Consumer protection in online payment methods

by

Henry Ndejapo Tshapumba Aderam

18243861

Submitted in fulfilment of the requirements for the degree

LLM Mercantile Law

In the Faculty of Law,
University of Pretoria

October 2019

Supervisor : Mrs Sylvia Papadopoulos

Acknowledgements

This research is an outcome of collective efforts and rightly so I would like to express my gratitude to those who have helped me throughout this academic journey. First and foremost I would like to thank God for being a source of spiritual strength. Then I would also like to thank my parents and elder brother Pichard Aderam for creating an enabling environment, in which I could realise my dreams of studying at such a prestigious university. Lastly, I express gratitude to Mrs Sylvia Papadopoulos for her constructive criticism and guidance which has assisted me throughout this journey.

I dedicate this research to myself for having an unrelenting spirit in pursuit of my aspirations.

Abstract

This research focuses on online payment methods which are premised on electronic funds transfer. It is a general discourse that the use of online payment methods is risky. It is held that the fear of fraud and abuse of a payment system is at the focal point of such risk.

Banks which provide these payment systems are usually not prepared to negotiate with their prospective customers. Resultantly, banks contract out of the risk associated with online payments, specifically the liability for unauthorized electronic funds transfers. This culminates in bank's customers bearing the majority of that risk as a result of the bank-customer contract.

Some of the laws applicable to this relationship also ascribe to the notion above. They burden bank's customers solely with the liability of the use of their cards until notification to the bank of its theft or misuse. This shows a completed disregard of the nature of how online payment methods operate.

Such imposition of liability is excessively one-sided in favour of the banks and detrimental to the bank's customers. Ultimately, the scope of application of the current applicable consumer protection laws is limited by factors such as non-applicability to juristic persons or limitation based on asset value for those that do. This thus denotes a large segment of online payment methods users who cannot avail themselves to measures of protection provided for by the current applicable consumer protection laws.

The research aims to avert the issues as demonstrated above, provide clarity in pursuit of equity and compliance, plus a comprehensive consumer protection approach for online payment methods users.

Table of Contents

1. Chapter One: Introduction

1.1 Introduction

The use of online payment methods forms part of various banking services which constitute a great part of our daily lives. Online payment methods specifically form part of a bank's methods of payments which in itself is quite wide. These refer to payment systems which use new methods to initiate payment instructions and ultimately the transfer of value. Payment systems in this regard denotes a set of arrangements of which the primary function is the transfer of value.[1]

The definition of a bank is not quite clear with statutes rather focusing on defining the business of a bank.[2] Nevertheless, a bank is defined as a juristic entity that advertises the taking of deposits from the general public in its ordinary course of business and grants loans, finances businesses and invests the money received as deposits.[3]

A bank's customer on other hand is defined as any person who has opened a current account with the bank which agrees to accept such a person as its customer.[4] However it is also widely accepted that a person who makes use of a bank's services in the ordinary course of their business is also regarded as a bank's customer.[5]

This research will focus on online payment systems which are premised on electronic funds transfer. That is payments by way of systems making use of electronic techniques only and those instances where electronic payment systems have an influence in paper-based payments.[6] The nature of these payments is such that there

[1] D Swart 2000 "Online banking law and payment systems". In R Buys (ed) *Cyber law @ SA The law of the Internet in South Africa* (2000) 278.

[2] WG Schulze "Banks and Banking Law" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 12 -13.

[3] MW Jones "The Relationship between the Bank and the Customer" In MW Jones & HC Schoeman (eds) *An Introduction to South African Banking and Credit Law* (2006) 2.

[4] Jones (2006) 2.

[5] A Ramdhin "The Bank-Customer Relationship" In Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 112.

[6] Swart (2000) 283.

is no physical movement of coins or notes, what is rather involved is a succession of mandates that result in the crediting and debiting of creditor's and debtor's accounts.[7]

A debtor who intends on paying a creditor by means of a credit transfer is referred to as an originator by virtue of their instructions to their bank which is called the originator's bank. The beneficiary whose account is credited is referred to as the creditor and the relevant bank in this instance is referred to as the beneficiary bank.[8]

It is common cause that there may be other banks involved as well in these transactions which play an intermediary role. These banks only execute payment orders given to them by the banks earlier in the chain and are thus referred to as intermediary banks.[9]

The role of a bank in these payments is not a representative one, the bank acts as a mandatory for its customers. The bank also accepts payments on behalf of its customer from non-customers as well.[10] The bank as a mandatory has the duty to ensure performance of a customer's order timeously, in good faith and without negligence. The banks must also ensure a safe and efficient security system.[11]

Despite the above, it is a general discourse that the use of online payment methods is risky. It is held that the fear of fraud and abuse of payment system is at the focal point of such risk. The risk of fraud may be at the hands of fraudulent websites or even the employees of trustworthy websites.[12] Furthermore, there is an increase in the use of information and communication technology by banks which is still far from being safe and secure.[13]

For instance, in December 2010 Bankserv Africa processed a total of 67 million credit and debit card transactions at point of sale terminals and over 65 million electronic

[7] FR Malan *et al Malan on Bills of Exchange, Cheques and Promissory Notes* (2009) 276.

[8] FR Malan & JT Pretorius "Credit Transfers in South African Law (1)" (2006) THRHR 597.

[9] *Ibid.*

[10] Malan & Pretorius (2009) 279.

[11] Malan & Pretorius (2009) 280.

[12] S Eiselen "E-commerce" In D Van der Merwe (ed) *Information and Communication Technology Law* (2008) 191.

[13] *Ibid*.

funds transfers.[14] Financial losses as result of credit card fraud on the other hand amounted to R403,15 million between 2010 and 2011 an increase of 53 % from R263,8 million.[15]

1.1.1 The bank-customer relationship

This relationship which postulates rights and duties for the respective parties is the focal point of the consumer protection analysis *in re* online payment methods. This relationship is mostly governed by a contract in which banks usually contract out of the risk associated with online payments despite the perceived inherent risk.[16] A typical clause to this effect would prescribe that a bank will not be liable for:

> "*any loss or damage arising from the client's data directly or indirectly caused by malfunction of the bank's system, third-party systems, power failures, unlawful access to or theft of data, computer viruses or destructive code on the bank system or third-party systems, programming defects, or negligence on the bank's part*."[17]

It is observed that the underlying reason for evading liability by the banks is owing to the fact that, these payment systems involve large amounts of money amongst large commercial entities and financial institutions, and that these transactions are quick and inexpensive.[18] If banks were to incur liability, they would be liable for huge amounts. The ease with which fraud can be used to effect an electronic transfer is also observed as another reason.[19]

It is a well-established principle in terms of our law that the nature of the law of contract is based on freedom of contract.[20] This principle postulates the liberty to decide

---

[14] CJ Nagel *Commercial Law* (2016) 484.

[15] T Budhram "Lost, Stolen or Skimmed -Overcoming credit card fraud in South Africa" (2012) SA Crime Quarterly 31.

[16] S Eiselen "E-commerce" In D Van der Merwe (ed) *Information and Communication Technology Law* (2008) 192.

[17] Eiselen (2008) 195.

[18] VA Lawack-Davids & FE Marx "Consumer protection measures for erroneous or unauthorized internet payments : some lessons from the European Union?" (2010) Obiter 452.

[19] C van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 372.

[20] *Sasfin v Beukues 1989 (1) SA 1 (1).* At paragraphs 7 – 10.

whether or not to contract; with whom to contract; and on what terms to contract.[21] It is observed that freedom of contract operates from a notion that the parties to a contract negotiate from equivalent positions. This is indeed not the case as factors such as necessity may be the underlying reason for entering a contract.[22]

The use of online payments is for instance greatly necessitated by banks limiting the maximum cheque value to R50 000.00 despite bank's customers generally enjoying more statutory protection in respect of cheques, than in the case of electronic transfer of funds.[23]

There is also a sense that freely concluded contracts should be enforced. This may prove to be displeasing where there contract referred to above is a standard form contract and as such presents no opportunity for negotiation.[24] In light of the above, freedom of contract may potentially be flawed and the exclusion of liability for banks is presumably unfair.

1.1.2 Applicable laws

The laws referred to in this section will serve as the basis on which the bank-customer relationship will be assessed. The discussion of these laws will be brief as an in depth discussion is realised in the following chapters.

The Electronic Communications and Transactions Act[25] governs automated transactions which is the way by which some of the online payment methods are initiated.[26] It mandates banks as suppliers within the context of the Act to provide secure payment systems with regards to accepted technological standards, failure of

---

[21] D Hutchison "The nature and basis of contract" In D Hutchison (ed) The Law of Contract in South Africa (2012) 23

[22] P Aronstam *Consumer Protection, Freedom of contract and the Law* (1979) 14.

[23] Available at; http://www.pasa.org.za/home/2019/07/30/media-statement---reduction-in-maximum-cheque-value; Last accessed on [08 February 2020]; C van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 370; WG Schulze "E Money and Electronic transfers: A shortlist of some of the unresolved issues" (2004) SA Merc LJ 64.

[24] WG Schulze "E Money and Electronic transfers: A shortlist of some of the unresolved issues" (2004) SA Merc LJ 58.

[25] 25 of 2002.

[26] Section 20.

which will result in the liability of a bank for any damages suffered by a user of the said system as a result of a bank's failure to comply with this duty.[27] However, this duty will not be applicable in instances where the bank's customer is a juristic person. This owing to fact that, the ECTA does not apply in instances where a consumer as the user of the payment system is not a natural person.[28]

The Protection of Personal Information Act[29] applies to the processing of personal information which is necessary to the processing of an EFT. It establishes certain obligations and rights to parties involved in such a process.[30] Specifically, the duty of a responsible party (bank) to ensure the security of processing personal information,[31] will be assessed to establish its impact.

The National Credit Act[32] deals with the liability for lost or stolen cards or other identification devices.[33] It's application is limited to credit agreements, the effect of which is an extension of credit having in an effect in South Africa.[34] It provides that a credit provider should not impose liability associated with the use of a credit card on the consumer after the consumer has informed the credit provider of the theft or loss of such credit card or pin.[35] The impact of this provision is that a consumer is solely liable for the risk of unauthorized transactions until he or she informs the card issuer, responsibility thereafter shifts to the card issuer.[36] This Act is applicable to EFT transactions being processed by virtue of a credit card.

The Consumer Protection Act[37] is the overarching legislative framework for consumer protection. Relevant to the discourse at hand is the right to fair, just and reasonable

---

[27] Section 43(5).

[28] Section 1.

[29] 4 of 2013. See chapter 3 at paragraph 3.4 for a detailed discussion.

[30] Chapter 3.

[31] Section 19.

[32] 34 of 2005.

[33] Section 94.

[34] Section 4; Section 8.

[35] Section 94(2).

[36] T Budhram "Lost, Stolen or Skimmed -Overcoming credit card fraud in South Africa" (2012) SA Crime Quarterly 32.

[37] 68 of 2008.

terms and conditions for consumers.[38] Factors such as excessive one sidedness which entails benefit for one party only, and adverse effect on the consumer are indicative of unfairness.[39] These are the factors that the study is going to rely on in the determination of the fairness of banks' exclusion of liability in online payment methods clauses.

Despite these provisions, the application of the CPA is also limited. It does not apply to transactions where the consumer as a juristic person has an asset value or turnover equal to or in excess of R2 000 000.00.[40]

1.2 Motivation

The research was invoked as a result of the competing interest between the use of technology on one hand and the associated risks on the other hand. More so, the growing use of online payment methods in effecting payment, the perceived associated risk and the absence of legislation that specifically deals with the subject matter has also greatly contributed to it. The unequal power dynamics existing between banks and their customers has further served as motivation for the study.

Foreign jurisdictions such as the United States of America and European Union have more advanced laws dealing with the subject matter specifically. They ascribe to different capping of liability of unauthorized payments with due consideration of different circumstances, overall liability with due consideration of different circumstances and plausible imposition of the burden of proof in proving that a purported unauthorized transaction was authorized.[41]

---

[38] Section 48(1).

[39] Section 48(2).

[40] Section 5(2)(b) of the Consumer Protection Act 68 of 2008; Government Gazette 34181.

[41] FM Grugas "The Allocation of Risk in Electronic funds transfer Systems for Losses caused by Unauthorized Transactions" (1979) University of San Francisco Law Review 410; M Budnitz "The Impact of EFT upon Consumers: Practical Problems Faced by Consumers" (1979) University of San Francisco Law Review 368; S Mason (2014) *When Bank Systems Fail: Debit Cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* 40; VA Lawack-Davids & FE Marx "Consumer protection measures for erroneous or unauthorized internet payments: some lessons from the European Union?" (2010) Obiter 450 – 451.

1.3 Problem Statement

The risk allocation in online payment methods is presumably unfair, more so when considered in light of a bank's customer's position. Banks do not usually negotiate the terms and obligations of the bank-customer relationship and as such banks ensure that the risk associated online payments is to a large extent borne by its customers.[42] It is worth noting that a potential bank's customer does not have much have much of a choice when it comes contracting with their prospective banks. Banks usually offer identical services and as such a potential bank's customer's options are limited.[43]

Consumer law in general has been developed as a response to such business disclaimers which seek to evade accountability for the negative connotations which are present in their dealings with consumers.[44] To this end, consumer protection aims to achieve a more balanced allocation of business risk between consumers and corporate entities.[45]

The NCA partially deals with allocation of risk of unauthorized payments, however it is somewhat problematic owing to its naivety towards the nature of how online payment methods work.[46] Effecting payment through some of these methods does not require the presence of a bank card, all that is required is the information.[47] So a bank's customer may well be in the presence of their bank card, but completely unaware of the theft of his payment information. Burdening a bank's customer solely with liability of the use of his card until notification to the bank of its theft or misuse will presumably lead to inequitable results.[48]

Similarly, despite the ECTA providing liability for damages as a result of an unsecure payment system provided by the banks, it burdens the bank's customer with the

---

[42] *Ibid*.

[43] WG Schulze "E Money and Electronic transfers: A shortlist of some of the unresolved issues" (2004) SA MERC LJ 58.

[44] E Van Eeden (2013) *Consumer Protection Law in South Africa* 4.

[45] *Ibid*.

[46] S Mason (2014) *When Bank Systems Fail: Debit Cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* 6.

[47] *Ibid*.

[48] Article 74 *Directive 2015/2366/EU*; *Regulation 205.6 of the Electronic funds transfer Regulations (Regulation E) of 1996*.

burden of proof.[49] It is observed that banks as the providers of these systems have more access to evidence in relation to the subject and should perhaps bear the burden of proof or limit liability.[50] The ECTA also does not apply to juristic persons.[51]

The CPA which does, limits its application in that regard also. Its provisions do not apply to juristic persons with a turnover or asset value of over R2 000 000.00, banks on the other hand do not accept cheques over R50 000.00.[52] It would then be reasonable to infer that the culminating effect of this, is an existence of a large segment of consumers who are neither protected in terms of the CPA nor the ECTA which both contain consumer protection measures applicable to the research.

Nevertheless if a contractual term such as the one stated earlier is then found to be unfair in terms of the CPA, the CPA falls short in its failure to prescribe as to what the equitable position will be in those circumstances. Other jurisdictions such as United States of America and the European Union have provided certainty in this regard.[53]

In light of the above it then seems as though a bank's customer is left in a precarious situation due to the "fend for yourself" position that a bank's customer assumes. The research will then seek to address the issues as identified, by striving to achieve a more comprehensive consumer protection approach.

1.4 Research questions

i. Whether or not there is unfair allocation of risk in online payment methods between the banks and their customers?
ii. Whether or not there is adequate consumer protection afforded to consumers who make use of online payment methods?
iii. Whether or not there is unequal bargaining power between banks and their customers?

---

[49] CJ Nagel *Commercial Law* (2016) 487.

[50] FM Grugas "The Allocation of Risk in Electronic funds transfer Systems for Losses caused by Unauthorized Transactions" (1979) University of San Francisco Law Review 410.

[51] Section 1.

[52] Available at; http://www.pasa.org.za/home/2019/07/30/media-statement---reduction-in-maximum-cheque-value; Last accessed [08 February 2020]; WG Schulze "E Money and Electronic transfers: A shortlist of some of the unresolved issues" (2004) SA Merc LJ 54.

[53] See Chapter Four.

iv. Whether or not there is uniform practice with regards to online payment methods in the banking industry?

1.5 Methodology

The research will mostly make use of secondary sources such books, journal articles, and internet sources. Primary sources to be used will entail case law, legislation which will also include statutes of foreign jurisdictions in fostering comparative analysis.

1.6 Research outline

Chapter two will deal with the different types of online payment methods and the risks posed by such systems. Chapter three will focus on the legal issues posed by such systems, the laws applicable and import thereof. Chapter four will deal with a comparative analysis with jurisdictions identified earlier and finally recommendations and the conclusion will be provided in chapter five.

1.7 Conclusion

It is clear that the use of online payment systems is growing and that bank's customers are afforded little choice with regards to whether or not make use of online payments. Despite its perceived inherent risk, it seems like banks unfairly leave that risk to be borne by their customers even when they are the providers of such systems. The attainment of the objectives of the research will become clear as the research proceeds as set out in the research outline.

2. Chapter Two: Online payment methods

2.1 Introduction

In this chapter the study will focus on the nature and functionality of online payment methods which are premised on electronic funds transfer. There will be an in depth discussion of the different kinds of electronic funds transfer systems and the risks associated with such.

2.2 The Concept of Payment

Payment refers to the discharge of a debt owed under a monetary obligation by a person regarded as competent to discharge it, to person deemed competent to accept it. In essence it involves the fulfilment of the obligation as well as any ancillaries.[54] It is thus a bilateral juristic act that encompasses an agreement between both parties, the one effecting payment and the one receiving payment.[55]

Payment is regarded to having taken place when the debtor in tendering payment, grants the creditor an unfettered right to immediate use of the funds.[56] Payment is not recognized in the case of an electronic funds transfer, unless the funds are immediately and unconditionally available to the creditor, that is until the funds reflect in the account of the creditor.[57] The transfer of funds thus has to be free of any encumbrances relating to its use. The place of payment in electronic funds transfer of is where the funds are received by the creditor and not where the debtor gives the instructions for the transfer of funds.[58]

According to *Standard Bank of South Africa Ltd v Oneanate Investments (Pty) Ltd (in Liquidation)*[59] it has been held that when a bank account has been credited with a payment amount, that in itself constitutes *prima facie* evidence of the completed

[54] R Sharrock "Payment systems" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 194 – 195.

[55] Sharrock (2016) 195.

[56] Sharrock (2016) 196.

[57] *Ibid*.

[58] Sharrock (2016) 208.

[59] 1998 (1) SA 811 (SCA).

transaction.[60] However this does not prevent one from looking behind such entries to discover the true state of affairs.[61]

In *Nissan South Africa (Pty) Ltd v Marnitz NO and Others*[62] the court held that, the fact that a bank has unconditionally credited a customer's account with an amount received does not require a bank to pay the amount to the customer on demand, regardless of whether or not such a customer received the funds as a result of fraud.[63] It was further held that:

> "*If stolen money is paid into a bank account to the credit of the thief the thief has as little entitlement to the credit representing the money so paid into the bank account as he would have had in respect of the actual notes and coins paid into the bank account*."[64]

Thus a credit transfer reversal is possible where the beneficiary consents and also without the beneficiary's consent where the beneficiary is not entitled to the money transferred.[65]

2.3 Electronic Funds Transfer

Electronic funds transfer (EFT) refers to "*a funds transfer in which one or more of the steps in the payment process that were previously done by paper-based techniques are now done by electronic techniques*."[66] Central to its nature is the fact that there is no physical movement of money but rather the adjusting of bank account balances of the payer and payee.[67]

---

[60] 1998 (1) SA 811 (SCA) at paragraph 18.

[61] CJ Nagel *Commercial Law* (2016) 473.

[62] 2005 (1) SA 441 (SCA)

[63] 2005 (1) SA 441 (SCA) at paragraph 23.

[64] *Ibid*.

[65] C Van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 381; *Nissan South Africa (Pty) Ltd v Marnitz NO and Others* 2005 (1) SA 441 (SCA) at paragraph 23.

[66] M Roestoff "Payment systems" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 273.

[67] *Ibid*.

The transfer of funds is initiated with an accepted access device through an electronic terminal, telephone, computer, magnetic tape or other similar electronic device, for the purposes of ordering, instructing or authorising a bank to debit or credit an account.[68]

When payment is effected through EFT, there are two elements which are usually present:[69]

i. The payment instruction is given by the person who wishes to effect or accept payment to the bank holding funds.
ii. The bank transfers the funds to the account of the beneficiary.

An access device would typically be a card, code or other means of access to an account or any combination thereof that may be used to initiate the EFT. An access device becomes an accepted access device when the consumer requests and receives, signs it, uses the access device to initiate a transfer.[70]

The term EFT is an umbrella term that encompasses various transactions and services, such as:[71]

(a) transfers effected through an automated teller machine (ATM);
(b) EFT at point-of-sale(EFTPOS);
(c) transfers effected by telephone, by mobile cellular phone, or by way of a personal computer of consumer who is registered as user of internet-banking services or through magnetic material such as magnetic tapes.

2.4 Bank Cards

2.4.1 The components of a bank card

Cards issued by banks usually comprise of three components, namely; the plastic card, the chip which is an embedded microprocessor and the magnetic strip. The card

[68] CJ Nagel *Commercial Law* (2016) 473.

[69] D Swart 2000 "Online banking law and payment systems". In R Buys (ed) *Cyber law @ SA The law of the Internet in South Africa* (2000) 285.

[70] CJ Nagel *Commercial Law* (2016) 473.

[71] M Roestoff "Payment systems" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 273.

has the following information embedded in it: (a) the principal account number (PAN), (b) the start and (c) expiry date of the card which signifies its validity.[72]

The PAN is usually a 16 digit number serving as a unique identifier for each customer. This is contained in the chip together with the customer's PIN. The sole purpose of the chip is to interact with terminals to enable cash withdrawals at ATMs and to enable payments and transactions on the account.[73]

A card verification value (CVV) which comprises of three or four digits in some instances, is also present on the backside of the card. This is utilised for transactions where the card is not present such as over the internet or telephone.[74]

2.4.2 Debit Cards

Transactions effected with a debit card basically entail the cardholder granting authorisation to the bank to debit the cardholder's account with the amount of the transaction. They do not involve the extension of credit to the cardholder as is the case with credit cards.[75]

An account associated with a debit card must have funds available to effect payment, as the account is immediately debited when a withdrawal or payment is made. Most debit cards are used to make withdrawals at ATM's or electronic transfer funds at point of sale terminals.[76]

2.4.3 Credit Cards

Credit card payments entail an extension of credit to the cardholder by the issuer.[77] The card issuer in this instance can either be a bank as is often the case or a supplier.

---

[72] S Mason (2014) *When Bank Systems Fail: Debit Cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* 6.

[73] *Ibid*.

[74] *Ibid.*

[75] S Miller "Payment in an On-Line World" In L Edwards & C Waelde *Law & the Internet : a framework for electronic commerce* (2000) 62.

[76] PM Weaver *Banking and Lending Practice* (2016) 139.

[77] Weaver (2016) 137.

Since the card issuer extends credit to the cardholder, the transactions are subject to the NCA's regulation.[78]

It follows that there's a minimum of three parties involved when a bank is the issuer of the card namely, the cardholder, the bank and the supplier. The crux in this instance is that, the bank undertakes to pay the supplier for the cardholder's purchases and the cardholder repays the bank these amounts either in instalments or in full at a later date.[79]

If the cardholder has a credit balance on his account by virtue of the credit extended, the issuer will debit the amount as evidenced by the transaction slips against it.[80] In the event where the cardholder does not have a credit balance, the issuer will debit the cardholder's account and the cardholder will have to repay the issuer as per their agreement.[81] The credit extended by the issuer is not infinite, the parties agree on a pre-determined credit limit for payments or withdrawals of cash at the bank or ATMs.[82]

The cardholder's liability to the issuer is thus two-fold as it is based on both mandate and credit.[83] The issuer agrees to carry out orders of payment by the cardholder in the form of electronic-fund-transfers-at-point-of-sale terminals from suppliers where purchases were made.[84]

On the other hand, the credit card can be used to purchase goods or services via the internet, telephone or fax. When used in this manner, the card is not physically presented to the supplier but the transaction is facilitated through a variety of electronic inputs such as card numbers, security codes and PINs.[85] The card number in this

[78] CJ Nagel *Commercial Law* (2016) 477; Section of 4 of National Credit Act 34 of 2005.

[79] CJ Nagel *Commercial Law* (2016) 477.

[80] *Ibid.*

[81] Nagel (2016) 478.

[82] Nagel (2016) 477.

[83] Nagel (2016) 478.

[84] *Ibid*.

[85] *Ibid*.

instance is usually the card verification number[86] which is virtual accessible to anyone who has sight of the relevant card.

These inputs are submitted electronically to the issuer which will either accept or reject the transaction. Once a decision is reached it will electronically communicate such a decision to the supplier within a few minutes.[87]

2.5 Electronic Funds Transfer at the Point of Sale (EFTPOS)

The EFTPOS payment system is technology that allows suppliers of goods and services to accept cards as access devices to make payments. Funds are directly debited from the customer's account and credited to the beneficiary's account.[88]

This system does not make use of cash, suppliers get credit immediately thus vitiating the need for cash handling or cheque clearance.[89] Banks benefit from access fees charged to access the system by suppliers.[90]

An EFTPOS transaction is initiated when:

(i) The supplier swipes or waves the card at a point of sale terminal, where after the cardholder chooses the account from which payment is to be made from.[91]

(ii) The customer then enters their personal identification number (PIN), which together with the use of the card constitutes the electronic signature needed to verify the transaction.[92]

(iii) The EFTPOS terminal encrypts the PIN for security and allocates a transaction number. This information including the merchant number and

[86] S Mason (2014) *When Bank Systems Fail: Debit Cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* 6.

[87] S Mason (2014) *When Bank Systems Fail: Debit Cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* 6.

[88] CJ Nagel *Commercial Law* (2016) 474.

[89] PM Weaver *Banking and Lending Practice* (2016) 135.

[90] Weaver (2016) 135.

[91] Nagel (2016) 474.

[92] Weaver (2016) 135.

terminal number, is then forwarded electronically to the appropriate bank for verification by the terminal.[93]

(iv) The bank then either accepts or declines the transaction depending on earlier set conditions such as the availability of sufficient funds, entering of the correct PIN, *et cetera*, and in turn communicates this information back to the EFTPOS terminal.[94]

(v) The corresponding amount is then debited from the cardholder's account and simultaneously credited to the account of the supplier. Confirmation of the transaction is evidenced by a receipt, as well as documentation on the cardholder's bank statement.[95]

The EFTPOS network holds all the funds that a supplier collects in a day and deposits them to the supplier's account in a lump sum when the terminal is settled usually the next business day.[96]

The transactions as envisaged above may either be effected with a credit or debit card. Credit card transactions provides the cardholder with an option to pay the outstanding balance on the card in full or in instalments to the bank as its the bank that extends the credit to the cardholder who in turns utilises it with the supplier.[97] This is not without risk as a contactless card that is stolen would not require an input of a PIN, waving the card is sufficient to effect payment.[98]

Debit card transactions grant full and immediate payment to the supplier.[99] However, that is dependent on whether the system is on-line or off-line. In the former, the funds are electronically transfer directly from the cardholder's account to the supplier's.[100]

---

[93] Nagel (2016) 474.

[94] CJ Nagel *Commercial Law* (2016) 474.

[95] *Ibid*; Weaver (2016) 135.

[96] Nagel (2016) 475.

[97] Nagel (2016) 475.

[98] S Mason (2014) *When Bank Systems Fail: Debit Cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* 8.

[99] *Ibid*.

[100] M Roestoff "Payment systems" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 277.

Whereas in the latter, the payment instructions are kept on a magnetic tape or disk for processing at a later stage.[101]

Since the supplier is not able to determine whether or not the cardholder has sufficient funds, which is confirmed when the EFTPOS terminal connects to the network and sends the transactions to the bank, which then accepts the transaction.[102] The franchise agreement will usually only authorise the supplier to accept payments up to a certain limit, which in this sense would confirm sufficiency of funds.[103]

Whether an off-line transaction constitutes a cash sale or credit will be determined by the intention of parties. However it has been correctly stated that, as a general rule "…*the parties, intention will be to conclude a cash sale thus that delivery and payment of the purchase price should be effected at the same timer or as soon as possible*."[104]

2.6 Automatic Teller Machines transactions (ATM)

Automatic teller machines or ATMs refers to bank vaults which allot money and are electronically connected to a bank's computer system.[105] They have been established to enable a wide variety of other banking functions or transactions encompassing cash withdrawals, account payments, inter-account transfers, account deposits, purchases of airtime to access mobile cellular phone or data services, and the viewing of account statements.[106]

These transactions are initiated with a bank card and are essentially authorised with an input of a PIN.[107] What follows is a series of prompts and inputs from the cardholder, where after a receipt of the transaction is produced and the card returned upon completion of the transaction.[108]

---

[101] *Ibid*.

[102] M Roestoff "Payment systems" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 277.

[103] *Ibid*.

[104] Roestoff (2016) 278.

[105] CJ Nagel *Commercial Law* (2016) 479.

[106] *Ibid*.

[107] *Ibid.*

[108] *Ibid*.

The information in the magnetic stripe is used to identify the cardholder via the PIN. The PIN and the usage of the card constitutes the cardholder's electronic signature that authenticates the transaction.[109] A credit or debit entry is then entered on the relevant account depending on whether cash was deposited or withdrawn or funds were transferred.[110]

The standard terms of use normally stipulate that when the correct PIN is entered it is considered to be the customer's mandate and effect will be given to that the instruction.[111]

ATM transactions seem to be the safest way of effecting payment due to the physical requirement of an access device. However the safety of ATM transactions should not be looked at in isolation by only focusing on their access thereof, the inquiry should involve a holistic approach focusing on the net impact of ATM transactions.

In the foregoing, ATM transactions dispense cash which makes bank's customers easy targets for thieves, thus rendering this method of payment risky. In addition to that, ATM transactions are highly inconvenient as they can only be effected by physically accessing an ATM.

2.7 Internet, mobile cellular phone and telephone banking (Electronic Banking)

This form of banking services provide access to banking facilities from virtually anywhere around the world. The customer can access statements, check balances, transfer funds between accounts, pay accounts, trade in shares, obtain information or additional services and correspond with the bank at any time.[112]

Access to these services is coupled with the issuing of a set of access codes, security procedures and data. It would typically involve electronic inputs of an account number or user number, a password and/or a customer selected PIN (CSP) to identify the user.[113]

---

[109] PM Weaver *Banking and Lending Practice* (2016) 134.

[110] *Ibid*.

[111] CJ Nagel *Commercial Law* (2016) 480.

[112] Nagel (2016) 280.

[113] Nagel (2016) 480.

Thereafter the bank has a system of email or SMS notifications with one-time passwords for customers, to inform them that the account has been accessed, that transactions have been processed through their accounts or to authorise a transaction to be processed through the account.[114] An additional security code is also required when customer wants to add new payment recipients to his or her account.[115]

The customer as is the case with other EFT systems is required look after all access codes, keep them secret and inform the bank immediately when they have been compromised.[116] The customer is further required to maintain an updated security software on their personal computers and not to make use of public computers.[117]

2.8 The Risk of Fraud

It is observed that the lack of consumer confidence in online-shopping may be attributed to the fear that someone might make use of the consumer's payment information to make purchases which the consumer will be held liable for.[118]

Encryption may be the catalyst to inspire confidence in this regard. To this end, MasterCard and Visa have developed the Secure Electronic Transaction (SET) protocol which is the technical standard for safeguarding payment card details conveyed over the Internet.[119] They make use of digital certificates and strong encryption which in essence reduces the risks of card information being abused.[120]

The identities of cardholders and retailers are verified by way of digital certificates, issued by the relevant card organisation. The effect of a transaction concluded through

[114] Nagel (2016) 480.

[115] S Eiselen "E-commerce" In D Van der Merwe (ed) *Information and Communication Technology Law* (2008) 193.

[116] S Eiselen "E-commerce" In D Van der Merwe (ed) *Information and Communication Technology Law* (2008) 193.

[117] *Ibid.*

[118] *Fourie v Van der Spuy and De Jongh Inc* 2020 (1) SA 560 (GP) cybercrime makes the internet unsafe. At paragraph 25; S Miller "Payment in an On-Line World" In L Edwards & C Waelde *Law & the Internet: a framework for electronic commerce* (2000) 56.

[119] Miller (2000) 57.

[120] *Ibid*.

SET is that the cardholder deals with the merchant that is SET-registered and the merchant knows that it is dealing with a valid cardholder.[121]

However these security mechanisms do not holistically address the risks associated with effecting online payments by way of a card, particularly the possible fraudulent use of card information by a merchant or its employees.[122] Thus where payment is effected through a payment instruction, the risk remains that the message could have been sent fraudulently or amended to replace the intended beneficiary with someone else.[123] Contactless cards do not require the input of a PIN, thus payment can easily be effected with just a bank card for an EFTPOS transaction.

Payment instructions may also be given in different forms. The instruction may be given at an ATM or EFTPOs by using a bank card or other electronic devices, alternatively, it also possible for it to be given orally or by written instructions.[124]

This danger was clearly demonstrated in *Absa Bank Ltd v Hanley*[125]. This was an appeal case concerning a fraudulent transaction initiated on the respondent's account held with the appellant.[126] An amount of USD 1.6 million was transferred from the respondent's account which he had not authorised, the court found that the respondent was to a certain extent negligent however, his negligence was not the proximate cause of the loss suffered.[127]

The transfer was occasioned by a broker (La Cote) who offered to finance the purchase of an aircraft for the respondent's brother's company Euroceltic. The terms

[121] *Ibid*.

[122] D Swart 2000 "Online banking law and payment systems". In R Buys (ed) *Cyber law @ SA The law of the Internet in South Africa* (2000) 288 – 289.

[123] D Swart 2000 "Online banking law and payment systems". In R Buys (ed) *Cyber law @ SA The law of the Internet in South Africa* (2000) 288 – 289.

[124] C Van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 371.

[125] 2014(2)SA 448 (SCA).

[126] 2014(2)SA 448 (SCA). At paragraphs 1 - 3.

[127] *Ibid.*

of the agreement were that the broker would avail USD 3.5 million to the borrower for a deposit of USD 1.75.[128]

La Cote had from the early stages insisted that the money be deposited into its account, and had on two occasions sent letters purporting to have been signed by the respondent to the appellant for the transfer of USD 1.75 million.[129] These requests were not however effected as the first was sent by facsimile, and the second's signature could not be verified.[130]

The appellant's employees then took it upon themselves and sent "two page transfer forms" to La Cote who at all materials had purported to be the respondent. More so, when the appellant's employees called him with regards to the two transfers.[131] La Cote then contacted the respondent to sign the forms under the pretext that they were required by the Reserve bank for approval of the transfer of the purchase price and payment of penalty as the sale was delayed.[132]

La Cote sent his associates with the forms to the respondent. The respondent was required to sign the second page only, authorising the transfer of USD100 000 with reference to the first page that was supposed to be left blank.[133] The reasons provided where that if the respondent indicated the beneficiary on the first page, the transfer would be delayed as the reserve bank would apparently require a contract between the two.[134]

The respondent eventually signed the two page form authorising a transfer of USD100 000. The details of the beneficiary were left blank on the first page whilst his signature and the USD100 000 amount appeared on the second page only.[135] This amount was altered to USD1.6 million by adding a one and changing the one into a

[128] 2014(2)SA 448 (SCA). At paragraphs 4 – 8.

[129] 2014(2)SA 448 (SCA). At paragraphs 10 – 11.

[130] *Ibid*.

[131] 2014(2)SA 448 (SCA) at paragraph 12.

[132] 2014(2)SA 448 (SCA) at paragraphs 13 – 14.

[133] 2014(2)SA 448 (SCA) at paragraphs 14 - 16.

[134] *Ibid*.

[135] 2014(2)SA 448 (SCA) at paragraph 20.

six, the respondent then noticed this transfer when the bank issued his monthly statement.[136]

The court then had to determine negligence on either the part of the respondent when it gave its payment instructions or the appellant's in executing its mandate. The court found that the respondent's conduct was not the proximate cause of the misappropriation of the funds. The respondent did not facilitate the alteration of the amount of the second page, as he had written the figures and words with care.[137]

The appellant was found to be negligent as its employees had not initially called the respondent at the numbers he provided when he opened his account, as La Cote purported to be the respondent. The appeal was accordingly dismissed.[138]

In light of the above a payment instruction can thus easily be changed, deleted or transmitted to another medium unbeknown to the medium in the absence of sufficient security measures.[139]

Unauthorized transactions in card not present transactions is virtually easy as well. Because authentication is observed through details printed on the card (CCV *etc.*) and email or SMS notifications with one-time passwords to authorise transaction.[140]

The case of *Nashua Mobile (Pty) Ltd v GC pale cc t/a invasive plant Solutions*[141] demonstrated how authentication mechanisms can be bypassed. The action instituted related to losses suffered when unauthorized money transfers were effected out of the plaintiff's internet bank account by a person (unknown to the plaintiff and unauthorized by it to do so) who managed to obtain from the defendant a SIM card containing the cell-phone number of an employee of the plaintiff.[142]

It is common cause that a reference number, sent by the bank by SMS exclusively to the registered cell-phone number of the accountholder is required in order to complete

[136] 2014(2)SA 448 (SCA) at paragraphs 20 - 21.

[137] 2014(2)SA 448 (SCA) at paragraphs 37.

[138] 2014(2)SA 448 (SCA) at paragraph 32.

[139] *Ibid.*

[140] CJ Nagel *Commercial Law* (2016) 480.

[141] A3044/2010.

[142] A3044/2010 at paragraph 3.

an internet banking transaction.[143] A "hypothetical fraudster" would require the accountholder's profile number, PIN and password and not just a SIM card to access the system.[144]

This information can however be obtained through a process of phishing. Fraudsters would typically send out an e-mail to a base of clients pretending to be the bank. It will for instance suggest that the client updates its "outdate information" by clicking a link. This link will then direct the client to the fraudsters website which would look like that of the bank. The client will then enter personal information that the fraudster will use.[145] Clearly, as exposited by this case that is required is personal information of the payer to effect payment.

2.9 Conclusion

The common denominator in online payment methods is the fact that they are all based on mandate. Resultantly, a bank will process an EFT on the basis of a payment instruction that appears to be from its relevant customer. Some of these methods of payment have safety aspects which are not attributable to other methods. However, the ease with which unauthorized transfers can be effected is rather alarming and thus safety concerns as a collective remains.

[143] A3044/2010 at paragraph 10.

[144] A3044/2010 at paragraph 18.

[145] A3044/2010. At paragraph 20.

3. Chapter Three: The legal position of a bank's customer in online payment methods

3.1 Introduction

This chapter will focus on the current legal position of a bank's customer in light of the prevailing legal framework. This will be done by assessing the culmination and effect of this legal position. An overarching outlook will then be provided with regards to the adequacy of the existing legal framework, to regulate the said legal position.

3.2 Liability for Transactions

Mandate which constitutes the basis of EFTs denotes that a bank as mandatory has to effect a customer's order timeously once the instruction is given in accordance with the terms agreed between the parties. Where an EFTPOS or an ATM transaction is initiated using the issuer's card and the correct pin entered, it would constitute an electronic signature signifying a payment order.[146]

It is common cause that, the bank as a mandatory has a duty to exercise reasonable skill and care when effecting its mandate. The customer in turn has to effect the payment order with reasonable care so as to limit the chances of fraud and deception.[147]

So when a bank transfers funds from the customer's accounts which the customer did not authorise, the bank breaches its duty.[148] Thus the bank will not be able to debit a customer's account if it pays out in consequence of a forged or unauthorized electronic funds transfer instruction.[149]

However, in light of the absence of governing legislation, the bank-customer contracts will continue to govern the issue of liability for unauthorized electronic payments.[150] It

---

[146] PM Weaver *Banking and Lending Practice* (2016) 134.

[147] C Van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 368. FR Malan *et al Malan on Bills of Exchange, Cheques and Promissory Notes* (2009) 280.

[148] Van Heerden (2016) 369; *Volkskas Bpk v Johnson* 1979 (4) SA 775 (C) at 777H-778A.

[149] Van Heerden (2016) 373.

[150] Van Heerden (2016) 373.

will further be a point of reference in the determination of whether or not it indemnifies the bank regarding such payments or otherwise allocates risk of loss to the customer.[151]

This is clearly evident from the *Absa v Hanley* case in which the customer was initially held liable for an EFT despite not having authorised the transaction. His innocence was only proved after the lengthy and costly process of litigation.[152] This will remain the position for South African bank's customers who are faced with similar issues for as long as liability it is governed privately between the banks and their customers.

Fourie v Van der Spuy & De Jongh Inc and Others[153] dealt with issue of cybercrime. The applicant entered into a contract of mandate with the second respondent of the first respondent law firm and as usual money was held in trust for applicant until further instructions. The second respondent later received payment instructions via email purportedly from the applicant to effect payment into identified bank accounts. It was later discovered that the payment instructions where not sent by the applicant, rather by criminals who had hacked the applicant's email.[154]

The applicant then sued the respondents for the payment of the said amounts with issue for determination being who had to incur liability for the loss suffered.[155]

The court found that an attorney has a duty to account to his or her client for the funds held in the trust account.[156] Resultantly, the second respondent failed to discharge its duty to pay the applicant when it effected payment erroneously and the occurrence of the fraud did not absolve it from such duty.[157] On that basis the respondents were jointly and severally liable, the one paying the other to be absolved.

---

[151] C Van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 369.

[152] T Naude "The use of black and grey lists in unfair contract terms legislation in comparative perspective" (2007) SALJ 132.

[153] 2020 (1) SA 560 (GP).

[154] 2020 (1) SA 560 (GP) at 560.

[155] 2020 (1) SA 560 (GP) at paragraph 12.

[156] 2020 (1) SA 560 (GP) at paragraph 15.

[157] 2020 (1) SA 560 (GP) at paragraph 31.

This case clearly indicates that liability in this instance was established on the basis of a legal duty of care and to account to a client by an attorney was not discharged. The second respondent was found to be negligent for not imploring measures to prevent fraud which was prevalent in the profession.[158] The court however pointed out that the determination of negligence is a question of fact which requires the consideration of all relevant circumstances.[159]

Ultimately, thus where mandate is established on the part of the bank, it would at face value entail that a purported transaction was duly authorised. The customer's account will then be debited with corresponding amount of the transaction. The onus will then be upon the bank's customer to prove that a purported transaction was indeed not authorised.

This is the position despite absence of sufficient security measures which entails that a payment instruction can thus easily be altered or directed to an unknown medium[160] and that it could have been sent fraudulently.[161]

However it is common cause that where a bank's customer initiates a payment instruction in a manner that makes it prone to fraud and resultantly the manner in which it was utilised is the causal link to the loss suffered by the customer, common law and the bank-customer contract dictates that the customer will be liable for those transactions.[162]

In addition, where the customer's bank card is lost or stolen and the customer fails to report such loss or theft before any unauthorized transfers or withdrawals, the customer will *ipso facto* be liable for any consequential losses. This is also the case where the bank's customer fails to safeguard his PIN or was aware forgery and results in consequential losses.[163]

---

[158] 2020 (1) SA 560 (GP) at paragraph 30.

[159] 2020 (1) SA 560 (GP) at paragraph 19.

[160] 2014(2)SA 448 (SCA) at paragraph 32.

[161] D Swart 2000 "Online banking law and payment systems". In R Buys (ed) *Cyber law @ SA The law of the Internet in South Africa* (2000) 288 – 289.

[162] Van Heerden (2016) 373.

[163] C Van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 373.

At first glance this may seem plausible, however this imposition of liability to great extent on a bank's customer is presumably unfair on consideration of other factors.[164]

3.3 Unfairness of banks' exclusion of liability for unauthorized electronic funds transfer clauses

The case of *Sasfin v Beukes*[165] which preceded the Consumer Protection Act dealt with unfair contracts on the grounds of public policy. It set out the principle as follows:[166]

(i) Public policy in essence refers to the interests of the community, thus such interests predicate the establishment of public policy.

(ii) Agreements which are patently against the interest of society be it on the grounds of law, morality or social or economic expedience are contrary to public policy.

(iii) Public policy is not however established when one's individual sense of property and fairness is merely offended as it fully acknowledges freedom of contract.

(iv) Freedom of contract in this sense dictates that commercial transactions should not unduly be trammelled and that simple justice between man and man should be upheld.

The legal issue in this case was the validity of a deed of cession which contained clauses which effectively sought to maximise protection for Sasfin's rights, while effectively subjecting Beukes to onerous burdens and restrictions.[167] Resultantly, it was found to be invalid for those reasons.

In a more recent case of *AB and Another v Pridwin Preparatory School and Others*[168] the Supreme Court of Appeal confirmed the elements of the principle of public policy as initially exposited by the *Sasfin* case. It held that a court will not unreservedly

---

[164] H Schulze "Unauthorized cash withdrawals with a credit card and unfair contract terms" (2004) Juta Business Law 145 – 146.

[165] 1989 (1) SA 1 (1).

[166] 1989 (1) SA 1 (1) at 7 – 10.

[167] 1989 (1) SA 1 (1) at 10 paragraphs A - D.

[168] 2019 (1) SA 327 (SCA).

invalidate a contract, it will only do so in the clearest of cases where harm to the public is to great extent undisputable and it not merely idealistic.[169]

The case of *Diners Club SA (Pty) Ltd v Singh and Another*[170] (*Diners* case) specifically dealt with the issue of unfairness of a contractual term relating to the use of a credit card. The plaintiff a credit card business had issued diners credit cards to the first defendant and his wife, the second defendant.[171] The plaintiff was suing the defendants for 190 successful ATM cash withdrawals in the amount 54000 pounds (approximately R500 000 at the time) performed in London on the first defendant's account.[172]

In terms of the contractual agreement governing the use of the said credit cards, the cardholder was liable for charges incurred on the cards.[173] The defendants' defence was twofold, firstly, the first defendant was adamant that he was not in London when the said transactions occurred and that the card and PIN were in his passion and had not been given to anyone else.[174] Secondly that clause 7.3 of the contract between the plaintiff and the first respondent was *contra bonos mores*.[175]

The defendant's plainly implied that some unknown person was guilty of effecting these transactions unlawfully.[176] Clause 7.3 provided that "…*use of a PIN by any person whatsoever, the cardholder is deemed to accept liability for all and any transaction incurred*".[177]

The contention was that the imposition of liability to a cardholder regardless of someone else using his card and PIN was inequitable, unjust and unconscionable. However the court held that, in as much this provision is one-sided in favour of the

[169] 2019 (1) SA 327 (SCA) at paragraph 27.

[170] 2004 (3) SA 630 (D).

[171] 2004 (3) SA 630 (D) at 632 paragraphs G - J.

[172] 2004 (3) SA 630 (D) at 634 paragraphs F - G.

[173] 2004 (3) SA 630 (D) at 633 paragraphs A - C.

[174] 2004 (3) SA 630 (D) at 634 paragraphs G - I.

[175] 2004 (3) SA 630 (D) at 645 paragraphs E – G.

[176] 2004 (3) SA 630 (D) at 633 paragraphs H – I.

[177] 2004 (3) SA 630 (D) at 655 paragraphs D – E.

plaintiff, it was entitled to protect itself as the card could be used throughout the world.[178]

The court also upheld the notion of freedom of contract by plainly stating that "…*the defendants accepted their cards knowing that they would be bound by contractual terms and conditions. They were not under any compulsion to do so*."[179] The second defence was on this basis dismissed and the aspect of good faith was not considered.

Regarding the first defence, it was established that the first defendant had in fact conspired with people who had effected the withdrawals in London by providing them with his card.[180] The plaintiff's claim was accordingly upheld.

It is an established principle in the South African law of contract that seriously concluded contracts should be enforced, however this should not be done without exception.[181] Contracts could be declared invalid if their found to be contrary to public policy, the interests of the parties and society at large are key factors of consideration in such determination.[182] Unfairness could exist where an economically superior party (e.g. bank) abuses its position when negotiating with an economically inferior party (e.g. customer.).[183]

Schulze contents that the case could have been decided differently with regards to the first defendant's second defence. However because of the evidence before court and the first defendant's fraudulent conduct, the judgment was as it was.[184]

---

[178] 2004 (3) SA 630 (D) at 658 – 659.

[179] 2004 (3) SA 630 (D) at 659 paragraphs D - E.

[180] 2004 (3) SA 630 (D) at 668 paragraphs G – I.

[181] *Afrox Healthcare Ltd v Strydom* 2002 (6) SA 21 (SCA) it was confirmed that freedom of contract is principle of the South African law of contract. This formed the sole basis upon which the validity challenge of a contractual clause based on public interest which insulated a hospital against the negligence of its staff was dismissed by court. At paragraphs 22 - 24; H Schulze "Unauthorized cash withdrawals with a credit card and unfair contract terms" (2004) Juta Business Law 144.

[182] H Schulze "Unauthorized cash withdrawals with a credit card and unfair contract terms" (2004) Juta Business Law 144.

[183] *Ibid*.

[184] Schulze (2004) Juta Business Law 145 – 146.

It is also contended that the aspect of good faith should have been explored by the court in arriving at its judgment.[185] It involves *inter alia* a consideration of the advancement of ones interest at the expense of another which would in that instance vitiate public interest of enforcing a contract.[186]

These are all valid arguments, however the mere allegation of a difference in bargaining power cannot in itself warrant a finding that a contract conflicts with constitutional values, evidence showing inequality of bargaining power between parties must be availed before a finding to this effect can be made.[187]

In this regard, it is without a doubt that a difference of bargaining power between banks and their customers exists. This is owing to the fact that, the bank-customer contract is usually a standard form contract and the major banks in South Africa subscribe to the same Code of Banking Practice[188]. Its provisions on the liability for unauthorized transactions losses are imported in bank-customer contracts.

However, Kay and Sewell are of the opinion that in as much as neediness may grievously impair the bargaining power of a consumer, it does not matter much if undue influence on the part of supplier cannot not be established.[189]

Neediness denotes necessity in this sense and if Roger and Tim's contentions are to be followed, this would result in a strict appliance of the freedom of contract principle which is potentially flawed.[190]

This is due to the fact that this would effectively lead to upholding of the notion that, persons are free to negotiate the terms of their contracts without any legislative interference and should be given full effect, freedom of choice with whom to contract

[185] WG Schulze "Of credit cards, unauthorized withdrawals and fraudulent credit-card users" (2005) SA Merc LJ 209.

[186] Schulze (2005) SA Merc LJ 208 -209.

[187] E Van Eeden *Consumer Protection Law in South Africa* (2013) 86.

[188] 2012.

[189] R Kay & T Sewell *A practical approach to Contract and Consumer Law* (1984) 131.

[190] P Aronstam *Consumer Protection, Freedom of contract and the Law* (1979) 14.

with or not to enter contracts at all.[191] This was evident in the *Diners* case specifically in the dismissal of the second defence.[192]

This state of affairs wrongly fails to take into account the personal circumstances of the parties to a contract,[193] which in my view forms central in the enquiry of consumer protection measures. This contention is affirmed by the principles established the *Barkhuizen v Napier*[194] case which dealt with the determination of the constitutionality of a time limitation clause of an insurance policy.

The essence of it was that it precluded the insured from instituting a claim if it was not lodged within the specified time period.[195] It was the applicant's contention that the said clause was contrary to public policy as reflected by section 34 of Constitution which guarantees the right seek redress from court.[196]

Public policy was found to encompass notions of fairness, justice and reasonableness. It thus impedes the enforcement of a contractual term if such would be unjust or unfair.[197]

The determination of fairness required the weighing of two considerations. The right to seek judicial redress on the one hand, and public policy on the other hand which requires compliance with contractual obligations that have been freely and voluntarily agreed to.[198] This upholds the *pacta sunt servanda* principle which enunciates freedom to regulate one's own affairs even to one's own detriment.[199] However this principle is not an end in itself, as the extent to which a contract was freely and voluntarily concluded is a vital consideration in the affirmation of this principle.[200]

---

[191] Aronstam (1979) 13 -14.

[192] 2004 (3) SA 630 (D) at 659 paragraphs D - E.

[193] Aronstam (1979) 14.

[194] CCT 72/05.

[195] CCT 72/05 at paragraph 1.

[196] CCT 72/05 at paragraph 19.

[197] CCT 72/05 at paragraph 73.

[198] CCT 72/05 at paragraph 57.

[199] *Ibid*.

[200] *Ibid*.

Unequal bargaining power is a factor of consideration for public policy owing to the potential injustice that may manifest. Although there was no evidence of an inequality of bargaining power "*this does this does not detract from the principle enunciated in that case, namely, that the relative situation of the contracting parties is a relevant consideration in determining whether a contractual term is contrary to public policy*".[201]

Therefore the relevance of power imbalances between contracting parties is an importunate aspect in pursuit of such determination.[202]

It is rightly so observed that consumers and suppliers are not on an equal footing and consumers can thus not be expected to protect their rights on their own. Legislation is better served in this regard.[203] Naude affirms the above contention by similarly opining that freedom of contract cannot be guaranteed where its being claimed by one party only, statutory intervention is thus necessary.[204] These principles have resultantly found expression in the Consumer Protection Act[205] which deals with unfair contractual terms specifically.

3.3.1 The right to fair, reasonable and just contractual terms

A consumer in this regard falls within the category of a person who has entered into a transaction with a supplier in the ordinary course of the supplier's business. Person includes a juristic person, however a juristic person does not encompass one that has an annual turnover of more than two million.[206] A supplier on the other hand entails a person who markets any goods or services, which services is established to encompass banking services.[207]

Section 48(1) specifically confers the right to fair, reasonable and just contractual terms to consumers who are in agreement with a supplier for any goods or services.

---

[201] CCT 72/05 at paragraph 59.

[202] CCT 72/05 at paragraph 87..

[203] T Woker "Consumers and contracts of purchase and sale" In D McQuoid-Mason (ed.) *Consumer law in South Africa* (1997) 25.

[204] T Naude "Unfair contract terms legislation the implications of why we need it for its formulation and application" (2006) StellLR 336.

[205] 68 of 2008.

[206] Section 1.

[207] Section 1.

More so, section 48(2) states that a contractual term is unfair, unreasonable or unjust if :

> "…(a) *it is excessively one-sided in favour of any person other than the consumer or other person to whom goods or services are supplied*"
>
> "…(b) *the terms of the transaction or agreement are so adverse to the consumer as to be inequitable.*"

Sharrock contends that these provisions are relatively broad and imprecise to be of any virtual assistance. The inquiry more importantly requires the determination of excessively and adversity to the consumer as to be inequitable,[208] and in the author's view rightly so.

The case of *Four Wheel Drive Accessory Distribution CC v Rattan NO*[209] dealt with this section in an orbiter. The case related to claim by the plaintiff against the deceased's estate executer for cost of repairs of a vehicle that was leased to the deceased. The deceased never returned the vehicle as it was damaged when he was shot and killed in it, it was naturally recovered from the police.[210] The plaintiff asserted that the deceased was obligated to insure the vehicle for 72 hours or return it before that period expired despite the absence of such conditions in the lease agreement.[211]

Although the case was dismissed on the grounds of lack of *locus standi* the court out of its own accord raised questions on the application of the CPA. Relevant to the discourse at hand, the court found that claiming obligations on the part of the deceased for insurance when they were not included in the lease agreement and when the deceased can neither accept nor refute such a claim and enforcing it when the deceased is physically unable to, amounts to unfair, unreasonable and unjust in terms according to section 48 of the CPA.[212] This so because they are excessively one-side in favour of persons other than the deceased and they are also so adverse to the deceased as to be inequitable.

---

[208] RD Sharrock "Judicial Control of Unfair Contract Terms: The Implications of Consumer Protection Act" (2010) SA Merc LJ 308.

[209] 2018 (3) SA 204 (KZD).

[210] 2018 (3) SA 204 (KZD) at paragraphs 1- 5.

[211] 2018 (3) SA 204 (KZD) at paragraph 66.

[212] *Ibid.*

The case went on appeal and the Supreme Court found that the High Court erred by adjudicating on issues that were not canvassed by the parties as they had no influence on the decision. Surprisingly, despite having found that the approach by the High Court was unnecessary, the Supreme Court expressed that the CPA was not applicable to the said agreement as it did not satisfy the requirements of a transaction as contemplated by section 5(1)(a) of the CPA.[213] This case is mentioned as its one of the few cases to deal with section 48 of the CPA.

This case indicated how the CPA as an instrument for consumer protection can be utilised to challenge contractual terms on the basis of unfairness. Sadly it did not provide clarity regarding the determination of excessively one-sided and adversity to the consumer as to be inequitable.

However a holistic look at the CPA specifically section 2(2) provides that the court may be guided by any foreign and international law when interpreting the Act. In the foregoing, the *European Union's Unfair Terms in Consumer Contracts Directive*[214] under Article 3 defines an unfair contractual term as one which has not been negotiated individually and which, against the requirement of good faith, results in a significant imbalance in the parties' rights and obligations under the contract, to the detriment of the consumer. A term is considered not to be individually negotiated when it has been drafted pre-negotiation thus negating the influence of the consumer on the substance of the term according to Article 3(2).

Similarly, Regulation 5(1) of the *Unfair Terms in Consumer Contracts Regulations*[215] of the United Kingdom ascribes to the same definition of an unfair contractual term as the EU word for word.[216] In the case of *Director General of Fair Trading v First National Bank plc*[217] (*Director General of Fair Trading* case) it was held that, the requirement of significant imbalance is met when a term is weighted in favour of a supplier by effectively ensuring that the rights and obligations are in his favour. This may manifest

[213] *Four Wheel Drive Accessory Distribution Cc v Rattan NO* 2019 (3) SA 451 (SCA) at paragraphs 24 & 32.

[214] Directive 93/13 [1993].

[215] SI 1999 No 2083 (UK).

[216] E Van Eeden (2013) *Consumer Protection Law in South Africa* 272.

[217] [2001] UKHL 52.

where a consumer is disadvantageously imposed with risk.[218] Good faith basically requires a supplier to not take advantage of *inter alia* a consumer's necessity or weak bargaining position.[219]

Under German law good faith is also said denote consideration of the other party's interest as opposed to the furtherance of one's interests only in the context of standard terms.[220]

Thus where there is an alleged contravention of section 48 in any proceedings before court, section 52(1) mandates the court to consider the principles, purpose and provisions of the CPA. As set out earlier the CPA makes provision for foreign and international law, and the principles as encompassed by section 48 are afforded clarity when interpreted in light of international law.[221]

In *Barkhuizen v Napier*[222] the court in its determination of fairness also made reference to the EU's directive on Unfair Terms in Consumer Contracts. It held that fairness is not measured with reference the price paid for services rendered, the criterion encompasses the balancing of reciprocal ancillary obligations and adherence to reasonable expectations.[223] This firstly suggests that "*an advantage obtained in ancillary terms, such as an exclusion of liability or a fixed measure of damages for breach, should be matched by corresponding benefits to the other party*." Secondly "that the ancillary terms should not deviate from a reasonable package of terms for transactions of that type unless the parties have expressly negotiated the point."[224]

It is common cause that the exclusion of liability for unauthorized transactions by banks compounds significant imbalances in the rights and obligations between them and the consumer, and to the detriment of the consumer as well.

---

[218] [2001] UKHL 52. At paragraph 17.

[219] *Ibid*.

[220] T Naude & C Koep "Factors relevant to the assessment of the unfairness or unreasonableness of contract terms" (2015) StellLR 92.

[221] Section 52.

[222] CCT 72/05.

[223] CCT 72/05 at paragraph 165.

[224] *Ibid*.

This is so because these clauses are outright excessively one-sided in favour of banks and *ipso facto* ensure that the consumers bear the majority of the risk of unauthorized transactions[225] and burden consumers with various obligations with very little obligations on their part. There is also no corresponding benefit for bank's customer's in light thereof.

Secondly, the sole liability of a bank's customer for unauthorized transactions only ensues as a result of the bank-customer contract. As it was correctly put by Van Heerden a bank would normally not be able to debit a customer's account for a transaction initiated on the basis of an unauthorized electronic funds transfer instruction in different circumstances. However in view of the lack of governing legislation, the bank-customer contract enables banks to do so.[226]

Resultantly, banks unilaterally determine the rules and procedures relating to the initiation of EFT's.[227] This manifests in standard form contracts that bank's customers are subjected to which negates their ability to negotiate the terms and conditions which will govern such use. This then culminates in a "take it or leave it" scenario for the South African consumer.[228]

This affects bank's customer's negatively as there is alternative choice for online payment methods, as most bank's online payments system's operations are similar.[229] The number of operating banks is also limited, thus negating any would be competition.[230] As was correctly put by Worker, "*Freedom of choice extends only to the extent that a consumer may decide not to use those services at all*."[231] It is patently clear that bank's customers do not have freedom of choice in this regard.

---

[225] C Van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 370.

[226] Van Heerden (2016) 373.

[227] WG Schulze "E Money and Electronic transfers: A shortlist of some of the unresolved issues" (2004) SA Merc LJ 58.

[228] *Ibid*.

[229] *Ibid*.

[230] *Ibid*.

[231] T Woker "Consumers and contracts of purchase and sale" In D McQuoid-Mason (ed.) *Consumer law in South Africa* (1997) 25.

In addition, section 52(2)(e) and (b) of the CPA provides the following factors respectively that the court must consider in determining contravention of section 48:

> "*whether there was any negotiation between the supplier and the consumer, and if so, the extent of that negotiation*" and the bargaining position of the parties to the agreement.

The strength of the parties' bargaining power may be indicated by inquiring as to whether or not " *the complaining party was offered a choice over a particular term, that party had a realistic opportunity to enter into a similar contract with other persons, but without that term*."[232] This is clearly not afforded to a prospective bank's customer, as most banks contract out liability of unauthorized transactions.[233]

It is common cause that banks do not negotiate the terms of the bank-customer contract, equally important is the fact that consumers are inclined to make use of electronic funds transfer,[234] thus denoting necessity. Necessity as alluded to in the *Director General of Fair Trading* case should not be taken advantage of by the banks, which they do. The lack of alternatives for bank's customers, effectively weakens their bargaining power which banks take advantage of.

It is also a general discourse that computer software is inherently unreliable, thus bugs and errors are ever present. This is owing to the inefficiency of testing procedures and the ineffective error resolution and debugging measures.[235] If computer software is thus inherently unreliable and the use of online payments methods inherently risky, it should then necessitate a more plausible risk allocation for equitable results.

In light of the above it is then trite to hold that the clauses referred to under this heading will not survive the unfairness test as discussed above. In the circumstances, section 52(3) of the CPA empowers a court in this regard to make declaration to this effect or

---

[232] T Naude "Unfair contract terms legislation the implications of why we need it for its formulation and application" (2006) StellLR 373.

[233] Schulze (2004) SA Merc LJ 58.

[234] WG Schulze "E Money and Electronic transfers: A shortlist of some of the unresolved issues" (2004) SA Merc LJ 64.

[235] Erlank & Ramokanate "Allocating the risk in software failures in automated message systems (autonomous electronic agents)" (2016) SA Merc LJ 210 - 211.

any order that the court considers to be just and reasonable. The inquiry will then delve into the discussion of other protection measures and their implications thereof.

3.4 Other protective measures for bank's customers

As shown in the preceding chapter, the operation of electronic transfers fund involves the use of personal data and is as a result subject to the Protection of Personal Information Act.[236] The POPI Act applies to the processing of personal information entered into a record by or for a responsible party by making use of an automated or non-automated means.[237]

Section 1 defines personal information as inclusive of any identifying number, symbol, online identifier, other particular assignment to the person, correspondence sent that is implicitly or explicitly of a private or confidential. This provision clearly encompasses within its meaning, payment instructions, CVV numbers and OTPs and as such extends protection to personal information used when effecting EFTs.[238]

A bank's role in this instance is established by befitting the definition of a responsible party in terms of the Act. A responsible party means "*a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.*"[239]

The bank as a responsible party is couched with certain obligations. A responsible party is mandated to ensure security and confidentiality of personal information in its possession or under its control, by taking appropriate, reasonable technical and organisation measures to prevent *inter alia*:[240]

(i) Unlawful access to or processing of personal information.

In pursuit of compliance with this duty, the bank as a responsible party must take reasonable measures:

[236] 4 of 2013.

[237] Section 3(1)(a).

[238] Section 1. Personal information definition.

[239] Section 1.

[240] Section 19.

(i) Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control
(ii) Establish and maintain appropriate safeguards against the risks identified
(iii) Regularly verify that the safeguards are effectively implemented; and
(iv) Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

This duty is complimentary to the section 43(5) of Electronic Communications and Transactions Act[241] duty. Herein a bank is required to maintain a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned. A bank would thus in this instance be liable for any damages suffered by a consumer as a result of its failure to comply with section 43(5).[242]

The obligating of banks to ensure the safety of payment system with reference to accepted technological standards is well intended. However, the lack of directions as to what these would constitute makes this provision vague and resultantly stifles compliance in this regard.

As this Act does not make reference to any foreign law for interpretation, it would be logical to hold that the "accepted technological standards" are confined to the South African jurisdiction only. If that is then the case, this will culminate in a situation where the South African banks will be the setters of these standards as they are the only ones who provide these payment systems. This effectively results in banks being the creators of a yardstick with which they will be measured.

There is also no direction as to what sufficiently secure means, which will also make it difficult to comply with this duty.[243] In addition to that, section 86(1) criminalises the interception or accessing of any data without authority or permission to do so. Despite these duties and provisions with a deterrence effect, EFT fraud is ever present.

[241] 25 of 2002.

[242] Section 43(6).

[243] VA Lawack-Davids & FE Marx "Consumer protection measures for erroneous or unauthorized internet payments : some lessons from the European Union?" (2010) Obiter 455.

The latest prospective legislation that is relevant to this matter and is disappointingly synonymous with the laws referred to earlier is the Cybercrimes Bill.[244] Similarly, it also criminalises the unlawful accessing of data,[245] however its definition of data limits its application to electronic representations of data only. Thus once gazetted, it will not apply to stolen cards that are used for online payments in card not present transactions. This is owing to the fact that the information required for this kind of a transaction is physically represented on the card and not electronically stored.

Unlawful and intentional access data refers to *inter alia* use of the data which in itself constitutes unlawful access.[246] Unlawful access refers to when any person which encompasses both natural or juristic person, exceeds their lawful authority to access data.[247]

The bill also makes provision for criminalisation of unlawful interception of data as opposed to access only. Section 3(1) provides that any person who unlawfully and intentionally intercepts data including electromagnetic emissions from a computer system is guilty of an offence. Furthermore possession of such data with knowledge of its unlawful and intentional interception is also an offence according to section 3(2). This also the case where there is reasonable suspicion that the said data was unlawfully and intentionally intercepted and such person cannot account for it satisfactorily.[248]

A computer system refers to one or more computers that are interconnected for the exchange of data with each other or any other computer system.[249]

Section 7 is more specific in that it criminalises the unlawful and intentional acquisition, possession, provision, receipt or use of a password, access codes or similar data or device. These are regarded *inter alia* as, a secret code or pin, access card, or a word or string of characters or numbers used for financial transactions.[250]

---

[244] B 6B-2017.

[245] Section 2(1).

[246] Section 2(a)(iv).

[247] Section 2(3).

[248] Section 3(3).

[249] Section 1.

[250] Section 7(3).

Section 8 and 9 respectively criminalise cyber fraud and cyber forgery and uttering. The former relates to unlawful and intentional misrepresentations to defraud by means of data or computer program to another that causes actual prejudice or is potentially prejudicial. Whereas the latter although similar, refers to the unlawful and intentional creation or passing off of false data or false computer program to defraud another person that causes prejudice or is potentially prejudicial to another.

All the offences referred to above form part of chapter two of the bill which are made reference to in section 54. Therein, certain obligations are imposed on financial institutions. They are required on becoming aware that their computer system is complicit in the commission of a chapter two offence to:[251]

(i) report to the South African Police without undue delay, where feasible no later than 72 hours and preserve any information necessary for investigating the offence.

This bill serves as a clear acknowledgement of the scourge of cybercrime and threats to cybersecurity. The preamble states that it aims to create offences and impose penalties which have a bearing on cybercrime and further to establish structures to promote cybersecurity.[252]

The culminating effect of all these provisions indicate that the unlawful accessing of data is criminal conduct which is punishable. However it does not in any way address the losses suffered by the owner of such data. These provisions all in all serve in an afterthought manner, they do not address the losses that such an owner suffers as the data is being unlawfully accessed.

As it is now, a bank's customer will be liable for unauthorized electronic funds transfers as long as such exclusionary clauses are considered "fair" by virtue of their inclusion in bank-customer contracts. This is a precarious situation as, the only recourse available for a bank's customer in that event is to seek a credit reversal at court.[253] However as correctly put by Naude judicial control always comes too late after the

[251] Section 52(1).

[252] Cybercrimes Bill B 6B-2017.

[253] C Van Heerden "Unauthorized Cheque Payments and Electronic Funds Transfers" In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) 378.

abuse has already taken place. The need for effective, proactive control that is not solely dependent on judicial control is obvious in the light of the costs and risk of litigation.[254]

3.5 Conclusion

The current practice of solely burdening bank's customer's with the liability of unauthorized transfers is clearly unfair as determined in terms of the CPA. Nevertheless the scope of application of the CPA and the existing legal framework is limited, it lacks certainty and fails in totality to advertently provide for equity with regards to the subject matter. The continued absence of legislation to govern this issue of liability will effectively ensure bank's customer's being in this onerous position as alluded to above.

[254] T Naude "The use of black and grey lists in unfair contract terms legislation in comparative perspective" (2007) SALJ 132.

4. Chapter Four: A comparative study between the United States of America and the European Union

4.1 Introduction

This chapter will serve as a comparative analysis between the European Union and the United States of America which jurisdictions have more advanced consumer protection regulations. The analysis will primarily focus on data protection principles, unauthorized transactions and the aspect of liability in respect thereof. This will be done in pursuit of equity regarding the bank-customer relationship. A commentary will then be provided on the two jurisdictions in light of the prevailing position in South Africa.

4.2 The European Union

4.2.1 Background

The risk of payment card details being stolen has been a primary concern for the EU which has been the backdrop of numerous laws dating from as far as 1997 onwards. Resultantly, the Commission 's Recommendation on Electronic Payments from 1997, drafted as a non-binding but nevertheless informative document in retaliation to fraudulent payments over the internet.[255]

Article 6 of this recommendation provided that, the holder of payment instrument is liable up to a certain limit (which was ECU 150 at the time) in an event of loss or theft of an electronic payment instrument up until notification to the issuer. If the holder is found to be negligent by being in contravention of his obligations or fraudulent, the limitation of liability will not apply at all.[256]

More so, Article 6(3) provided that in order for the holder to be liable, the payment instrument or the electronic identification (of the instrument) must be physically presented for payment. Thus where the payment data of the holder is presented electronically without the actual card, the holder is absolved from any liability that would otherwise have ensued. This culminates in instances where the credit card

[255] A Savin *EU Internet Law* (2017) 242.

[256] *Ibid*.

numbers and other associated information (start date, end date, name on card, security code) have been stolen, obtained fraudulently or generated.[257]

The absence of a payment instrument was the determining factor for liability, thus even when extra security information (such as a password or security code) has been presented, liability does not ensue for the holder.[258] It is observed that this high standard of consumer protection effectively prevents the banks from claiming, without proving the contrary, that fraudsters have the data because the holder had been negligent.[259]

4.2.2 Data protection

Data protection under the EU is governed by the *General Data Protection Regulation (GDPR)*.[260] Its application is determined by notions of "processing" and "personal data".[261] Processing is relatively broad in that it relates to any act performed upon personal data including but not limited to, collection, recording, storage, disclosure by transmission, dissemination and even destruction.[262] Personal information relates to any information relating to an identified or identifiable natural person.[263]

Similarly it also provides for the lawful processing of personal information on the basis of consent by the data subject as is the position in South Africa.[264] Furthermore the burden of proof of consent is on the data controller[265] which is synonymous with a responsible party.[266]

---

[257] *Ibid*.

[258] A Savin *EU Internet Law* (2017) 242.

[259] *Ibid*.

[260] *Regulation (EU)* 2016/679.

[261] Article 2; THA Wisman "Privacy, Data Protection and E-Commerce" In AR Lodder & AD Murray (eds) *EU Regulation of E-Commerce* (2017) 352.;J Trzaskowski "Privacy and the Processing of Personal Data" In J Trzaskowski et al *Introduction to EU Internet Law* (2015) 81.

[262] Wisman (2017) 352

[263] *Ibid*.

[264] Article 6.

[265] Article 7. Section 11 of POPI Act.

[266] Article 5. "*Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."*

Article 24(1) of General Data Protection Regulation[267] imposes a duty on the controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulations.

The implementation of such measures should be done at the time of the determination of the means for processing and at the time of the processing, through measures such as pseudonymisation, which are intended to implement data-protection principles, such as data minimisation.[268]

Article 32(2) imposes duties to ensure a level of security appropriate to the risk associated with the processing such as unlawful access to personal data. The controller can signify compliance by virtue of adoption of internal policies and implementation of measures which meet the principles of data protection as set out in Article 25.[269] Article 32(3) provides that compliance can also be signified by adherence to an approved code of conduct or certification mechanism.

These certifications once granted, are made publicly available and are valid for a period of three years subject to renewal.[270] This will enhance consumer confidence of consumer's whose data is processed by controller's who are certified.

4.2.3 Unauthorized transactions and liability

There has subsequently been a series of directives passed that deal with the subject matter. The latest which also supersedes the earlier directives is *the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market* which repeals 2007/64/EC 2015 Directive. The processing of personal data by payment systems and payment service providers in this directive is informed by the *GDPR*.[271]

The *Directive of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market*[272] although similar to the 2007 Directive, has

[267] *Regulation (EU)* 2016/679.

[268] Article 25(1).

[269] Recital 78.

[270] Article 42 (7) - (8).

[271] *Regulation (EU)* 2016/679.

[272] 2015/2366/EU.

certain differences. These address the subject of enquiry much better as opposed to the 2007 Directive. It is common cause that in both Directives there are obligations imposed on the payment service user (PSU) and the payment service provider (PSP) equally.

A PSU refers to a natural or juristic person making use of a payment service, which encompasses the transfer of funds.[273] A payment service provider on the other hand includes banks amongst others.[274]

A payment service instrument refers to "personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order."[275] Unauthorized use of a payment instrument is however not defined.

Similarly, they both provide that the PSU shall act in accordance with the governing terms of use of a payment instrument.[276] They should further notify the PSP of any loss, theft or misappropriation of the payment instrument or its unauthorized use without undue delay on becoming aware of it.[277] However, the 2015 Directive further provides that the governing terms should be objective, non-discriminatory and proportionate.[278]

Once notification is received, the PSP must ensure that reasonable steps are taken to keep its personalised security features safe.[279]

The PSP is obliged *inter alia* on the other hand, to ensure that the personalised security credentials are not accessible to third parties, provision of free of charge notification on the part of the PSU and prevention use of a payment instrument after notification by the PSU to the PSP as described above.[280]

---

[273] Article 4; Annex I.

[274] Article 1.

[275] Article 4.

[276] Article 56(1) of *Directive* 2007/64/EC; Article 69(1) of *Directive* 2015/2366/EU.

[277] Article 56(2) of *Directive* 2007/64/EC; Article 69(2) of *Directive* 2015/2366/EU.

[278] Article 69(2).

[279] *Ibid*.

[280] Article 79 of *Directive* 2015/2366/EU.

Article 71(1) provides that a PSU should have a right to a rectification of an unauthorized or incorrectly executed payment transaction from the PSP upon notification to the PSP without undue delay but at least not later than 13 months.

Article 72(1) places the burden of proof on the PSP to establish authorisation in an event where the PSP denies having authorised an executed payment transaction or claims that it was not executed correctly. Subsection (2) provides that the record of a transaction does not in itself constitute proof that it was authorised where the PSU denies such authorisation. The PSP must provide supporting evidence to prove fraud or gross negligence on the part of the PSU.

This denounces the presumption that, the fact that there is a record of a transaction constitutes proof of authorisation by the user or that the user acted fraudulently or negligently.[281]

Article 73(1) further provides that the PSP must refund the PSU the amount payed in the case of an unauthorized payment transaction no later than by the end of the following business day after having duly been informed about the unauthorized transaction. However, the PSP is not obliged to abide by this obligation where reasonable grounds to suspect fraud exist and they have been reported to the relevant national authority in writing.

Liability of a payer is addressed by Article 74. Subsection (1) states, where a payment instrument has been stolen, lost or misappropriated, the payer may only be liable for losses relating to unauthorized use up to a maximum of EUR 50. However this limitation of liability does not apply if:

(a) "*the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or*"

(b) "*the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced*"

[281] A Savin *EU Internet Law* (2017) 243 - 244.

Obviously where the payer acts fraudulently or fails to comply with the obligations set out earlier intentionally or on account of gross negligence, the payer will be liable for the losses incurred relating to any unauthorized payment transactions. Subsection 3 provides that:

> "*the payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with point (b) of Article 69(1), except where the payer has acted fraudulently.*"

4.2.3.1 Strong customer authentication principles

Article 97(1) provides that a PSP applies strong customer authentication where the payer, accesses its payment account online, initiates an electronic payment transaction, carries out any action through a remote channel which may imply a risk of payment fraud or other abuse. [282]

Regulation EU[283] which supplements the above mentioned directive provides insight as to what constitutes strong customer authentication. PSP's are mandated to have transaction monitoring mechanisms that enable the detection of unauthorized or fraudulent payment transactions for the purpose of applying strong customer authentication and exemptions for applying them.[284]

Strong customer authentication is said to encompass two or more elements which relate to knowledge, possession and inherence which result in the generation of an authentication code.[285] This authentication code is accepted by the PSP when the payer uses it to perform the activities referred to in Article 97(1) of the 2015 directive.

These principles require that PSPs to ensure that strong customer authentication categorised under such principles is not uncovered by unauthorized parties.[286] According to an opinion by the European Banking Authority, inherence refers to something the user is and it includes amongst others, elements such as fingerprint

[282] *Directive* 2015/2366/EU.

[283] 2018/389.

[284] Article 2(1).

[285] Article 4(1).

[286] Article 6 - 8.

scanning and voice recognition.[287] Possession refers to something only the user has such as possession of a device evidence by an OTP. This does not encompass card possession evidenced by card details.[288] Knowledge elements refers to something only the user knows such as a password or PIN but not an OTP.[289]

This basically warrants a two factor authentication for online payments that should come from two different elements as discussed above. This would render an authentication process that for instance only makes use of card details printed on the card plus an OTP being non-compliant by use of one element only.[290] Furthermore authentication factors from the same element will also negate compliance with strong customer authentication.[291]

The PSP should thus ensure that the authentication code cannot be compromised through forgery or generated based on the knowledge of any other authentication code previously generated .[292]

This is achieved by ensuring that the number of failed authentication attempts before temporarily or permanently blocked do not exceed five after a given period and that the maximum time without activity by a payer online should not exceed 5 minutes *inter alia*.[293]

These monitoring mechanisms should encompass risk-based factors such as, lists of compromised authentication elements, the amount of each payment transaction signs of malware infection in any authentication procedures.[294]

---

[287] JM Campa *European Banking authority on the element of strong customer authentication under PSD2* (21 June 2019) 5 Available at https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2; Last accessed [28 October 2019].

[288] JM Campa *European Banking authority on the element of strong customer authentication under PSD2* (21 June 2019) 7.

[289] JM Campa *European Banking authority on the element of strong customer authentication under PSD2* (21 June 2019) 8.

[290] JM Campa *European Banking authority on the element of strong customer authentication under PSD2* (21 June 2019) 10.

[291] *Ibid*.

[292] Article 4(2).

[293] Article 4(3).

[294] Article 2(2).

Strong customer authentication regulations may be exclude where for instance the electronic payment transaction is considered as low risk.[295] This could manifest where the PSP having conducted a risk analysis failed to identify for instance, abnormal spending or behavioural pattern of the payer, unusual information about the payer's device/software access.[296] Relatedly, the PSP in such pursuit should consider risk factors such as the previous spending patterns of the individual payment service user.[297]

Compliance with strong customer regulations is also not required in contactless cards provided that, the individual amount does not exceed EUR 50; and the cumulative amount of previous transactions from the date of the last application of strong customer authentication does not exceed EUR 150; or the number of consecutive transactions from the last application of strong customer authentication does not exceed five.[298]

4.3 United States of America

4.3.1 Background

The non-limitation of consumer's liability for unauthorized use in EFT payments was the backdrop towards enacting legislation that deals with the subject matter.[299] Data had shown that most banks ensured that their customers were fully or mostly liable for any losses suffered as a result of unauthorized EFT transactions.[300]

Before the enactment of the Electronic Funds Transfer Act, bank's customers were liable for unauthorized transfers caused by their negligence.[301] Negligence in this regard was confined to;(a) the writing of the PIN on the card (b) having the PIN and

[295] Article 18(1).

[296] Article 18(2)(c).

[297] Article 18()3(a).

[298] Article 11.

[299] M Lewis "The Making of the Electronic funds transfer Act: A Look at Consumer Liability and Error Resolution" (1979) University of San Francisco Law Review 232.

[300] Lewis (1979) University of San Francisco Law Review 233.

[301] M Lewis "The Making of the Electronic funds transfer Act: A Look at Consumer Liability and Error Resolution" (1979) University of San Francisco Law Review 236.

card near each other, (c) providing someone else with the card and PIN to use.[302] This was thought to be plausible as it placed liability on the consumer in situations where the consumer could prevent the losses.[303]

However this created problems of proof for the consumer in that, in doing so the consumer was effectively at the bank's satisfaction if the consumer was to be reimbursed.[304] This was depicted in an example as follows:

> "…*a consumer's card was stolen and the thief wrote the consumer's PIN on the card for his or her own convenience before draining the account. If the consumer's bank eventually recovered the card, the consumer would have to prove his or innocence to the bank's satisfaction if the account was to be reaccredited."*

A consumer's PIN could easily be compromised for instance by someone peeping over the consumer's should as they enter their pin at an ATM.[305] It is also a observed that, it is required of the consumer to recall his or her PIN to effect an EFT, nevertheless the number should not be susceptible to exposure by virtue of a direct link to the consumer, e.g. birth date.[306]

Grugas contends that this places consumer's in a dilemma as consumers would then write down their PIN and keep it with the card or on the their card.[307] However, this should not really prove to be a dilemma as a consumer could very well write down the pin, but should just not keep it in close proximity with the relevant card.

---

[302] *Ibid.*

[303] *Ibid*.

[304] Lewis (1979) University of San Francisco Law Review 237.

[305] *Ibid.*

[306] FM Grugas "The Allocation of Risk in Electronic funds transfer Systems for Losses caused by Unauthorized Transactions" (1979) University of San Francisco Law Review 408.

[307] *Ibid*.

4.3.2 Data protection

Data protection in the USA is sectoral and random, there is no comprehensive general data protection law in the USA at federal level.[308] This thus entails different intensities of protection in relation to personal information, depending on the type of personal information involved.[309] Most US companies thus ascribe to voluntary guidelines of the OECD since the USA is a member of the OECD which are not legally binding.[310] This proved to be a serious drawback due to instability and lack of an independent data protection authority.[311]

The achievement of an equivalent level of data protection for free movement of data between member states was the primary goal for the EU. However this illuminated the issue of data transfer between member states and countries which do not constitute member states such as the USA.[312]

The EU thus made provision for such instances in order to prevent the circumvention of data protection laws. This is done through principles such as adequacy decision, appropriate safeguards, binding corporate rules and a limited set of derogations.[313] There was doubt as to whether USA afforded "adequate protection" in light of the prevailing circumstances.[314]

The USA is undoubtedly the most important non-member state to which the EU transfers data.[315] In order to enhance free flow of information for US companies, an adequacy decision known as "safe harbour" was thus adopted in 2000 which allowed

---

[308] A Roos "Data Protection: Explaining the international backdrop and evaluating the current South African position" (2007) SALJ 414; K Feng & S Papadopoulos "Student (K - 12) Data Protection in the Digital Age: A comparative Study" (2018) CILSA 270.

[309] Roos (2007) SALJ 414.

[310] *Ibid*.

[311] Roos (2007) SALJ 415.

[312] THA Wisman "Privacy, Data Protection and E-Commerce" In AR Lodder & AD Murray (eds) *EU Regulation of E-Commerce* (2017) 364.

[313] Wisman (2017) 365.

[314] Roos (2007) SALJ 415.

[315] THA Wisman "Privacy, Data Protection and E-Commerce" In AR Lodder & AD Murray (eds) *EU Regulation of E-Commerce* (2017) 365.

US companies to certify themselves through the US Department of commerce.[316] The effect of this was that the Safe Harbour principles where in compliance with the EU's data protection principles.[317]

However this decision was nullified by the *Maximillian Schrems v Data Protection Commissioner*[318] case as the US failed to provide equivalent data protection as the EU. This was due to surveillance practices by NSA, which had unrestricted access to data which enabled them to arbitrarily interfere with everyone's personal information not just EU citizens.[319]

Nevertheless, the USA government and the commission found a new solution by adopting a new adequacy decision known as Privacy Shield which allows US companies to certify themselves as was with the Safe Harbour principles.[320] Despite this new formation, Wismann opines that the factors which led to the nullification of the safe harbour principles are still present with the Privacy Shield.[321] There is for instance no obligation for US organisation to delete data that is no longer necessary.[322] In the contrary, this would be synonymous with the right to be forgotten in EU's GDRP.[323]

Nevertheless, the Privacy Shield[324] also mandates organizations disseminating personal information to impart measures to safeguard it from unauthorized access by considering the risk involve in processing and the nature of the personal data.

4.3.3 Unauthorized transactions and liability

Online payments in terms of USA law are regulated in terms of the Electronic Funds Transfer Act of 1978 which has passed Electronic funds transfers regulations known as (Regulation E) of 1996. Regulation 205.2 (3)(m) defines an unauthorized electronic

---

[316] THA Wisman "Privacy, Data Protection and E-Commerce" In AR Lodder & AD Murray (eds) *EU Regulation of E-Commerce* (2017) 365.

[317] *Ibid*.

[318] C-362/14.

[319] C-362/14 at paragraph 96; Wisman (2017) 365.

[320] Wisman (2017) 365.

[321] 366.

[322] *Ibid*.

[323] Article 17.

[324] Privacy Shield framework principles issued by the U.S department of commerce. Principle 4.

funds transfer as "…*an electronic funds transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit* " This excludes electronic funds transfer initiated:

(a) By any person granted access to a consumer's account by the consumer, unless the consumer has duly notified the financial institution that such authorisation has ceased;

(b) Fraudulently by the consumer or any person acting in concert with the consumer; or

(c) By the financial institution or its employee.

Regulation 205.3(b) defines an electronic funds transfer as the transfer of funds "*initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering , instructing, or authorizing a financial institution to debit or credit a consumer's account*." In essence it encompasses debit card transfers whether not performed as a POS transaction or at an ATM. Missing of note is the use of credit cards.

A consumer's liability for unauthorized transfer is neither based on a flat limitation nor fault based, but rather a hybrid of both. A fault standard places emphasis on the consumer's behaviour and his or her banks with due consideration of their circumstances and allocates liability based on principles of negligence.[325] In pursuit of such consideration a consumer's duty of safeguarding of the method of authenticating an EFT is usually factored in. A flat limitation on the other hand does not involve the analysis of the care exercised by the consumer.[326]

The US Commercial Code Subchapter VI - Electronic funds transfers[327] in section 1693g(a) provides that:

[325] FM Grugas "The Allocation of Risk in Electronic funds transfer Systems for Losses caused by Unauthorized Transactions" (1979) University of San Francisco Law Review 406.

[326] *Ibid*.

[327] Available at; https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-VI; Last accessed [12 September 2019].

"…*A consumer shall be liable for any unauthorized electronic funds transfer involving the account of such consumer only if the card or other means of access utilized for such transfer was an accepted card or other means of access and if the issuer of such card, code, or other means of access has provided a means whereby the user of such card, code, or other means of access can be identified as the person authorized to use it, such as by signature, photograph, or fingerprint or by electronic or mechanical confirmation*."

This statement is contradictory in the sense that an unauthorized electronic fund by definition denotes no authority to access and use the instrument. An accepted card on the other hand entails authorisation to make use of it by the owner, or where the owner grants authorisation to use to someone else.[328]

Section 1693f provides that a bank may within sixty days after having issued the customer's monthly statement or transaction receipt and after having received notice of an unauthorized transaction from the bank's customer investigate such a transaction and making a determination and correction within ten business days.[329]

As is the position in the European Union, in the event of a dispute of authorisation of an electronic funds transfer, the burden of proof is upon the bank to show that the electronic funds transfer was authorized or, alternatively the bank should establish that the conditions of liability set forth in subsection (a) have been met.[330]

Liability of the consumer is not static as it is dependent on the time, notice of an unauthorized transfer was given to the Bank. Regulation 205.6 provides that:

(1) A consumer's liability is limited to the lesser of $50 or the amount utilised in an unauthorized transfer where the Bank has been notified of the theft or loss of the access device use within two days becoming aware; or

[328] Section 1693(a)(1).

[329] Available at; https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-VI; Last accessed on [12 September 2019].

[330] Section1393g(b); BW Burrows "Consumer Protection and Electronic funds transfer Systems: An Analysis of the Electronic funds transfer Act of 1978" (1979) Oregon Law Review 383.

(2) Where notice is given but not within two days, liability is limited to the lesser of $500 or $50 or the amount utilised within two days before such notification.

It is not possible to change these limitation provisions by an agreement between the consumer and the financial institution.[331] The rationale behind the limitation of liability was said to be that:[332]

(i) The $50 limitation provided an incentive for the consumers to safeguard their card and pin, and report any loss or theft promptly.
(ii) It is also incentivised banks to provide secure EFT systems.
(iii) Limitation of liability provided certainty of total losses for consumers and equally that the use of PIN in the absence of any robust methods of authentication rendered it vulnerable.

Banks on the other hand had contended that $50 is very little to incentivise careful conduct and that non-limitation on their part effectively exposed them to unlimited liability.[333] However, in light of most banks placing withdrawal limits within a limited time period, the latter argument was dismissed.[334]

Regulation 205.7 makes it mandatory for banks to include the following disclosures in their contracts with consumers who make use EFT's before liability can ensue:

(a) A summary of the consumer's liability as set out above;
(b) The telephone number and address for notification of unauthorized transfers purposes.
(c) The financial institution's business days.

[331] BW Burrows "Consumer Protection and Electronic funds transfer Systems: An Analysis of the Electronic funds transfer Act of 1978" (1979) Oregon Law Review 383; FM Grugas "The Allocation of Risk in Electronic funds transfer Systems for Losses caused by Unauthorized Transactions" (1979) University of San Francisco Law Review 413;

[332] Grugas (1979) University of San Francisco Law Review 418.

[333] M Lewis "The Making of the Electronic funds transfer Act: A Look at Consumer Liability and Error Resolution" (1979) University of San Francisco Law Review 239.

[334] *Ibid*.

Despite such disclosure requirements, disclosure is still limited which leads to consumers making uninformed choices.[335] This so because, although its required of banks to inform consumers of circumstances under which they will be held liable for unauthorized transfer losses.[336] It is not a requirement to advise consumers on prompt reporting of any losses in order to avoid further liability, which in itself also lacks clarity.[337]

These provisions which limit liability for consumers are ineffective if the consumers are not informed as to when they should in order to avail themselves to these limits.[338] This contention is valid, because limitation of consumer's liability is in essence based on the time at which the compromise is reported after notice by the consumer.[339]

Another prerequisite for liability is that, where an access device has been used, it must have been an accepted access device which the bank should have provided measures to enable identification of the consumer to whom it was issued.[340] An access device is considered accepted basically when the consumer makes use of it or authorises another to make use of it.

The regulations also make provision for unauthorized transfers that is noticeable on account of a periodic statement. Once a bank issues a periodic statement that contains an unauthorized electronic funds transfer, a consumer must report such a transfer within 60 days of the bank's issuing of the statement to avoid liability for subsequent transfers.[341]

> "…*If the consumer fails to do so, the consumer's liability shall not exceed the amount of the unauthorized transfers that occur after the close of the 60 days and before notice to the institution, and that the institution establishes would not*

[335] M Budnitz "The Impact of EFT upon Consumers: Practical Problems Faced by Consumers" (1979) University of San Francisco Law Review 367 - 368.

[336] Budnitz (1979) University of San Francisco Law Review 386.

[337] Budnitz (1979) University of San Francisco Law Review 368.

[338] *Ibid*.

[339] *Ibid*.

[340] Section 205.6(a).

[341] Section 205.6(3)

have occurred had the consumer notified the institution within the 60-day period".[342]

This time limit may extended to a reasonable period where the consumer is unable to notify the bank due to extenuating circumstances. Thus consumers are liable for unauthorized transactions that could be prevented by being reported within sixty days or within a reasonable time in the event of extenuating circumstances.[343]

The consumer may notify the bank in person, by telephone, or in writing. Notification is effected when a consumer has taken reasonably necessary steps to provide the bank with the relevant information, and it does not matter whether or not an employee or agent of the bank actually received the information.[344] Thus, where the consumer mails the notice or delivers it for transmission to the bank by any other usual means, notice is deemed to have been given at that particular time.[345]

Notice may be deemed to have been constructively given when the bank is aware of circumstances leading to the reasonable belief that an unauthorized transfer concerning a consumer's account has been.[346]

4.4 Commentary in terms of South African law

The above foreign jurisdictions have robust data protection regulations. The GDRP's duty to ensure security of data from unlawful access in the EU is commensurate with POPI Act's duty ensure security and confidentiality of personal information from unlawful access. However unlike POPI Act, the GDRP further requires a banks in the context of the research to demonstrate compliance with this duty. This can be signified by means of a certificate which ultimately enhances consumer confidence.

The GDRP further mandates banks to apply strong customer authentication for online payments. The ECTA's duty to maintain a payment system that is sufficiently secure with reference to accepted technological standards is perhaps in pursuit of the same

[342] Section 205.6(3).

[343] E Broadman "Electronic funds transfer Act: Is the Consumer Protected" (1979) University of San Francisco Law Review 256.

[344] Section 205.6(5).

[345] *Ibid*.

[346] *Ibid.*

objective as the GDRP. However, the GDRP goes further by providing detail of what strong customer authentication would constitute through two factor authentication from two different elements as discussed above. This provides clarity for purposes of compliance.

Both jurisdictions' approach to the issue of liability of unauthorized transactions is quite commendable when compared to South Africa. Like South Africa, the limitation of a bank's customer's liability of an unauthorized transactions depends on the bank being notified of such transactions. The difference is in the time required for notification and the ensuing liability.

Under the EU it is required of a bank's customer to notify the bank without undue delay on becoming aware of any unauthorized transactions, where after it is required of the bank to prevent the use of the payment instrument. A bank's customer must then be refunded the amount utilised in the said transaction no later than the next business day after having notified the bank. This negates the whole process of seeking a credit reversal in South Africa which is costly and length.[347]

Under the USA jurisdiction notification warrants an investigation which must be concluded within ten days. Under both jurisdictions the onus is on the bank to establish authorisation of a transaction.

This is unlike the position in South Africa, where the consumer will have to sue the bank for breach of mandate which ultimately also entails that the onus will be on the customer to prove that the transaction was not authorised. This proves to be onerous in light of the bank's customer's circumstances. Negligence is a question of fact that warrants consideration of all relevant circumstances and such cannot be predetermined.

Liability for unauthorized electronic funds transfer under South African law is unlimited up until the point where the bank has been notified of the compromise of an access device. Under the EU, liability is limited to a maximum of EUR 50 before any notification, there's no indication however as what constitutes notification "without

[347] T Naude "The use of black and grey lists in unfair contract terms legislation in comparative perspective" (2007) SALJ 132.

undue delay". Under the USA, liability is dependent on the time of notification to the bank.

The limitation of liability under the EU is existent despite the fact they have robust authentication mechanisms specifically the strong customer authentication elements. Authentication in South Africa as discussed earlier makes use of elements in the same category such as in card not present transactions over the internet. Authentication is observed through details printed on the card (CCV *etc.*) and email or SMS notifications with one-time passwords to authorise transaction.[348] These falls under the possession element.[349]

This also the position in instances of the transfer of fund over the internet as evidenced by *Nashua Mobile (Pty) Ltd v GC pale cc t/a invasive plant Solutions*[350] All that is required to complete such a transfer is the accountholder's profile number, PIN and password an exclusive SMS sent by the bank.[351] All these authentication factors fall within one element of "knowledge" and South Africa would thus be non-compliant by the EU's standards.

4.5 Conclusion

The comparative study has given directions as to what a fair term for the allocation of the risk of unauthorized transfers in the bank-customer contract would be. Both foreign jurisdictions are quite similar in most aspects. The EU jurisdiction provides a robust regulatory regime in totality, however the USA jurisdiction provides better clarity with regards to issue of liability. In contrast to South Africa, it is clear that the background that predated regulation in the two foreign jurisdictions is similar to that of South Africa's and as such legislation should similarly be enacted. More so, safety standards in the foreign jurisdictions are robust when compared to South Africa's. Yet, they have provided for limited liability for bank's customers in online payments in certain circumstances despite their robust safety standards.

---

[348] CJ Nagel *Commercial Law* (2016) 480.

[349] JM Campa *European Banking authority on the element of strong customer authentication under PSD2* (21 June 2019) 7 Available at https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2; Last accessed [28 October 2019].

[350] A3044/2010.

[351] A3044/2010. At paragraph 18.

5. Chapter Five: Recommendations and Conclusion

5.1 Introduction

This chapter will conclude the preceding chapters as a coherent body of work. It will be indicated as to whether or not the objectives of the study were attained. Recommendations essential to the research problem will then be advanced which will mostly be derived from chapter four.

5.2 Results of the Study

Chapter Two discussed the nature and functionality of the different kinds of electronic funds transfers and their risks. It found that mandate formed the basis of electronic funds transfers and that an electronic funds transfers will be effected on the basis of payment instruction that appears to be from its relevant customer. It found alarming, the ease with which unauthorized transfers can be initiated safety concerns thus remain owing to the risk of fraud.

Chapter Three analysed the legal position of a bank's customer in light of the prevailing legislative framework. The contractual imposition of liability of unauthorized transfers on a bank's customer is unfair as determined in terms of the CPA. The CPA and the existing legal framework is inadequate in alleviating the current legal position of a bank's customer. However, the CPA is definitely the starting point for enacting legislation that deals with liability of an unauthorized transaction on the basis of unfairness of such exclusionary clauses.

Chapter Four served as a comparative analysis between the European Union and the United States of America. It found that the two foreign jurisdictions have dealt with risk allocation of unauthorized transactions between banks and their customers equitably to different strengths. Ultimately, the backdrop of the regulations in the two foreign jurisdiction is similar to the current position in South Africa, thus necessitating a legislative framework to equally. In addition, data protection laws are much clear in the EU. Principles of the *GDPR* inform the directives governing liability of unauthorized transactions. The obligations to ensure safety of personal information is further supplemented with regulations which provide much needed clarity which lacks in South Africa at the instance of the POPI Act and the ECTA.

Ultimately, it has been established that the allocation of risk in online payment methods between the banks and their customers is unfair as it is detrimental to the bank's customers and is excessively one-side in favour of the banks. There exists unequal bargaining power between the said parties owing to the lack of alternatives and freedom of choice for bank's customer's as result of necessity to make use online payments. This is relatable to the fact that the operation of most banks in South Africa similar due to little competition. The standards of a secure payment system in South Africa are relatively low in comparison to the EU's strong customer authentication principles. Yet, legislation has been enacted in the EU to regulate EFT's.

In light of the above, the existing legislative framework is inadequate in affording consumer protection to online payment methods users owing to non-applicability provisions, low standards of security of payment systems and lack of clarity for compliance.

5.3 Recommendations

Having established that the exclusionary clauses by the banks are unfair, the CPA empowers the court to make a declaration to this effect or to make an order that it considers just and reasonable. It was thus necessary to establish what would constitute a fair position for both parties in that regard.

The comparative analysis has shown that the United States of America and the European Union have provided clarity with regards to what would constitute a fair contractual term. They ascribe to limited liability as opposed to unlimited liability up until the point of notification to the bank which is the case in South Africa.

Despite this, the application of the CPA is limited in that it does not apply to juristic persons with an annual turnover of more than two million denoting a large segments of consumers who lack protection in terms of the CPA. Furthermore, litigation in pursuit of challenging unfair contractual terms is generally costly, lengthy and is only resorted to in most cases when the abuse has already taken place. There is a need for effective and proactive control that is not solely dependent on judicial control in light of the costs and risk of litigation.

The non-limitation of consumer's liability for unauthorized use in EFT payments which is the position in South Africa was the backdrop towards regulations of same in the

USA. It goes without saying that South Africa should similarly enact legislation that governs EFT transactions. South Africa's standards of safety in relation to protection of personal information from unlawful access and the maintenance of secure payments system are low and uncertain for compliance purposes. Yet when compared to the two foreign jurisdictions, the said jurisdictions specifically govern EFT transactions despite having more advanced and robust security systems in relation to data protection.

South Africa should ensure that banks demonstrate their compliance in relation to the duty to secure personal information from unlawful access this will enhance consumer confidence. In addition to that, in order to achieve a sufficiently secure payment system. The GDRP's principles of strong customer authentication should be adopted in relation to online payments.

It follows that liability of unauthorized transactions is better dealt with in the USA jurisdiction, which should form as a basis for South Africa. Liability is neither based on a flat limitation or fault standard, it consists of both which renders it being fair as opposed to the EU. Limitation of liability provides certainty of total losses for consumers, however under the EU there is no certainty as to what constitutes notification without undue delay.

Thus the USA is much more clear in limiting the liability of a bank's customer depending on the time notification was given to a bank regarding an unauthorized transaction or missing or stolen access device. This serve as an incentives for consumers to safeguard same and prompt notification on the one hand, and encourage banks to maintain secure EFT systems on the other hand. This is a win-win situation.

It should be mandatory for banks to ensure that their customers are informed about the time periods of notification for limitation of liability to ensue. It should further not be open to the two parties to alter the provisions which govern this issue of liability. This is the sole basis of the research as liability for unauthorized EFT transactions is governed privately in terms of the bank-customer contract. The scope of application should be applicable to both natural and juristic persons, to ensure broad consumer protection.

Where a dispute exists regarding the authorisation of an electronic funds transfer, the burden on proof should be on the banks to prove authorisation and not on the bank's customer.

There should equally be a duty on the banks to ensure free of charge notification by bank's customer as discussed above. Notification should encompass both oral and written means at address given to the banks at the time of opening an account. Notifications should also be deemed to have been given at the time where a consumer transmits such notification.

A definition of an authorised transaction should be provided for clarity and certainty. This will be vital for immediate remedial action for bank's customer, where such a transaction has been alleged. Where such allegations are made, the bank should de be mandate to investigate same as is the position in the USA and make resolution in respect thereof. It would be unfair to require a bank to credit a bank's customer's account no later than the next business day after notification of same without having done an investigation of its own.

5.4 Conclusion

All in all it is clear that the exclusionary terms that form part of the bank-customer contract are unfair. The existing legislative frame work is inadequate in providing consumer protection for bank's customers. The EU and USA have developed legislative measures which address this issue of liability equitably. This should form as a point of reference for South Africa. Failure to enact governing legislation, will advertently ensure that banks continue to dictate these terms and conditions to the detriment of their customers.

6. Bibliography

Books:

A Murray *Information Technology Law: The Law and Society* (2016) Oxford: Oxford University press

A Savin *EU Internet Law* (2017) Cheltenham: Edward Elgar Publishing Limited

CJ Nagel Commercial Law (2016) Durban: Lexis Nexis

E Van Eeden *Consumer Protection Law in South Africa* (2013) Durban: Lexis Nexis

FR Malan *et al Malan on Bills of Exchange, Cheques and Promissory Notes* (2009) Durban: Lexis Nexis

P Aronstam *Consumer Protection, Freedom of contract and the Law* (1979) Cape Town: Juta & Company Limited

PM Weaver *Banking and Lending Practice* (2016) Sydney: Thomson Reuters

R Kay & T Sewell *A practical approach to Contract and Consumer Law* 1984 London: Financial training Publications

Chapters in Books:

C van Heerden “Unauthorized Cheque Payments and Electronic Funds Transfers” In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) Claremont: Juta and Company (Pty) Ltd

D Hutchison “The nature and basis of contract” In D Hutchison (ed) *The Law of Contract in South Africa* (2012) Cape Town: Oxford University Press

D Swart 2000 “Online banking law and payment systems”. In R Buys (ed) *Cyber law @ SA The law of the Internet in South Africa* (2000) Pretoria: Van Schaik Publishers

M Roestoff “Payment systems” In R Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) Claremont: Juta and Company (Pty) Ltd

MW Jones “The Relationship between the Bank and the Customer” In MW Jones & HC Schoeman (eds) *An Introduction to South African Banking and Credit Law* (2006) Durban: Lexis Nexis

J Trzaskowski “Privacy and the Processing of Personal Data” In J Trzaskowski et al *Introduction to EU Internet Law* (2015) Copenhagen: Ex Tuto Publishing A/S

Ramdhin “The Bank-Customer Relationship” In Sharrock (ed) *The Law of Banking and Payment in South Africa* (2016) Claremont: Juta and Company Ltd

S Eiselen “E-commerce” In D Van der Merwe (ed) *Information and Communication Technology Law* (2008) Durban: Lexis Nexis

S Eiselen “E-commerce” In D Van der Merwe (ed) *Information and Communication Technology Law* (2016) Durban: Lexis Nexis

S Miller “Payment in an On-Line World” In L Edwards & C, Waelde *Law & the Internet: a framework for electronic commerce* 2000 Oxford: Hart Publishing

S Papadopoulos “Online consumer protection” In S Papadopoulos & S Snail (eds) *Cyber law @ SA The law of the internet in South Africa* (2012) Pretoria: Van Schaik Publishers

Schulze WG. “Banks and Banking Law”. In Sharrock (Ed.) *The Law of Banking and Payment in South Africa*. 2016 Claremont: Juta and Company Ltd

T Woker “Consumers and contracts of purchase and sale” In D McQuoid-Mason (ed.) *Consumer law in South Africa* (1997) Kenwyn: Juta and Co Ltd

THA Wisman “Privacy, Data Protection and E-Commerce” In AR Lodder & AD Murray (eds) *EU Regulation of E-Commerce* (2017) Cheltenham: Edward Elgar Publishing Limited

Journal Articles:

A Roos “Data Protection: Explaining the international backdrop and evaluating the current South African position” (2007) 124 SALJ 400 - 436

BW Burrows “Consumer Protection and Electronic funds transfer Systems: An Analysis of the Electronic funds transfer Act of 1978” (1979) 58 Oregon Law Review 363 - 386

E Broadman “Electronic funds transfer Act: Is the Consumer Protected” (1979) 13 University of San Francisco Law Review 245 - 272

Erlank & Ramokanate “Allocating the risk in software failures in automated message systems (autonomous electronic agents)” (2016) 28 SA Mercantile Law Journal 201 - 237

FM Grugas “The Allocation of Risk in Electronic funds transfer Systems for Losses caused by Unauthorized Transactions” (1979) 13 University of San Francisco Law Review 405 - 429

FR Malan & JT Pretorius “Credit Transfers in South African Law (1)” (2006) 69 THRHR 594 - 612

H Schulze “Unauthorized cash withdrawals with a credit card and unfair contract terms” (2004) 17 Juta Business Law 143 – 146

K Feng & S Papadopoulos “Student (K - 12) Data Protection in the Digital Age: A comparative Study” (2018) 2 CILSA 261 - 281

M Budnitz “The Impact of EFT upon Consumers: Practical Problems Faced by Consumers” (1979) 13 University of San Francisco Law Review 361- 404

M Lewis “The Making of the Electronic funds transfer Act: A Look at Consumer Liability and Error Resolution” (1979) 13 University of San Francisco Law Review 231 - 244

RD Sharrock “Judicial Control of Unfair Contract Terms: The Implications of Consumer Protection Act” (2010) 22 SA Merc LJ 308 - 325

T Budhram “Lost, Stolen or Skimmed -Overcoming credit card fraud in South Africa” (2012) 40 SA Crime Quarterly 31 - 37

T Naude & C Koep “Factors relevant to the assessment of the unfairness or unreasonableness of contract terms” (2015) 1 Stell LR 85 -109

T Naude “The use of black and grey lists in unfair contract terms legislation in comparative perspective” (2007) 124 SALJ 128 - 164

T Naude “Unfair contract terms legislation the implications of why we need it for its formulation and application” (2006) 17 Stell LR 361 - 385

VA Lawack-Davids & FE Marx “Consumer protection measures for erroneous or unauthorized internet payments : some lessons from the European Union?” (2010) 31 Obiter 446 – 458

WG Schulze “Countermanding Electronic transfers: The Supreme Court of Appeal takes a second bite at the cherry” (2004) 16 SA Merc LJ 667 - 664

WG Schulze “E Money and Electronic transfers: A shortlist of some of the unresolved issues” (2004) 16 SA Merc LJ 50 - 66

WG Schulze “Of credit cards, unauthorized withdrawals and fraudulent credit-card users” (2005) 17 SA Merc LJ 202 - 213

Cases:

AB and Another v Pridwin Preparatory School and Others 2019 (1) SA 327 (SCA)

Absa Bank Ltd v Hanley 2014 (2) SA 448 (SCA)

Afrox healthcare Ltd v Strydom 2002 2002 (6) SA 21 (SCA)

Barkhuizen v Napier CCT 72/05

Diners Club SA (Pty) Ltd v Singh and Another 2004 (3) SA 630 (D)

Director General of Fair Trading v First National Bank plc [2001] UKHL 52.

Four Wheel Drive Accessory Distribution Cc v Rattan NO 2018 (3) SA 204 (KZD)

Four Wheel Drive Accessory Distribution Cc v Rattan NO 2019 (3) SA 451 (SCA)

Fourie v Van der Spuy & De Jongh Inc and Others 2020 (1) SA 560 (GP)

Maximillian Schrems v Data Protection Commissioner C-362/14

Nashua Mobile (Pty) Ltd v GC pale cc t/a invasive plant Solutions A3044/2010

Nissan South Africa (Pty) Ltd. v Marnitz NO and Others 2005 (1) SA 441 (SCA)

Sasfin v Beukes 1989 (1) SA 1 (1)

Standard Bank of South Africa Ltd v Oneanate Investments (Pty) Ltd (in Liquidation) 1998 (1) SA 811 (SCA)

Volkskas Bpk v Johnson 1979 (4) SA 775 (C)

Legislation:

Consumer Protection Act 68 of 2008

Electronic Communications and Transactions Act 25 of 2002

National Credit Act 34 of 2005

Protection of Personal Information Act 4 of 2013

Foreign regulations:

Directive (EC) 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market

Electronic funds transfer Regulations (Regulation E) 1996

European Union's Unfair Terms in Consumer Contracts Directive 93/13 [1993]

General Data Protection Regulation (EU) 2016/679

Privacy Shield framework principles issued by the U.S department of commerce

Regulation (EU) 2016/679

Regulation EU 2018/389

Unfair Terms in Consumer Contracts Regulations SI 1999 No 2083 (UK)

Others:

Code of Banking Practice of 2012

Cybercrimes Bill B 6B-2017

Government Gazette 34181

Online sources:

JM Campa *European Banking authority on the element of strong customer authentication under PSD2* (21 June 2019) 5 Available at https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2; Last accessed [28 October 2019].

US Commercial Code Subchapter VI - Electronic funds transfers available at; https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-VI; Last accessed on [12 September 2019]

Available at; http://www.pasa.org.za/home/2019/07/30/media-statement---reduction-in-maximum-cheque-value; Last accessed [08 February 2020]

Available at; https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-VI; Last accessed [12 September 2019]