) These transactions should be done in such a way that it would impossible to circumvent the detection of changes by unauthorised individuals;
4) "Monitoring and testing of procedures should be in place to protect against system changes that may erroneously or unintentionally compromise controls or data reliability";[79]
5) Any tampering should be recorded and detected.

Principle 9: Banks should ensure that clear audit trails exist for all e-banking transactions. The difficulty which arises is that in the normal banking environment most people grew up with banking that was done in a branch by the signing and submitting of the necessary documentation. In the internet banking environment all this documentation is in electronic format. The principle of Basel III is to the effect that sound business practise requires the keeping of clear audit trials and to ensure that these electronic audit trails can be independently audited. In this respect they suggest that an audit trail should be kept of the following:

1) Opening, modification and closing of an account;
2) Any transaction with financial consequences;
3) Any authorisation granted by a customer to exceed a pre–set limit;
4) Any granting, modification or revocation of systems' access rights or privileges.

"Principle 10: Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should commensurate with the sensitivity of the information being transmitted and/or stored in databases."[80] This brings us back to the discussion above regarding the bank's duty of confidentiality. The customer wants to utilise the bank's services knowing that the information given won't be disclosed and accessed by unauthorised individuals who will use the information for a purpose other than that intended by the customer. The Basel Committee says that banks need to ensure that:

1) All confidential data is only accessible by authorised persons;
2) "All confidential data is maintained in a secure manner ensuring that it can't be viewed without authorisation or modified over a public, private and internal network";[81]
3) The bank should maintain these measures when third parties have access through outsourcing;

[79] *ibid.*
[80] The Basel Committee on Banking Supervision (n 64) 18.
[81] *ibid.*

4) All access to restricted data is recorded and these records are resistant to tampering through static data.

"Principle 11: Banks should ensure that adequate information is provided on their website to allow potential customers to make an informed conclusion about the bank's identity and regulatory status prior to entering into e – banking transactions."[82] The Basel Committee also sets ground rules in this regard as these risks include legal and reputational risks both locally and across borders. The banks must provide certain information on their websites to minimise these risks. They include:

1) "The name of the bank and location of its head office;
2) The identity of the primary bank authority responsible for the head office;
3) Contact details of the bank's customer service regarding any queries;
4) How customers can access the applicable ombudsman or consumer commission;
5) Access to information regarding deposit insurance schemes and the level of protection they offer;
6) Other information applicable to certain jurisdictions."[83]

"Principle 12: Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services."[84] This principle ensures that the Bank takes into consideration different jurisdictions in which it conducts business. It is important not only to comply with the internal privacy policies and standards but also to have regard to certain extra rules contained in another country regarding privacy laws relating to individuals. The Basel Committee suggests "informing customers in other jurisdictions of the bank's privacy policies and that the general rule is applied that customer's data not be used for any purposes to which the individual did not consent. These measures should also be met by third parties employed by the bank when accessing sensitive data".[85]

"Principle 13: Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services."[86] This principle includes the requirement that the electronic services must be delivered on a consistent

[82] *ibid.*
[83] The Basel Committee on Banking Supervision (n 64) 19.
[84] *ibid.*
[85] *ibid.*
[86] The Basel Committee on Banking Supervision (n 64) 20.

and timeous manner. It is after all the selling point for banks, being able to provide these services 24 hours of the day without delay and this at lower rates than attending the bank. The general principle is that banks must have back-up systems to be able to provide these services even in peak times when the system should be under severe constrains. The Basel Committee suggests the following guidelines:

1) The electronic banking systems should be analysed in light of the overall market dynamics and the projected rate of growth regarding acceptance of internet banking. This will ultimately increase drastically as e-banking grows;
2) "The bank should process the capacity estimates and the stress on the system periodically";[87]
3) Contingency plans should be in place in the event of the systems taking severe strain due to exessive usage by customers and same should be tested regularly.

"Principle 14: Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks that may hamper the provision of e–banking systems and services."[88] This principle boils down to that banks should have the appropriate mechanisms in place to ensure the immediate detection of unexpected events such as an internal breach, and should have the necessary procedures in place to mitigate financial loss including that of outsourced systems.

Although the Basel Committee's[89] principles set out above are not binding on the members, it still carries a lot of weight. The Basel Committee was set up and joined by countries voluntarily. Non-compliance with the standards set out by the committee can have the effect of other member countries refusing to do business with those who do not follow these guidelines. It has, however, no "formal supranational supervisory authority"[90]. The Basel Committee, however, has a Regulatory Consistency Assessment Programme (RCAP) that monitors its members. In its findings in assessing 3 of the members so far, it has shown that compliance by members is stronger and that they have promptly rectified the identified issues. They are further continuing with regulatory reforms.[91] This shows compliance with the guidelines set out

[87] *ibid.*
[88] The Basel Committee on Banking Supervision (n 64) 20 – 21.
[89] *ibid*.
[90] History on the Basel Committee and its Membership (March 2001) 1 available at http://www.bis.org/publ/bcbsc101.pdf (28/11/2014).
[91] Basel Committee on Banking Supervision "Report to G20 Leaders on monitoring implementation of Basel III regulatory reform" (2013) 1 7 available at http://www.bis.org/publ/bcbs260.pdf (11/01/2015).

by The Basel Committee. Customers can rest assured that banks will comply but should they fail to adhere to the guidelines, they are not contravening any act.

The Second set of guidelines is provided by the Banking Association of South Africa in the form of the Code of Banking Practice.[92] This code is also voluntary but all South African banks abide by it. It promotes the key principles of fairness, transparency, accountability and reliability. It further provides for a better understanding of the rights and obligations of both parties. This code also provides mechanisms for complaint resolution. The Banking Association of South Africa undertakes in clause 9.3 to ensure that its internet banking systems and technology are secured and will be regularly reviewed and updated. This is in line with the Basel Committee's[93] guidelines of ensuring that security measures are in place and kept updated.

All South African banks (as members of the Banking Association of South Africa) undertake in terms of clause 9.3:

a) to provide the customer with regular information on how to use internet banking which includes details about the customer's ID, selecting the right passwords and informing the customer of the additional security options available and of the customer's liability for unauthorised transactions;[94]
b) to inform the customer of the terms and conditions relating to the use of internet banking including fees and charges;[95]
c) to advise the customer of transaction limits applying to internet banking services, and that these may change from time to time and are available upon request;[96]
d) to inform the customer of the applicable procedures to report unauthorised access to their information, accounts or disputed transactions and to provide the customer with effective and convenient ways to inform the bank of security incidents and to report the activity as soon as possible;[97] and

[92] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf (05/12/2014).
[93] The Basel Committee on Banking Supervision (n 64) 5.
[94] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf par 9.3.1 (05/12/2014).
[95] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf par 9.3.2 (05/12/2014).
[96] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf par 9.3.3 (05/12/2014).
[97] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf par 9.3.4 (05/12/2014).

e) to ensure that internet banking transactions can be traced and checked as long as they are received by the bank's systems.[98]

Looking at the 5 undertakings made by banks, it is clear that the Basel Committee is on the right track and it is clear that South African banks are incorporating the principles into their guidelines. The banks, however, also incorporated in the Code of Banking Practice,[99] certain duties placed on customers. These duties are not, as previously stated, legal obligations. However, non-compliance can be seen as negligence on the customer's side. Against this background clause 9.3.6 to 9.3.14 of the Code set out the duties for the benefit of the customers. They are as follows:

1) Customers must review their statements and reconcile their accounts regularly;
2) Customers must change their temporary password with their own password and failure to do so will immediately be construed as negligence of the customer;
3) The customer must not reveal his secret access code/password to anyone, especially not to the bank's staff as this can be used to access their account;
4) The customer must change his password/access code immediately if unauthorised access is suspected;
5) The customer must not use the browser function to save the password in order to be entered automatically the next time the website is opened;
6) The customer must preferably type the bank's internet banking website address rather than using a link, and customers must check the site security certificate each time they use these services;
7) Customers must not use computers to access their internet banking to which members of the public normally have access;
8) Customers must install adequate virus and security programs on their computer;
9) Customers mustn't leave their computer unattended when logged in;
10) Customers should treat e-mails, smses or calls with caution and remember that the bank will never ask its client to reveal any details in a letter, sms or e-mail;
11) Clients must ensure that the correct numbers are entered when entering amounts or account numbers (the Code also informs the customer that the bank can't reverse

[98] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf par 9.3.5 (05/12/2014).
[99] https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf (05/12/2014).

payments made more than once or erroneously without the specific consent of the account holder receiving the payment);

12) The customer is to follow the bank's advice (the Code further informs the customer that the bank's website is a good place to be informed on how to stay safe online)"[100].

As mentioned above there is currently no dedicated act in South Africa dealing directly with electronic money and electronic fund transfers. This does not mean that there are no duties. The Basel Committee sets out numerous duties on the banks of all member countries. In South Africa this is reflected in the Banking Association of South Africa's Code of Banking Practice. The Code differs, however, by including duties that are imposed on the customer. This is not a legal standpoint *per se* in South Africa but should either party fail to adhere to these basic duties, it can be proven in court to be negligence.

In South Africa the legislation that must be applied to electronic money is firstly the South African Reserve Bank Act[101] which states that the bank is required to implement such rules and procedures and, in general, to take the steps required to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems. Apart from these duties, "the Reserve Bank also has the power to issue position papers in order to set out its regulatory stance."[102]

As pointed out by Lawack "[a]lthough position papers do not have the same legal binding power as directives, they are usually followed because of the Reserve Bank's moral persuasion powers."[103] She further states that "although the South African Reserve Bank has issued 3 position papers in this regard, they have not yet issued one dealing directly with electronic money or payments made by electronic money".[104] She further states that the Reserve Bank's powers extend to issue "a special directive which sets out its stance in the Position paper that must be complied with; otherwise the Reserve Bank may apply to court to compel a person to comply with the directive issued."[105]

This power granted to the South African Reserve Bank can resolve the problem we currently have which is the lack of a dedicated act. The Reserve Bank can take a stand and issue appropriate directives. Compliance with such directives can be enforced by a competent Court.

---

[100] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf (05/12/2014).
[101] 90 of 1989.
[102] Lawack VA "Mobile Money, Financial Inclusion and Financial integrity: The South African Case" (2013) 318 *WJLTA* 322 326.
[103] *ibid.*
[104] *ibid*.
[105] *ibid*.

5 WHO CARRIES THE RISK?

The benefits of internet banking attract customers and banks' attention. This far outweighs the risks involved when making payment through the bank's internet banking website. The banks implemented internet banking and all that goes therewith, like ATM's, cell-phone banking, electronic money etc. as this increased their geographical range of business. Further it allows the bank to offer its services 24 hours a day without having to have their doors open to the public. For clients and banks alike it offers many advantages, being able to effect payment sitting at home with reduced bank charges. All these advantages encourage the customer to join the technological era which includes internet banking. This advantageous service, however, is not infallible and people are sometimes defrauded out of large amounts of money. The public is not always informed of these statistics; banks prefer not disclosing this information as it also amounts to a disclosure that their security can be penetrated. The customers who are defrauded will also often agree keeping the breach confidential in return for the "money" back in their accounts.

Thus far in South Africa there hasn't been much reported case law dealing with the legal position of electronic money. Therefor it is necessary to look at foreign case law in order to analyse upon whom the risk for breaches in the security falls.

In the *Patco*[106] case heard in the United States the facts were as follows. Over a period of one week Ocean Bank authorised six fraudulent withdrawals worth $588 851.26 from the account of Patco after the fraudsters correctly entered Patco's customized security question answers. All six transactions were red flagged by Ocean Bank's security systems in regards to the timing, value and geographical location of Patco's usual payments. Patco was not informed of these red flags and payment went through. The sum of $243 406.83 was recovered by the bank leaving Patco with a loss of $345 444.43. Patco had been a client of Ocean Bank from 1985. They added internet banking in September 2003 and made weekly transfers on Fridays from their offices and weekly deductions went off for tax contributions. These transfers were made from a single static IPaddress[107] from one of the office computers and never for more than $36 634.74.

---

[106] *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6.
[107] A static internet protocol address is a number that gets assigned to a computer by the internet service provider.

Patco firstly alleged that the bank's security system was not commercially reasonable under article 4A- 202 of UCC.[108] This article sets out the duty of the bank to ensure that its security measures are commercially reasonable. This is a question of law to be determined by considering the wishes of the customer expressed to the bank and the circumstances of the customer known to the bank, which includes the size, type and frequency of payment orders normally issued to the bank. Alternatively security procedures offered to the customer and security procedures in general used by the customer should be evaluated.

Secondly Patco alleged that it didn't consent to the procedures and the bank was thus negligent. This allegation translated back to the mandate that exists in the customer-bank-relationship. The other allegations were breach of contract, breach of fiduciary duty, unjust enrichment and conversion. The court of first instance heard the application for summary judgment and entered judgment in favour of Ocean Bank holding that its systems were commercially reasonable and that the claims thus had to fail. The judgment was taken on appeal and the United States Court of Appeals for the First Circuit[109] had to decide what obligations and/or responsibilities were imposed by Article 4A on Patco as the customer and the Ocean Bank.

When Patco requested internet banking in September 2003, it entered into several agreements with the bank, one of which was the "eBanking for Business Agreement". This agreement *inter alia* stated that the bank will not be responsible if the internet banking is used by an unauthorised person as any use of the password constitutes payment by the customer or on his behalf. It further excluded Ocean Bank's responsibility for any transmission of sensitive data (hence Patco bore this risk). In this regard it further provided that the bank could only have attracted liability for gross negligence limited to 6 months of fees. Further Patco had to contact the bank immediately on discovery of unauthorised access.

It was alleged that sometime before May 2009 the bank published its amended e-banking agreement in terms of which the customer assumed all the risk and liability. The bank reserved the right to modify the terms and conditions at any time with effect from the date of publication. Patco denied that these modified terms and conditions were applicable to it as they had not been published on the website before May 2009 and could not apply retrospectively. The fraudulent transfers were made during the beginning of May 2009.

[108] Uniform Commercial Code.
[109] *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6.

In respect of Article 4A[110] the court had to decide whether Ocean Bank complied with the obligation imposed on banks to have commercially reasonable security procedures. The court analysed the six security measures Ocean Bank had in place to decide whether its security measures complied with the code.[111] The bank outsourced its security regarding internet banking to a third party. The security measures employed by them included the following:

1) User ID's and passwords: The systems required each employee of Patco who was authorised to access by entering their user specific ID and password.[112]
2) Invisible device authentication: This entails placing a cookie in the internet browser which helps with a secure connection between the customer and the bank. It contributes to the statistics and verifies whether the account was accessed from the regular computer. Whenever the cookie is changed or is new, it will trigger potential security questions to the user attempting to access the internet banking services.[113]
3) Risk profiling: This entails the service provider analysing the statistics from each logging previously done on the account. Risk is assessed by looking at *inter alia* cookie ID's, geographical location, and transaction activity. Should the score be more than 750 out of 1000, additional security questions are asked and the transaction is red flagged.[114]
4) Challenge questions: Patco had 3 pre-selected challenges and responses. If the threshold exceeded a score of 750 the questions will be asked. Should it be entered wrongly 3 times, the customer will have to attend the bank with their ID document to change their details.[115]
5) Dollar amount rule: This security measure allows the customer to set a threshold in dollar amount to which the challenge questions would be asked. Patco set the limit to $100 000.00 in August 2007 and lowered it to $1 in June 2006. This meant that the security questions had to be posed every time.[116]

[110] Uniform Commercial Code.
[111] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 9-11.
[112] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 9.
[113] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 9 -10.
[114] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 10.
[115] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 10 - 11.
[116] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 11.

6) Subscription to the e-fraud network: Ocean Bank was provided access to the e-fraud services. The e-fraud network allowed financial institutions to report certain IP's connected with instances of fraud and would not even allow the fraudster to attempt to enter the response to the challenge questions if the IP address matches one on their list. Ocean Bank further implemented notification of the trigger by email to its customers.[117]

Ocean Bank had several extra security features available to subscribe to but chose not to. These security features were *inter alia* as follows:

1) Out-of-band-authentication: This authentication refers to additional steps being taken beyond the technological boundaries of a transaction. It includes notification to customers, "call back" verification and cell phone based responses/processes.[118]
2) User selected picture: As discussed earlier in chapter 2, this authentication method is an anti-phishing method. It involves the bank displaying a pre-selected picture after the account details are entered but before the password is entered. This ensures the customer is verifying that he is in fact visiting the correct website of the bank.[119]
3) Tokens: Tokens involve a device the customer possesses like a usb token device or a password generating token.[120]
4) Monitoring of risk scoring reports: The bank had the ability to monitor manually the risk scoring reports and conduct regular reviews but failed to do so. They could further contact the customer if fraud was detected.[121]

The court examined Article 4A of the UCC[122] and held that the parties may not vary any rights and obligations arising under Article 4A. The court further held that this article causes a bank receiving a payment order ordinarily to bear the risk of loss of any unauthorised fund transfers. The bank, however, can shift the loss of any unauthorised transfer to the customer in one of

[117] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 11 - 12.
[118] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 13.
[119] *ibid.*
[120] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 13 – 14.
[121] Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 14.
[122] Uniform Commercial Code.

two ways. "One involves the commercial reasonableness of the security procedures and one does not."[123]

Firstly the bank has to show that "the payment order received...is the authorized order of the person identified as the sender if that person authorised the order or is otherwise bound by it under the law of agency".[124] The court further held that "if the sender of the payment order had no authority to do so and there are no additional facts on which estoppel can be found, the customer will not be liable for the loss which loss the bank will bear".[125]

Secondly the court discussed another way the bank can shift the loss of the unauthorised access to the customer. This involves investigating whether the security measures are commercially viable. The court held that if "a customer and bank agrees that the authenticity of payment orders in the name of the sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order expressed by the client if:

1) The security procedure is a commercially reasonable method of security against unauthorised payment orders; and
2) The bank can prove that it accepted the payment order in good faith and in compliance with any written agreement or instruction of the customer."[126]

As discussed above, the court has to determine whether a security system is commercially reasonable in terms of Section 4A-202.[127] The court held that the article is explicit and does not depend on whether the bank utilised the best available security measures. The determination is rather whether the procedure was reasonable in regard to the customer and particular bank. This makes it reasonable towards banks as the costs involved in the high end security measures fall back to the bank and ultimately the customer. Therefore it is necessary to evaluate the risks involved in relation to each particular customer. The court also stressed the "importance of

[123] *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6 23.
[124] *ibid*.
[125] *i* Patco Construction Company Inc v People's United Bank t/a Ocean Bank 684 F 3d 197 78 UCC Rep Serv 2d 6 24.
[126] *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6 24-25.
[127] Uniform Commercial Code.

evaluation of each customer as the beneficiary bank is in the best position to evaluate the security procedures to combat fraud".[128]

Article 4A-202 of the UCC[129] states that to determine reasonableness the court has to consider the following:

1) "Whether the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer";[130] and
2) "The customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer."[131]

The loss then shifts from the receiving bank to that of the customer should the bank prove the commercial reasonableness of the security procedure and that it accepted the payment order in good faith in line with instructions or agreement between the parties. The agreement will cause the consumer to accept liability in writing to be bound by a payment order.

The customer can then shift the risk of loss back to the bank in terms of Section 4A-203(2).[132] This Section states that the receiving bank is not entitled to enforce or retain payment of the payment order if the customer proves that the order was not caused, directly or indirectly, by a person:

1) "Entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure";[133] or
2) "Who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the

[128] *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6 26.
[129] Uniform Commercial Code.
[130] *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6 26.
[131] *ibid.*
[132] *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6 27.
[133] *ibid.*

> information was obtained or whether the customer was at fault. Information includes any access device, computer software, or the like."[134]

Section 4A-203(2)[135] thus places the obligation on the customers to ensure that their systems and confidentiality are not breached by any of their employees. This insurance of confidentiality at the client's side will allow the client to shift the risk of loss back to that of the beneficiary bank and the bank must thus refund the customer its "money" together with interest.

In the *Patco* case[136] it was alleged that a zbot malware[137] was installed in Patco's browser add on. The court, however, did not make a ruling in this regard as it was reserved as a matter to be dealt with at trial. The court reversed the decision of the court of first instance to grant summary judgment in favour of the bank as the court was of the opinion that Ocean Bank's systems were not commercially reasonable. This was due to the fact that the bank knew that keylogging was a major problem at that stage and had to foresee that security measures had to be implemented against this.

The court further held that the common law claims of breach of contract and breach of fiduciary duty are not inherently inconsistent with Article 4A[138] and could in theory be by way of contract or assumption of fiduciary duties, which imposes a higher duty of care on banks.

The court further overturned the decision to dismiss Patco's claim and reversed the judgment granted in favour of Ocean Bank. The court further advised that it would be more favourable for both parties to settle out of court considering its judgment. The court examined the question whether customers will bear some of the losses when the bank's security systems are found to be unreasonable but did not provide an answer. The Judge, instead, recommended that the parties settle out of court. The parties ended up settling and Patco was compensated by Ocean Bank in the sum of $500 000.00.[139]

---

[134] *ibid.*
[135] *ibid*.
[136] *Patco Construction Company Inc v People's Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6.
[137] Trojan Zbot is a trojan horse that attempts to steal confidential information from the compromised computer. It can also download numerous application files and update them over the internet.
[138] Uniform Commercial Code.
[139] Available at http://www.bankinfosecurity.com/choice-escrow-fraud-case-settled-a-7301 (16/11/2014).

A more recent judgment was handed down in the *Choice Escrow* case[140] where the court of first instance's decision was also taken on appeal. The facts of the matter were as follows. Fraudsters stole the sum of $440 000.00 from Choice Escrow and Land Title LLC, a real estate escrow service. The money was transferred to an overseas account in the Republic of Cypress. Their account was held at Bancorp South Bank. Choice utilised the internet banking services Bancorp offered to effect payments from its trust account to the sellers at closing in their normal business as an escrow agency.

The security measures used by Bancorp were that firstly these payments were made using the bank's online banking platform "InView". Each employee with access to the online banking was assigned a username and password and to gain access the users would be asked to enter their details.

Secondly Bancorp installed authentication software called "Pass mark". This software caused it to record the IP address when the user first registered for InView. If the InView services were accessed from another IP address or from a computer with different specifications as the first recorded one, the program automatically would pose challenge questions. Should the answers be supplied correctly the computer would also be added to the list.

Thirdly Bancorp allowed its customers to place a dollar limit on their accounts per day and any amount above this pre-set amount would be denied. Choice failed to place a daily limit on its account.

"Fourthly Bancorp offered its customers a service called 'dual control'."[141] This involved one authorised user submitting a payment order. This order would not be sent to the bank immediately and a second authorised user would have to authorise the payment order before it was sent to the bank. "If a customer declined the use of 'dual control', Bancorp required that customer to sign a waiver acknowledging that they waived dual control and understood the risks involved in the single authentication system."[142] Choice enquired to Bancorp about limiting their foreign transfers and was informed that this service was not available. Bancorp further enquired whether Choice would like to take up the "dual control" services which Choice declined as an unsuitable option due to their requirements from internet banking.

---

[140] Choice Escrow and Land Title, LLC v Bancorp South Bank No 10-03531 CV S JTM.
[141] Choice Escrow and Land Title, LLC v Bancorp South Bank No 10 03531 CV S JTM 1 4.
[142] *ibid*.

A short while thereafter Choice was defrauded by a fraudster who installed a computer virus which had the account details and password and sent it to a third party. It further mimicked the required IP address and computer specifications. The district court granted summary judgment in favour of Bancorp and Choice took it on appeal.

The court held that "one of the liabilities balanced by Article 4A[143] is the risk that a third party will steal a customer's identity and issue a fraudulent payment order to the bank".[144] The court held further that there are only two exceptions where the risk of loss shifts to the customer. It was further held that the first circumstance is rare in that the bank can seldom prove the identity or the authority of the person who sent the message. It is accordingly unusual for the bank to be able to prove the customer authorised the order or is bound to it by the law of agency.

The court further held in the *Choice* case[145] that "Article 4A of the UCC[146] permits the bank to protect itself from liability by implementing 'commercially reasonable security procedures' and accepting the payment order in good faith and in line with the customer's written instructions".[147]

The court *a quo* interpreted "a security procedure" and came to the conclusion that only security measures established by agreement are considered security procedures. Section 4A[148] clearly states that "a security procedure is a procedure established by agreement of a customer and receiving bank for the purpose of verifying that a payment order is that of the customer."[149] This clearly places the obligation on the bank to offer all the necessary security procedures it deems essential to protect the customer's account. By agreement the bank will then activate and deactivate the security measures as instructed by the customer. The court thus considers the security measures offered by the bank and whether the customer agrees to use same.

The "only exception to the established by agreement"[150] is when the bank offers the customer an additional security procedure and the customer decides not to utilise the procedure in

[143] Uniform Commercial Code.
[144] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531 CV S JTM 1 8.
[145] *ibid.*
[146] Uniform Commercial Code.
[147] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531 CV S JTM 1 9.
[148] *ibid*.
[149] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531 CV S JTM 1 10.
[150] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531 CV S JTM 1 10.

accordance with another standard procedure; and, further, that the customer agrees in writing to bear the risk of loss if that declined procedure is commercially reasonable.

The court had to evaluate the *Bancorp* case[151] and firstly came to the conclusion that according to the facts of this matter the program Pass mark was not mentioned in any of the written agreements between the parties. However, it was not possible to run the InView program without installing Pass mark. The court held that an agreement under the UCC[152] doesn't need to be a written agreement and it is necessary to differentiate between an agreement and a contract. The UCC clearly states that "an agreement means the bargain of the parties in fact, as found in their language or inferred from other circumstances".[153] The court held that in this case the security procedure was established by agreement.

The court further discussed the multi factor systems as dealt with in chapter 2 and said that in 2010 these authentication systems might have already been inadequate. Due to technology evolving at a rapid speed, new methods are discovered to manipulate computer systems. They are able to mimic the IP addresses and specifications of their victim's computers and to obtain authorised employees' access details in order to defraud the customer.

The court suggested the security measure Bancorp had in place called "dual control". This involves one employee making a payment order and another approving the payment by logging in with their own details. This method works very efficiently as the fraudsters will have to get the details of both authorised employees which are very unlikely as they would normally access the internet banking services from their own computers respectively. The court concluded in this instance that Bancorp's security procedures complied with the standards in general use by customers and receiving banks.

The court further had to analyse whether the security procedures were suitable for Choice. The court also had to consider "the wishes of the customer expressed to the bank and the circumstances of the customer known to the bank".[154] This includes size, type and frequency of payment orders normally issued by the customer to the bank. It came to the conclusion that a customer declining a security procedure which is commercially reasonable, in this matter "dual control", will cause the court to accept that "the customer has voluntarily assumed the risk of

---

[151] *ibid*.
[152] Uniform Commercial Code.
[153] *ibid*.
[154] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531 CV S JTM 1 12.

failure of the procedure and cannot shift the loss to the bank".[155] This is reasonable as the bank cannot be held liable after the customer insisted on a higher risk procedure because it is cheaper and more convenient.

Finally the court discussed the last requirement Bancorp had to prove, namely, "whether it accepted the payment order in good faith and in compliance with a security procedure".[156] This depended on whether there was a written agreement or instruction, and only then the customer could shift the risk of loss back to the bank in terms of Section 4A-203(2).[157] The Court held that in order for the bank to prove it accepted the payment order in good faith when its security measures were commercially reasonable, the bank merely had to prove that its "employees executed a payment order in a way commensurate with the customer's reasonable expectations, as established by reasonable commercial standards of fair dealing".[158] If the employees of the bank fail to notice an unsuspicious payment order it does not constitute bad faith of the bank. Only when there was a clear indication that a payment order is suspicious in that a flag is raised and the bank fails to notice it, would the bank not satisfy the burden of proof.[159]

Grenova and Eloff[160] in their article on the risks involved in the South African context analysed an occurrence of identity theft during the period of May and July 2003 at ABSA Bank. They are of the opinion that the bank may, in such an event, theoretically be charged criminally, but that this is unlikely due to the fact that "the desirability of criminally prosecuting a corporate body has always been a controversy".[161] They further list each of the elements of fraud and are of the opinion that in regard to misrepresentation, the bank makes itself guilty thereof when they fail to inform the customers of the potential risks. Banks thus misrepresent by "creating a false sense of security".[162]

They are further of the opinion that the elements of fraud, namely prejudice and unlawfulness, can be found in the bank's inactions and that "it may in no way be argued that the inactions of the bank are lawful or not prejudicial to the customers".[163] They further state that the element of intention is the only aspect which might be problematic. It is, however, present as the bank

[155] *ibid.*
[156] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531n CV S JTM 1 18.
[157] *ibid*.
[158] *ibid.*
[159] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531n CV S JTM 1 20.
[160] Grenova & Eloff "South African Online Banking: Who carries the Risk?" (2004) No 11 *Computer Fraud and Security* 1 2 available at http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/081.pdf (11/01/2014).
[161] Grenova & Eloff (n 160) 5.
[162] *ibid.*
[163] *ibid.*

then had the intention not to disclose the existence of spyware. The solution of criminal prosecution of banks is said to be unreasonable bearing in mind that the actions of the fraudster may also cause losses to the bank.

In regard to civil liability Grenova and Eloff[164] state that the bank can be held liable in delict by using the *Acquilian* action for negligence when it has claimed to provide secured online banking. They further take the view that if they keep quiet on the importance of security and the obligations of the customer to ensure security of his computer, they fail to fulfil their duty of care and make themselves guilty of negligence.

The writer agrees with their opinion that banks in general market their online services by distributing free software and educating the public about internet banking. They do this as "the standard of care required by South African law goes as far as to require that a person or organisation has done everything reasonable expected from it by the society at large".[165] This places a huge responsibility on banks to ensure that the public is sufficiently informed in order to escape liability. Should they fail to do so they could be held accountable for the losses of people falling for scams designed to catch out "stupid people".

They further state that the customer can also claim from the bank based on contract and that these claims would be based on implied warranties and misrepresentation. Implied warranties are there to protect the customer and to ensure fair dealings in the market. Grenova and Eloff[166] say that through representation and certain circumstances implied warranties become part of the contract between the customer and its bank. This is due to "the assumption that it is reasonable for the customer to assume that their (sic) money is safe in the bank, which is sound and therefor valid".[167] Secondly they state that the clients can't request the bank to change their terms and conditions and therefor the rule of he who drafts the contract, owes a heavier duty towards the other, applies.[168]

In regard to misrepresentation as mentioned above, Grenova and Eloff are also of the opinion that due to the bank's misrepresentation at the time that the ABSA incident occurred, the general public was informed not "to give or make available their PIN and account details and

---

[164] Grenova & Eloff (n 160) 6.
[165] *ibid.*
[166] Grenova & Eloff (n 160) 9.
[167] *ibid.*
[168] *ibid.*

that the bank will be liable if loss is incurred due to the Bank's negligence or internal fraud".[169] They are further of the opinion that the bank's customers did comply as they did not give or make available their pins but that they were in fact stolen.[170] This misrepresented to the community that internet banking is safe as long as customers do not give out or make available their account details and passwords. They were thus under the impression that the bank will in this instance be liable for any loss suffered.

Grenova and Eloff further point out that "[a]ll banks in South Africa have terms and conditions drawn up and the customer may not make use of the internet banking services if they do not accept the terms and conditions".[171] They state further that although these terms and conditions contain a clause that the bank will not be held liable for any damage whatsoever, the bank will not be able to rely thereon as the ECT Act[172] read with the King II Report on Corporate Governance overrides such a provision.[173] This places the responsibility of ensuring security on the website owner.

The advantages of internet banking are *inter alia* the following:

1) The convenience of being able to do your banking any time of the day;
2) The convenience of logging in at any time to view balances of any of your accounts;
3) Reduced rates when utilising internet banking;
4) The transfer of funds in payment of an account via EFT; and
5) The speed of internet banking.

The disadvantages of internet banking are *inter alia* the following:

1) Losing the personal relationship formed between customers and, for example, their bank managers;
2) Security risks such as man-in-the-mirror techniques as discussed above;
3) The learning and navigating of the complex computer systems on the bank's website can be cumbersome for some customers.

[169] *ibid*.
[170] Grenova & Eloff (n 160) 12.
[171] *ibid*.
[172] Electronic Communications and Transactions Act 25 of 2002.
[173] Grenova & Eloff (n 160) 10.

The question that finally arose is whether the advantages outweigh the disadvantages, of which the security concern plays the biggest role for customers. Guangying[174] is of the opinion that trust plays the most important role in whether the customer will make use of the services of internet banking. He is also of the opinion that trust is built up by banks by them promoting privacy and security. People want to feel that their hard earned money is safe and secure and if that isn't the case they would much rather use traditional methods of banking even if it means paying the normal bank charges applicable. Banks know this and therefor they ensure that they comply with the applicable legislation such as the ECT Act[175] and codes such as the Code of Banking Practice.[176]

It is in the bank's best interest as the alternative is to have security procedures which are commercially unreasonable and which will cause the bank to accept the risk of loss. "Privacy and security do not, however, exist independently."[177] He further states that they must co-exist with each other as "their transaction data is important to customers but even more so as the privacy of their profiling data as this is associated with their financial status." [178] Disclosure of a wealthy customer's profiling data can make him a target for fraud as his financial position attracts fraudsters. It is thus extremely important to keep this information private failing which the customer may suffer losses.

[174] Hua G "An Experimental Investigation of Online Banking Adoption in China" (2009) Vol 14 No 1 *JIBC* 1 5.
[175] Electronic Communications and Transactions Act 25 of 2002.
[176] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf (05/12/2014).
[177] Hua G (n 174) 5.
[178] *ibid*.

6 CONCLUSION

Money in its traditional form evolved to such an extent that it will eventually be replaced by us having only electronic money. Money is merely a token of bank credit. So viewed, electronic money can fulfil the requirement of money in the traditional sense. Therefore electronic money can be seen as legal tender.

There are numerous authentication and security procedures that are readily available to banks offered by independent third parties. These security procedures, however, are expensive and the bank has to decide on appropriate security procedures for each specific customer. The bank cannot implement all security procedures as this would make internet banking more expensive and unnecessarily cumbersome (for example in that logging in would require multiple authentication methods).

The Basel Committee sets out numerous principles as guidelines to its member countries. It can be seen in the Code of Banking Practice[179] wherein the guidelines are set out as undertakings by all South African banks with the addition of placing certain obligations on the customer. The position papers of the South African Reserve Bank can be issued and compliance with them can be enforced in a court. Thus far a special directive dealing with electronic payments or payments made by EFT has not been issued by the South African Reserve Bank.[180]

Currently there is no dedicated legislation but that does not mean that there are no obligations on banks and on their customers. According to Mthembu[181] banks have the duty to ensure that they adequately "protect the privacy of the consumer, trustworthiness of the retailer and the safety of the payment itself".

Article 4A[182] of the UCC places certain obligations on the bank and its customer but cannot bevaried by the parties. Article 4A also causes a receiving bank ordinarily to bear the risk of loss of any unauthorised payment orders. There are two ways in which the receiving bank can shift this risk of loss placed on the bank to the customer. Firstly the risk will shift to the customer if the bank can prove that the payment order received was authorised by the customer or that he will be bound to the order under the law of agency.

---

[179] Available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf (05/12/2014).
[180] Lawack VA (n 102) 326.
[181] Mthembu MA(n 50) 202-203.
[182] Uniform Commercial Code.

Secondly the risk can be shifted to the customer if the receiving bank can prove that its security systems are commercially reasonable and that the bank accepted the payment order in good faith and in compliance with any written agreement or instruction of the customer.

In order to be "commercially reasonable" the bank has to prove that the customer refused a security procedure after it was commercially reasonable to have this specific security measure. The procedure offered must provide adequate security for that customer and the customer must expressly agree to be bound by a payment order which is accepted in compliance with the security procedure chosen by him. The security procedure also has to be by agreement but this agreement doesn't mean that it must be a written contract. It can be oral or implied.

In regard to accepting the payment order in good faith and in compliance with security procedures and written agreement or instructions, the bank merely has to prove that its employees executed a payment order in a reasonable way as can be expected by the customer, and as established by reasonable commercial standards of fair dealing.[183] The risk of loss then shifts back to the customer except if the customer can prove that the payment order was not made by any person entrusted with the account details employed by the customer. This causes the customer to ensure the privacy of its account details.

As the bank is burdened by its duty of care owed to the customer, it distributes free software and informs the general public of the correct facts. Banks are generally burdened with a duty of care to inform the public of the correct facts and to ensure that they are properly informed.[184] This places the duty of care on banks. An informed public will ensure that the banks' customers utilising internet banking, know and understand the risks involved in using internet banking. They must further be informed of the fact that there will be consequences to declining a security procedure merely for the reason of inconvenience. As long as the customer accepts the security procedures offered by the bank and ensures that the security breach does not directly or indirectly occur from any of its employees entrusted with the account details, the bank will generally accept liability for unauthorised payment orders. Although there is no dedicated legislation in South Africa dealing directly with internet fund transfers, the legal position is relatively clear. The guidelines and UCC[185] strive to reach a balance between the bank offering electronic transfers and the customers with no prior knowledge in regard to the risks and procedures available to these systems with endless possibilities.

---

[183] *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531 CV S JTM 1 19.
[184] Grenova & Eloff (n 160) 8.
[185] Uniform Commercial Code.

Internet banking is still relatively new in South Africa but, as discussed[186] by Guangying, the general public utilises internet banking services when they have trust in the bank that their financial status and information won't just be revealed and accessed by fraudsters. The internet offers endless possibilities and customers should not be scared off from utilising these services with countless advantages. Even in environments without technological elements there are always fraudsters and customers should not decline internet banking due to the fact that it is relatively unknown to them. They also need not fear that they will suffer losses as these incidents are isolated.

[186] Hua G (n 174) 5.

SOURCE LIST

BIBLIOGRAPHY:

BOOKS

- Greco TH Jnr *Understanding and creating alternatives to legal tender* 2001 1 18 available at https://www.community-exchange.org/docs/Greco%20MoneyEbook.pdf (18/11/2014)
- Mann FA *The Legal Aspects of Money* 5 Ed (1992).
- Rutledge GP *Law & Regulation of Electronic Finance & Internet Banking* (2014).

ARTICLES

- Grenova & Eloff "South African Online Banking: Who carries the Risk?" (2004) No 11 *Computer Fraud and Security* 1 2 available at http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/081.pdf (11/01/2015).
- Hua G "An Experimental Investigation of Online Banking Adoption in China" (2009) *JIBC* Vol 14 No1 1 5.
- Lawack-Davids VA "The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa" (2012) *JICLT* 318.
- Lawack VA "Mobile Money, Financial Inclusion and Financial Integrity: The South African Case" (2013) 318 *WJLTA* 322.
- Mthembu MA "Electronic Funds Transfer: Exploring the Difficulties of Security" (2010) *JICLT* 201.
- Prasad and Kumar "Authentication factors for Internet Banking" (2012) *IDRBT* 11 2 available at http://www.idrbt.ac.in/publications/workingpapers/Working%20Paper%20No.%2011.pdf (13/11/2014).
- Schultze "Countermanding an Electronic Funds Transfer: The Supreme Court of Appeal takes a Second Bite at the Cherry" (2004) *SA Merc LJ* 667.
- Schultze "E Money and Electronic Fund Transfer. A Shortlist of Some of the Unresolved Issues" (2004) 16 *SA Merc LJ* 50.
- Sun Z "Using Two – factor Authentication Systems to Prevent Social Phishing & Man – In – The – Mirror Attacks for Internet Banking" Dissertation in the Department of Computer Science, University of Aucklandpark available at

https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/zsun.pdf
.

TABLE OF CASES

- *First Rand Bank Ltd v Chaucer Publications (Pty) Ltd and another* case no.12645/07 (CPD) (Unreported).
- *Choice Escrow and Land Title, LLC v Bancorp South Bank* No 10 03531 CV S JTM 1.
- *Moss v Hancock* [1899]2 QB 111.
- *Patco Construction Company Inc v People's United Bank t/a Ocean Bank* 684 F 3d 197 78 UCC Rep Serv 2d 6.
- *Take and Save Trading CC & others v The Standard Bank of South Africa Ltd* [2004] 1 All SA 597 (SCA).
- *Tournier v. National Provincial & Union Bank of England* (1924) 1 KB 461.

LEGISLATION AND DIRECTIVES

- ECB, Blue Book available at https://www.ecb.europa.eu/stats/money/aggregates/emon/html/index.en.html (26-10-2014).
- Electronic Communications and Transactions Act 25 of 2002.
- European Parliament 2009 Directive available at https://www.ecb.europa.eu/stats/money/aggregates/emon/html/index.en.html (26/10/2014).
- South African Reserve Bank Position Paper available at https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem (NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf. (26-10-2014).
- The Banks Act 94 of 1990.
- The Protection of Personal Information Act 4 of 2013.
- The Protection of Personal Information Bill B9 – 2009.

REPORTS

- Basel Committee on Banking Supervision "Report to G20 Leaders on monitoring implementation of Basel III regulatory reform" (2013) 1 7 available at http://www.bis.org/publ/bcbs260.pdf (11/01/2014).
- The Basel Committee on Banking Supervision "Risk Management principles for Electronic Banking" (2013) available at http://www.bis.org/publ/bcbs98.pdf (23/11/2014).
- Code of Banking Practice available at https://www.fnb.co.za/downloads/legal/Code-of-Banking-Practice-2011.pdf (05/12/2014).
- Federal Financial Institutions Examinations Council available at http://www.ffiec.gov (13/11/2014).
- US Department of Treasury in preparation for the United States Department of the Treasury Conference in 1996 available at http://www.occ.gov/topics/bank-operations/bit/intro-to-electronic-money-issues.pdf (23/11/2014).