

Liability of banks for unauthorised credit transfers

By

D N Morifi

Student Number: 15395172

Submitted in Partial fulfilment of the requirements for the degree

LLM Banking Law

in the FACULTY OF LAW

at the University of Pretoria

Supervisor

Professor C M Van Heerden

December 2019

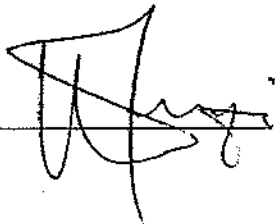
DECLARATION OF ORIGINALITY

I, D N Morifi (student nr 1539172)

hereby declare that:

1. I am aware of the University's policy on plagiarism and the implications thereof,
2. This mini dissertation is my own work, and that all sources of information contained herein have been acknowledged and referenced in accordance with the departmental policies.
3. To my knowledge, the dissertation has not previously been submitted by anyone for any academic examination towards any degree in any other University.
4. I have not allowed anyone to copy this dissertation.

Signed:
D N Morifi

A handwritten signature in black ink, appearing to be 'D N Morifi', written over a horizontal line. The signature is stylized and somewhat cursive.

ACKNOWLEDGEMENTS

First thing first, I would like to thank God for His divine enabling grace in my life, indeed His grace gave me everything I will ever need to live this life. I will forever be grateful and thankful for His fresh mercies that endures forever.

I would also like to thank my supervisor professor CM Van Heerden for her invaluable guidance and support. More importantly, I would like to thank her for her enduring patience and restraint in spite of the repeated and at times senseless errors. I am certain I tested your patience to the very last, and how you managed to always smile and be supportive (at least in our meetings) will always be both baffling and admirable to me. May my richly God keep increasing you and your family.

I would also like to thank my whole family especially my parents Eliphaz and Dinah Morifi who supported me through thick and thin, my wife Minkie Morifi my three princesses Phuti, Phuti Junior and Bokamoso Morifi, my aunt Rosalia Selepe, my granny Crestinah Selepe, Sebolaishi Morifi (may your precious soul continue to rest in eternal peace), my sister Rose Morifi, my brothers Mahlatse Morifi, Noko Chokoe & my nephews Thato and Kgaugeo Morifi. I am indebted to say thank you to all my primary, high school teachers and all my lectures at the University of Limpopo. Finally, I would like to thank my classmates and colleagues who kept me plugging away when I felt I could not do no more. The faith and love you showed me when it mattered most can never be quantified.

Summary

Modern consumers rely largely on electronic fund transfers as a method by which to effect payment to other persons. In South Africa the situation is no different except that South Africa lacks a comprehensive framework for the regulation of electronic fund transfers.

The absence of such legal framework is especially problematic in the context of credit transfers that are made without authorization or sometimes as a result of a mere mistake by the originator of the payment instruction. Given the absence of a dedicated legal framework to govern the liability of the parties in these situations, the position is that the bank customer agreement largely govern such liability. Because the ease with which fraud and theft can be perpetrated in respect of electronic transfers and because these transfers are effected so speedily banks have sought to cover themselves against the risks of loss or theft and onload most of the liability onto the customer in the bank-customer agreement. Banks are also reluctant to assist with credit transfers even in cases where the transfer was caused by theft or fraud.

Despite developments in case law the position has not yet reached an acceptable solution. This dissertation considers the nature of credit transfers and the position where the bank and alternatively the customer is to blame for unauthorised and erroneous credit transfers. The developments in case law in relation to reversal of credit transfers is also specifically interrogated. In order to find a solution the dissertation consider the adoption of an ePayments Code such as in Australia.

Index

1 Chapter one Background to the study

1.1 Introduction.....	1
1.2 Research Statement.....	2
1.3 Research Objectives.....	3
1.4 Research Methodology.....	3
1.5 Slection of Comparative Jurisdiction.....	3
1.6 Lay-out.....	3

2 Chapter two Where the originator's bank effects an erroneous credit transfer

2.1 Introduction.....	4
2.2 The sui generis nature of electronic transfer.....	6
2.3 Erroneous credit transfers by the originator's bank.....	7
2.4 Forged/Unauthorized payment instruction	10
2.5 Development in case law.....	12

3 Chapter Three

3.1 Introduction.....	13
3.2 Countermand of payment.....	14
3.3 Reversal of credit transfer	16
3.4 Further developments in case law.....	18
3.5 Development in case law subsequent to Pestana.....	20
3.6 The problem revealed in the Lombard Insurance case.....	22
3.7 Final Remarks.....	24

4 Chapter four

4.1 Introduction	26
4.2 The payment code.....	26
4.3 When the holder is not liable.....	27
4.4 When the holder will be liable for loss.....	28
4.5 Pass code (pin) security requirements.....	30

BIBLOGRAPHY	34
--------------------------	-----------

1.1 Introduction

The modern consumer lives in a world where technology reigns. His life is digitised, he surfs the internet and craves the newest smartphone and Netflix-series on his flat screen television. As a consumer of financial products and services he does not make use of what he perceives as archaic payment instruments, namely cheques. In fact many young adults in these modern times have rarely ever seen a cheque. They use electronic fund transfers as their preferred payment method.¹

As observed by Schulze, in its most simple form an electronic funds transfer, which can be divided into credit and debit transfers, is just like a cheque – “an instruction by the customer to the bank for the transfer of money to another account or to the beneficiary.”² In the case of a credit transfer, the person who wishes to make payment (the originator), gives an instruction to his bank (the originator’s bank) to transfer the funds from his account to the account of the person he wishes to pay (the beneficiary).³ In the case of a debit transfer, the person to whom payment must be made (the creditor), claims the money from the bank where the debtor keeps his account.⁴ The money that is transferred into the account of the beneficiary, once it becomes available to be withdrawn, loses its separate identity. This is because of the principle of *commixtio*⁵ which means the money that is transferred becomes part of the debit or credit balance in the account of the beneficiary.

¹ An electronic funds transfer is not a payment instrument but rather a method of payment. See Schulze 'Countermanding an electronic funds transfer: The Supreme Court of Appeal takes a second bite at the cherry' (2004) 16 *SA Merc LJ* 668 670-671.

² Schulze in *Havenga (ed) Commercial law* 413.

³ *Ibid.*

⁴ *Ibid.*

⁵ See Schulze 'Electronic funds transfers and the bank's right to reverse a credit transfer: one small step for banking law, one huge leap for banks' (2007) 19 *SA Merc LJ* 379 384

1.2 Research statement

South Africa does not currently have any comprehensive and dedicated legislative framework dealing specifically with electronic fund transfers.⁶ As indicated by Schulze, the legal relationship between the parties to electronic transfers are therefore governed in a fragmented manner by the common law of contract and the common law of mandate (as captured in the bank-customer agreement), and to a very limited extent by legislation such as the National Credit Act,⁷ and the Electronic Communications and Transactions Act⁸ and soft law such as the Code of Banking Practice and the (confidential) inter-bank agreement.⁹

The absence of a dedicated legislative framework on electronic fund transfers is particularly problematic when one considers the situation of erroneous (wrong) credit transfers. Such erroneous credit transfers may occur where an account holder (the originator) gives incorrect instructions regarding the amount, or date or beneficiary to whom the payment has to be made. The incorrect instruction may for example be given in writing to a bank but will most likely these days occur via an Automated Teller Machine (ATM)-transaction or an internet banking transaction. It may of course also happen that the originator's bank can make a mistake that causes the wrong person to be paid, or a wrong amount to be transferred or results on payment on a wrong date.¹⁰ Given the lack of legislation to regulate these issues the question then arises who is responsible for the loss suffered by the customer and whether such an erroneous credit transfer can possibly be reversed? This dissertation will consider the liability of the parties in the event of an erroneous credit transfer and whether reversal of an erroneous credit transfer is possible and if so, under what circumstances. It will first consider the situation where the originator's bank is responsible for the mistake. Thereafter it will consider the situation where the account holder (originator) has

⁶ See Schulze (2004) 16 *SA Merc LJ* 50; Visser 'The evolution of electronic payment systems' (1989) 1 *SA Merc LJ* 189.

⁷ Act 34 of 2005.

⁸ Act 25 of 2002.

⁹ Schulze (2004) 16 *SA Merc LJ* 57 indicates that although the Electronic Communications and Transactions Act provides a wide and general framework for the facilitation and regulation of electronic communications and transactions, including electronic transactions for financial services (e.g. s 42) it does not deal exclusively with electronic banking services and a number of aspects surrounding the use of electronic banking products are not necessarily covered by the said Act.

¹⁰ Van Heerden in Sharrock (ed) *The Law of Banking and Payment in South Africa* chapter 10 at 162 (hereinafter Van Heerden).

caused the erroneous credit transfer to be made. This study will focus on credit transfers only and will not deal with debit transfers.

1.3 Research objectives

The research objectives of this study will be: (a) to determine the nature of a credit transfer and what implications it holds for the liability of the parties for erroneous credit transfers and the issue of reversal of an erroneous credit transfer;

(b) to consider how the bank-customer relationship and Code of Banking Practice may impact the liability of the parties for erroneous credit transfers and the issue of reversal of a credit transfer;

(c) to consider any developments in case law that impacts on the liability of the parties for erroneous credit transfers and the question as to whether an erroneous credit transfer may be reversed;

1.4 Research Methodology

The research methodology will, given the lack of legislation specifically governing credit transfers, mainly comprise of a critical analysis and evaluation of applicable cases and opinions of authors as expressed in text books and law journals.

1.5 Selection of comparative jurisdiction

This dissertation will make reference to Australia as a comparative jurisdiction. Australia has had a Code dealing with electronic payments since 1986 and the current ePayments Code makes extensive provision for addressing the position relating to unauthorised credit transfers.

1.6 Lay-out

Chapter one provides the roadmap to the study and gives background as well as the research question and objectives, research methodology and selection of comparative jurisdiction, and the chapter lay-out. Chapter Two deals with the situation where the bank made unauthorised or erroneous payments and Chapter Three deals with erroneous payments by the customer. Chapter 4 is the final chapter-it gives an overview of the ePayments Code and makes some suggestions for the way forward for South Africa.

Chapter 2 Where the originator's bank effects an erroneous credit transfer

2.1 Introduction

Before exploring the research question and objectives of this study it is necessary to contextualise the discussions that follow by dealing with some general principles applicable to credit transfers.

Credit transfers (as a type of electronic fund transfers) are effected by means of payment orders by a customer (the originator) to his bank in terms of the general bank and customer agreement or general mandate in terms of which the bank is obliged to give effect to payment orders of the customer.¹¹ Malan and Pretorius indicate that, by characterising the bank - customer agreement as a "general mandate" that provides for the payment of payment orders given by the customer, the naturalia of the agreement can be determined.¹² When payment is effected by electronic funds transfer the bank that effects the payment does not represent its customer – this means it is not its customer's "agent" but only functions as a mere mandatary.¹³ Similarly the payee or beneficiary is also not represented by the beneficiary bank (the bank that receives the payment into the account of the beneficiary) when it collects payment and the beneficiary banks thus also acts as a mandatary only.¹⁴

The common law of *mandatum* lays down certain requirements that banks must comply with when they are acting as a customer's mandatary, namely: ¹⁵

- (a) banks must exercise reasonable care and skill in the exercise of their mandate;
- (b) the mandate should be carried out within a reasonable time;
- (c) the mandate should be carried out without negligence; and
- (d) the mandatary must perform its mandate in good faith.¹⁶

¹¹ Malan and Pretorius 2006 (69) *THRHR* 602; Schulze 'The sources of South African Banking Law - A Twenty-First Century Perspective (Part 11)' 2002 *SA Merc LJ* 601-621; Schulze 'Duty of a Bank to Act with Necessary Skill and Care when Issuing an Automated Teller Machine Card' (2007) *De Jure* 371-372-377; Schulze 'Depositum, Deposit and Deposit-taking Institutions – Birds of a Feather? Not Quite' (2001) 13 *SA Merc LJ* 78.

¹² Malan and Pretorius 2006 (69) *THRHR* 603.

¹³ Malan, Pretorius & Du Toit 279. See *B&H Engineering v First National Bank of SA Ltd* 1995 (2) SA 279 (A) 293. See also Schulze 'E money and electronic fund transfers. a shortlist of some of the unresolved issues' (2004) 16 *SA Merc LJ* 5053.

¹⁴ Malan, Pretorius & Du Toit 279.

¹⁵ Malan, Pretorius & Du Toit 280.

¹⁶ Malan, Pretorius & Du Toit 280; Comte 12-16.

The main duty of the originator's bank, arising from banking practice, is to adhere strictly to the terms of the payment order.¹⁷ In addition, the bank who provides electronic funds transfer services is obliged to install and maintain a reasonably efficient security system and to ensure that the system is operating efficiently.¹⁸

Like the bank the customer also has certain duties imposed by the common law and generally confirmed in the bank-customer agreement. It is the customer's duty at common law to draw his payment instruction with reasonable care "so as not to facilitate fraud or deception" and to make sure that the payment order is 'clear and unambiguous'.¹⁹ This duty is also confirmed by paragraphs 7 and 9 of the Code of Banking Practice which is a soft law instrument adopted by the Banking Association of South Africa (BASA) in 2004 and subsequently revised in 2012.²⁰

It is also necessary to consider the role of the beneficiary bank to determine whether the beneficiary bank has any specific obligations in respect of the customer (the originator) who gives his bank (the originator's bank) instructions to effect a credit transfer to the beneficiary's account that is held in the beneficiary bank. As pointed out by Malan and Pretorius there is no contractual relationship between the originator and the beneficiary bank, even if the beneficiary bank is regarded as a mere submandatary of the originator's bank.²¹ In principle therefore the beneficiary bank owes no contractual duty to the originator in terms whereof the originator can require the beneficiary bank to return monies that were erroneously transferred.

Due to the absence of legislation in South Africa on electronic fund transfers it is therefore clear that the bank-customer agreement between the originator and the originator's bank is the main source to which regard must be had if one wishes to determine the position in relation to credit transfers that were erroneously made.

A last aspect to mention is that South Africa has a comprehensive legal framework, the Bills of Exchange Act,²² in relation to cheque payments that provide for various matters relating to cheques and also deals with the liability of the parties for erroneous

¹⁷ Malan and Pretorius 2006 (69) *THRHR* 604. See also Comte 15-16.

¹⁸ Malan, Pretorius & Du Toit 280.

¹⁹ Comte 15.

²⁰ See par 7 and 9 of the Code of Banking Practice 2012 available at www.banking.org.za (accessed on 19 September 2019).

²¹ Malan & Pretorius 2006 (69) *THRHR* 606. See also *Gilbeys Distillers and Vintners v ABSA Bank* unreported case no 12698/94 (C) par 60.

²² Act 34 of 1964.

cheque payments. However it should be noted that cheques are payment instruments whereas electronic credit transfers are payment methods. The Bills of Exchange Act is not applicable to electronic fund transfers. The Bills of Exchange Act provides some protection to banks that made erroneous cheque payments in certain listed instances. This means that insofar as cheques are concerned there is a legislative framework governing the liability of the parties. There is however no such legislative framework that deals with liability of the parties where erroneous credit transfers are made. Malan and Pretorius²³ however indicate that although the techniques involved in making payment by electronic funds transfer, specifically credit transfers, may differ from those employed when a cheque is used, their legal constructions are not necessarily different.²⁴ In this regard they emphasise that payment by credit transfer is payment of the underlying debt for which the payment order is given.²⁵ This is a very important principle as it plays a guiding role in how to deal with the liability aspect when an erroneous credit transfer is made.

2.2 The sui generis nature of electronic fund transfers

One of the hallmarks of electronic funds transfers is the speed and ease with which they can be effected. Generally the transfer is effected instantaneously at the moment that the payment instruction is received and processed. There is generally no "lag"-time within which to stop an electronic funds transfer that has been given to the customer's bank before the money gets transferred to the beneficiary's account at the beneficiary bank. Although the speed and ease with which electronic fund transfers can be effected is one of the reasons that make this payment method so popular it is unfortunately also one of its greatest drawbacks when viewed from the perspective of erroneous electronic fund transfers because it means that there is generally very little, but more usually no time to stop a transfer that follows pursuant to an erroneous transfer instruction.²⁶

A further important issue to take note of is that payments by electronic fund transfers in general, are processed or cleared on the basis of an account number only.²⁷ This

²³ Malan & Pretorius 2006 (69) *THRHR* 597.

²⁴ Malan & Pretorius 2006 (69) *THRHR* 605.

²⁵ Schulze (2004) 16 *SA Merc LJ* 673 provides an indication of the differences between payment by electronic funds from payment by cheque.

²⁶ Meiring 41.

²⁷ Schulze (2004) 16 *SA Merc LJ* 60.

means the bank works with the account number only and does not verify that the account to which the money is transferred indeed belongs to the beneficiary to whom the originator of the payment instruction indicated that the money should be transferred. Schulze states that this is in stark contrast with the clearing processes of cheques. He points out that in the case of a non-transferrable cheque, the practice is that both the account number and name of the payee are compared to ascertain whether the payment instruction indeed matches the designated payee or beneficiary and his bank account.²⁸ So with cheques there is at least some safeguard built into the process of clearing cheques that may serve to prevent loss to customers should it appear that the cheque is paid into an account which does for example not match the details of the payee of the cheque.

As observed by Van Heerden there is a dearth of authority in South Africa regarding the liability of banks for unauthorised payments in the context of electronic funds transfers. She indicates that this is due to the lack of a dedicated legislative framework. She is also of the view that it because the bank-customer agreement generally allocates the risk for unauthorised electronic payments to the customer, it explains why very few cases make their way to the courts.²⁹ Nevertheless when an erroneous credit transfer is made it gives rise to questions regarding the liability of the parties and who should bear the loss as well as whether it may be possible to reverse such a credit transfer.

2.3 Erroneous credit transfers by the originator's bank

As indicated above an originator's bank that is instructed to make a credit transfer on behalf of its customer merely acts as a mandatory of the customer. This means that the bank does not act as the customer's agent and does not incur any obligations in this regard on behalf of its customer. The bank merely has to make sure that it complies with its duties as mandatory which includes processing the transaction with reasonable care and skill, without negligence, in good faith and within a reasonable time. It has also been indicated that the main duty of the mandatory is to act strictly in

²⁸*Ibid.* See also Pretorius 'Aspects of the collection of a cheque cleared through an Automated Clearing Bureau' (1998) 10 *SA Merc LJ* 326; 'Codeline clearing' (2001) 13 *SA Merc LJ* 260.

²⁹ Van Heerden at 166.

accordance with its customer's payment instruction. Where an erroneous credit transfer is effected by a bank a number of questions should therefore be asked:

(a) did the customer draft the payment instruction with the necessary care so that it was clear what the bank's mandate was?

(b) did the bank execute the transfer with the necessary skill and care, without negligence, in good faith and in a reasonable time?

(b) if the customer was not negligent in drafting the payment instruction can the bank who erroneously effected a credit transfer (for example to the wrong person or in the wrong amount) be liable towards the client for any losses that the client suffers due to the erroneous payment?

(c) will it be possible for a bank who has erroneously effected a credit transfer without or contrary to its mandate, to prevent loss to its client by merely reversing such erroneous credit transfer?

The general rule, having regard to the law of contract and the law of mandate as captured in the bank-customer agreement, is that if the originator's bank transfers funds from its customer's account without the customer's authorisation, the bank breaches its mandate. In such instance the bank generally has no defence and can be held liable in terms of the bank-customer agreement which lays down its responsibilities as mandatary.³⁰ If the bank pays out money by means of an electronic funds transfer that was not authorised by the customer, it will thus as a general rule not be able to debit its customer's account. However, because it is so easy to perpetrate fraud in respect of electronic funds transfers and because of the lack of governing legislation, the bank-customer agreement will generally govern and tailor the liability of the bank for unauthorised electronic payments and, unless of course the client happened to be negligent and failed to draft or give its payment instruction with the required care, it will provide for the risk of erroneous transfers by indicating which party will bear the loss in such an instance.

As a starting point the particular bank-customer agreement will therefore have to be consulted in such an instance in order to determine whether it indemnifies the bank

³⁰ Schulze (2004(2)) 61.

regarding such payments or whether it otherwise allocates the risk of loss to the customer.³¹ If it is merely a case where the bank clearly made a mistake, for instance by transferring an amount to a wrong beneficiary because the bank employee who had to make the payment negligently typed in the wrong digits, then there should be no doubt that the bank, based on the clear and negligent breach of mandate, should be (vicariously) liable towards its customer for any loss that the customer may suffer. It is submitted that it is highly unlikely that the bank-customer agreement would exclude the bank's liability in such an instance of clear mistake by the bank.

However the matter becomes more problematic when the bank effects an incorrect transfer that the client never authorised because someone, pretending to be the bank's real customer, fraudulently gave the bank instructions to make the transfer. This can happen where for instance the customer's bank card is stolen and the thief knows or ascertains the pin of the card and instructs the bank through the use of an automated teller machine (ATM) to make a credit transfer into the account of a beneficiary of the thief's choice. It can also happen where a person, pretending to be the bank's real customer, issues a written payment instruction to the bank to pay someone of his choice by means of a credit transfer made from the real customer's account. Also, it is possible that a written payment instruction by a customer of the bank may be intercepted by a fraudster who changes the amounts on the instruction or the account details of the beneficiary. There are numerous scenarios in which such an unauthorised transfer may be triggered by a thief or fraudster. Especially with bank cards such fraudulent transactions can easily be perpetrated. The question then arises whether the bank can be held liable towards its own customer to make good any losses suffered by the customer?

³¹ Van Heerden at 167.

2.4 Forged or unauthorised payment instruction

As pointed out, where a customer gives an oral or written instruction to his bank to effect a credit transfer, the risk of forgery and unauthorised payment clearly presents itself. Where the payment instruction is expressed in computer language, for example by means of a payment instruction made via a bank card at an ATM machine, the handwritten signature is replaced by an electronic key that is used to authenticate the message.³² Schulze points out that this instruction or message can, in the absence of sufficient security measures, be altered, erased or transferred to another medium without this fact becoming known by examination of the medium.³³ A third party who has knowledge of the PIN for the card will thus be in a position to use the card to make withdrawals or to effect credit transfers from the account of the bank's real customer.

Because it is so easy to perpetrate fraud where a bank card is used to effect an electronic funds transfer it is to some extent quite understandable why banks generally seek to incorporate provisions into the bank–customer agreement to protect themselves against the risk of liability for unauthorised payments. Generally, because there is no comprehensive and dedicated governing legislation in South Africa regarding electronic funds transfers, banks have taken measures to protect themselves by incorporating certain standard terms in the bank–customer agreement that deal with liability in the context of unauthorised electronic fund transfers. These provisions generally entail that the risk for loss due to unauthorised payment as a result of theft or fraud is largely allocated to the customer.³⁴

As pointed out by Van Heerden, the Code of Banking Practice impliedly reinforces the measures taken by banks to protect themselves against liability in the context of electronic funds transfers. This is because the Code requires the customer to keep his PIN, password or other unique means of identification personal and never to disclose it to anyone, including a bank employee.³⁵ The Code also states that the customer will be responsible for all transactions relating to additional or secondary cards. The customer is required to take care of his cards, passwords and other means of personal

³² Schulze *Commercial Law* 430.

³³ Schulze *Commercial Law* 430–1..

³⁴ See Comte 19 for examples.

³⁵ Paragraph 7.6 of the Code of Banking Practice 2012.

identification 'to help prevent fraud'.³⁶ In terms of the Code the customer must inform the bank "as soon as possible" if the customer suspects that his card has been stolen. The same applies where the customer knows or suspects that or a third party unlawfully knows the customer's PIN, password, information regarding the customer's accounts or personal information or other unique means of personal identification.³⁷ If the customer notes any unauthorised transactions on his account the Code obliges him to inform the bank thereof as soon as possible.³⁸

In addition to loading these safekeeping and notification obligations onto the customer, the Code also sets out some specific rules regarding liability for transfers that the customer allegedly did not authorise. In this regard the Code provides that the customer will be responsible for losses where he acted fraudulently or negligently because he did not keep his PIN confidential or because he failed to report the theft or loss of his card as soon as he became aware thereof.³⁹ Comte states that the extent to which these provisions will be binding in a court of law are uncertain because the Code is not a binding legal instrument.⁴⁰ However it is submitted that the Code clearly reflects the practice of the banks in relation to erroneous payments and one can surmise that if the Code merely mirrors what the bank-customer agreement provides then in practice this reflects the way that liability of the parties will play out where an erroneous electronic transfer that was effected by means of fraud or theft, is concerned.

Where a customer gives a written instruction for an electronic funds transfer and the customer drafted the payment instruction in a manner which facilitates fraud and which can be said to be the proximate cause of his loss, the customer will have to bear the loss. This is clear from the common law that requires the customer to take care when drafting a payment instruction and the Code of Banking Practice which also imposes such an obligation on him. As pointed out by Comte, the bank–customer agreement generally also provides that if the proximate cause of the unauthorised payment was that the client lost his card or his card was stolen and he failed to report such loss or

³⁶ These precautions that the customer is obliged to take are listed in para 7.7 of the Code of Banking Practice 2012.

³⁷ Paragraph 7.7.8 and 7.7.9 of the Code of Banking Practice 2012.

³⁸ Paragraph 7.7.10 of the Code of Banking Practice 2012.

³⁹ See para 7.8 of the Code of Banking Practice 2012. The Code explicitly excludes the liability of banks for certain losses beyond their reasonable control and lists examples of these in paras 7.10.6–7.10.9.

⁴⁰ Comte 18.

theft timeously (that is, before any unauthorised transfers or withdrawals are made) to the bank he bears the risk for the subsequent loss of money.⁴¹ This will also be the position where the customer does not guard his PIN and it becomes possible for a third party who has acquired the number of the PIN to make unauthorised transfers or withdrawals from the customer's account. In these situations the customer will not be able to hold the bank liable for his loss. This will also be the situation also where the customer was aware of a forgery or unauthorised payment instruction but failed to warn the bank timeously thereof, as indicated in the bank-customer agreement and the Code of Banking Practice.

2.5 Developments in case law

*Diners Club Ltd v Singh*⁴² is the first case that is pertinent to the issue of unauthorised credit transfers made with a bank card. In this matter the relationship between a bank and its customer was considered in the context of alleged unauthorised withdrawals made with the customer's credit card. The bank-customer agreement between Diner's Club and Singh contained a clause which provided that the customer, being the cardholder to whom the card was issued, would be liable for amounts credited to the customer's account by the use of the card, regardless of who actually used the card and PIN. Singh attacked the provisions of the bank-customer agreement as being unfair and unenforceable but the court upheld the said clause and Singh lost the case.

Van Heerden submitted that due to the subsequent coming into operation of the Consumer Protection Act⁴³ courts will now, in instances where the said Act applies, be able to scrutinise the provisions of the bank-customer agreement for unfair contract terms and non-compliance with the prescriptions of the Act regarding exemption clauses. However these remarks by Van Heerden were made before the recent coming into operation of the Financial Sector Regulation Act 9 of 2017 as a result whereof the Consumer Protection Act does not apply to financial services anymore. Given that the envisaged Conduct of Financial Institutions Act (COFI), which will provide provisions regarding financial consumer protection, has not yet been enacted it would thus seem that the customer in the aforesaid instance will not have legislative backing from either the Consumer Protection Act nor from any dedicated financial

⁴¹ See Comte 19.

⁴² 2004 (3) SA 630 (D).

⁴³ Act 68 of 2008.

sector legislation as same is currently lacking. It would thus seem that the decision in *Diners Club v Singh* would still reflect the current legal position – as has also since been confirmed by paragraphs 7 and 9 of the Code of Banking Practice.

Very few cases have since made their way to the courts in instances where unauthorised payments take place in circumstances as described above. One such recent case where things played out for the better, from the customer's perspective, was *ABSA Bank Ltd v Hanley*.⁴⁴ In this matter the defendant was a customer of the plaintiff bank who kept an investment account at the bank. Hanley alleged that he did not authorise a certain large transfer of money from his account. He alleged that the transfer was effected through a fraudulent document submitted by another customer of the bank. The bank raised as defence that the amount was transferred as a result of Hanley's negligence in allowing the other customer to come into possession of a transfer instruction document that Hanley had signed. However, the court of first instance held that the bank transferred the money from the Hanley's account, not because of Hanley's negligence in drafting the transfer instruction, but primarily because the bank failed to apply prudent and acceptable banking practices that would have enabled them to detect that the payment instruction was forged.⁴⁵ The bank appealed the matter but the judgment of the court a quo was upheld.⁴⁶

These two cases serve to reinforce the principle that generally the customer will bear the loss in the event of an unauthorised erroneous credit transfer unless the bank acted carelessly or negligently or without good faith.

⁴⁴ [2014] All SA 249 (SCA).

⁴⁵ At 254E.

⁴⁶ There were a number of factors that indicated that the bank was negligent: it did not phone the customer to confirm his signature, it made the payment on the basis of a fax and not an original form and it had opened a bank account for the other company without a company resolution authorising the opening of the account. It further held that the customer could not reasonably have foreseen that the amount on the second page of the instruction form would be altered. He also did not facilitate the alteration and wrote the words and figures with care. It was not his negligence but that of an employee of the bank that was the proximate cause of the loss as the employee did not notice that the payment instruction had been altered.

Chapter 3 Where the customer has instructed an erroneous credit transfer

3.1 Introduction

Often in practice it is the customer who is the party at fault that gave erroneous payment instructions to his bank to effect a credit transfer from his account. Very often the problem is that the customer makes a mistake regarding the beneficiary's account number or decides that he does not want to make payment to the beneficiary anymore. The question then arises whether, in such a situation where the customer is clearly at fault and the bank can generally not be blamed for the mistake, there is any remedy that can be invoked to prevent loss to the bank's customer. In particular the question arises whether it would be possible for the customer to instruct the bank to merely reverse the credit transfer and debit the customer's account with the amount transferred as a result of the customer's error? Can the consumer countermand or require the reversal of the payment effected by an erroneous credit transfer?

3.2 Countermand of payment

In terms of the common law of *mandatum*, a mandator is entitled to revoke a mandate at any time *before* its performance or completion.⁴⁷ In terms of the bank and customer agreement the bank is obliged to give effect to a countermand of payment of a cheque or of any other payment instruction.⁴⁸ Notably the Bills of Exchange Act provides rules for the countermand of cheques in terms whereof the bank must give effect to a countermand of the cheque by the customer if the countermand is timeously made before the cheque is paid out. If the bank still goes ahead and makes the transfer in spite of the countermand the bank will be liable for any subsequent loss as it then acted contrary to the client's (changed) mandate.

However since no legislation for electronic funds transfers exists that arrange this position the question arises whether it is at all possible for the customer to countermand a credit transfer once he realises that there is something wrong with the account number or simply because he decides he no longer wants to effect transfer of the money into the beneficiary's account, for whatever reason. However, as pointed

⁴⁷ *Ex parte Kelly* 1943 OPD 76. Schulze (2007(1)) 383.

⁴⁸ Van Heerden at 164.

out the speed with which credit transfers are effected may complicate matters when it comes to trying to countermand an erroneous credit transfer.

Schulze explains that in the case of an electronic funds transfer the time that it takes for delivery of the payment instruction depends on whether it is only a "bilateral transfer" between banks or whether it has to be routed through a clearing system before the transfer is transmitted to the recipient bank.⁴⁹ If it is a bilateral transfer, then delivery of the payment instruction and effecting of the credit transfer into the beneficiary's account is basically immediate.⁵⁰ However, if the payment instruction has to be "routed" through a clearing system, the clearing system causes a delay because the payment instructions have to be sorted first and then batched before they are sent forward.⁵¹ This delay may, in Schulze's opinion, then possibly allow the originator of the instruction to revoke or countermand the payment instruction.⁵²

The question is whether the beneficiary's account is also at the originator's bank or whether it is at a different bank may also influence the position regarding countermand. Malan, Pretorius and Du Toit indicate that in the case of an instruction to pay a customer at the same bank the notice of countermand must reach the bank *before payment* into the beneficiary's account.⁵³ In the case of an inter-bank transfer it is only possible to countermand a credit transfer *before* the beneficiary's bank *receives* the instruction.⁵⁴

However, in practice by the time that the customer realises that the credit transfer was erroneous the transfer would almost always already have been effected. In any event Meiring is of the opinion that countermand of a credit transfer, given the speed with which these transfers are effected is generally not possible and I agree with her. Maybe in the case of a written instruction to transfer a payment on a specified date only it will be possible for the customer to countermand the payment before the due date for transfer but in the case of credit transfers with bank cards or with internet banking for example, the transfer will basically go through immediately and the client

⁴⁹ Schulze *Commercial Law* 414; Comte 4, 21. The recipient bank, otherwise called the 'receiving bank', is the bank to whom the payment order is addressed and is not necessarily the beneficiary bank.

⁵⁰ Schulze *Commercial Law* 414.

⁵¹ Schulze *Commercial Law* 414.

⁵² Schulze *Commercial Law* 414. See also Meiring 41 .

⁵³ Malan, Pretorius & Du Toit 292.

⁵⁴ *Ibid.*

will not be able to countermand it timeously. This means that generally such a payment is final.

Also, Van Heerden points out that the bank–customer agreement usually contains provisions to the effect that once a payment instruction to effect an electronic funds transfer has been received from the customer and processed by the receiving bank it cannot be revoked; the customer will be bound by the agreement and will not be able to countermand the payment instruction. The bank can thus debit the customer's account with the amount paid.⁵⁵

One may then ask, if the credit transfer has been completed but it transpires that it was an erroneous transfer and the client mistakenly gave instructions for the transfer of gave wrong account details, and it was not possible to countermand the transfer timeously - would it then not be possible to just reverse the credit transfer?

3.3 Reversal of a credit transfer

The difficulty of reversing a credit transfer came to the fore in the matter of *Take & Save Trading CC v The Standard Bank of SA Ltd.*⁵⁶ In this case the customer tried to "countermand" a credit transfer that had already been effected by instructing its bank to 'reverse' electronic payments that were made to another party. The other party, was a creditor of the originator and apparently received the money as payment for a debt in respect of cigarettes that were bought. This party objected to the reversal because he said it was payment for the debt owing to him. Because of this objection the bank refused to comply with its customer's instruction to reverse the payment.⁵⁷ When the matter went to court the court made an obiter remark to the effect that the transfer was (a) final and (b) could only be reversed with the consent of the beneficiary.⁵⁸

What is also notable about the *Take & Save* is that in the court a quo an employee of the bank testified about a "confidential" inter-bank agreement under the auspices of the Automated Clearing Bureau. The employee indicated that this inter-bank agreement provided that unless the beneficiary gave his consent, an electronic funds

⁵⁵ Van Heerden 167.

⁵⁶ [2004] 1 All SA 597 (SCA).

⁵⁷ At 597D–E.

⁵⁸ At 594B.

transfer could not be reversed.⁵⁹ The appeal court made the following noteworthy obiter remark:⁶⁰

One may assume in the [customer's] favour that the instruction [to transfer money electronically] had been given. One may even assume in their favour that there is no inter-bank agreement preventing the reversal of electronic transfers. All that being assumed, how can a bank retransfer an amount transferred by A into the account of B back into the account of A without the concurrence of B? ... could not suggest any ground on which this can be done, there simply is none.

As pointed out by Van Heerden, this dictum thus implies that "a credit transfer, once effected, is final and cannot be reversed without the consent of the beneficiary."⁶¹

Schulze does not agree with this view. He is of the opinion that where the beneficiary was never entitled to receive the money in the first place, his consent should not be necessary before the transfer may be reversed.⁶² He remarks that because the inter-bank agreement is apparently confidential, the evidence presented in the *Take and Save*-case that the inter-bank agreements prohibit the reversal of an electronic funds transfer unless the beneficiary consents to it, must be accepted.⁶³ However, he is not convinced that this should govern all reversals of electronic funds transfers. Schulze points out that there are many instances where a reversal of a credit transfer without the consent of the beneficiary, would not only be fair but would also be in line with public policy. He gives the example of a transfer that was obtained by the beneficiary's fraudulent conduct.⁶⁴

In Schulze opinion there could be a number of valid reasons why a bank would be entitled to reverse a credit transfer unilaterally without the beneficiary's consent, such as:

- (a) in the case of "mistaken identity" (where the money was transferred to the wrong person);

⁵⁹ At 598.

⁶⁰ At 599.

⁶¹ Van Heerden 168.

⁶²Schulze (2004(1)) 677.

⁶³Schulze (2004(1)) 677.

⁶⁴Schulze (2004(1)) 677.

- (b) where the wrong amount was transferred;
- (c) where the correct amount was transferred to the correct person but it was transferred prematurely on the wrong date; or
- (d) where the correct amount was transferred to the correct person on the correct day but the bank was not entitled to effect the transfer.⁶⁵

3.4 Further developments in case law

In the various cases concerning Mr Pestana as discussed herein it should be noted that the payment instruction to effect a credit transfer on behalf of Mr Pestana was not unauthorised. Also Mr Pestana did not give an erroneous instruction for a credit transfer. It is however important to have regard to the Pestana-cases as they deal with the general question of whether a bank can just unilaterally decide to reverse a credit transfer. The Pestana cases thus by analogy informs the approach that the courts will tend to take in the case where a bank decides to "help" its client by quickly unilaterally reversing a credit transfer.

In *Nedbank v Pestana*,⁶⁶ the customer, Mr Pestana senior, conducted a current account at the Nedbank (who in this instance was both the originator bank and the beneficiary bank). Another client of the bank, Mr Pestana junior, instructed the bank to transfer funds from his account to the account of Mr Pestana senior. What the specific branch of the bank where the account was held did not know was that the receiver of Revenue had, a few hours before the credit transfer on behalf of Mr Pestana junior was made, instructed the Head Office of Nedbank to take a large amount from Mr Pestana Junior's account in terms of section 99 of the Income Tax Act for outstanding income tax. This instruction from the Receiver of Revenue was unfortunately only communicated to the branch after the branch had already effected the credit transfer from Mr Pestana junior's account into the account of Mr Pestana senior. The branch then decided to unilaterally reverse the payment made by means of the credit transfer into Mr Pestana senior's account without first asking Mr Pestana senior's consent to the reversal.

⁶⁵ For an example of such a set of facts see *Nedbank Ltd v Pestana* [2009] 2 All SA 58 (SCA).

⁶⁶ [2009] 2 All SA 58 (SCA). The facts in this matter were presented by way of a stated case.

The matter served before court a number of times. Eventually the Supreme Court of Appeal confirmed the decision by the full bench⁶⁷ that a completed and unconditional payment had been effected into Mr Pestana senior's account when the bank credited the account, hence (like was stated in the *Take & Save*-case) the bank could not unilaterally reverse the payment.⁶⁸

Schulze points out that *Pestana* was presented by way of a stated case and it contained no statement about whether the initial credit transfer instructed by Mr Pestana junior to Mr Pestana senior's account was a fraudulent instruction that was aimed at moving the money out of reach of the Receiver of Revenue. Thus the court could not make any ruling in that regard.⁶⁹ Schulze however emphasises that the court did state:⁷⁰

'It is well established that, in general, entries in a bank's books constitute *prima facie* evidence of the transactions so recorded. This does not mean, however, that in a particular case one is precluded from looking behind such entries to discover what the true state of affairs is.... [E]xamples of where a credit transfer may be validly reversed include cases where ... the client came by the money by way of fraud or theft.'

So from the *Pestana*-cases one can see that the court will be reluctant to allow a unilateral reversal of a credit transfer by a bank. Generally it will only allow such a reversal if the beneficiary consents thereto. One can also expect that a beneficiary will not easily give his consent if the payment relates to a debt that the bank's customer (the originator) owes to the beneficiary. This is because he will be receiving the money as payment for the debt owed to him - meaning that there is a valid reason for him to be receiving the money. However, where a thief or fraudster is receiving money erroneously transferred into his account by means of a credit transfer there is no legally valid basis on which he can claim to be entitled to such money. It seems that the court in *Pestana* recognised the unfairness that would follow if in such a case the thief or fraudster's consent first had to be obtained before the transfer could be reversed.

⁶⁷ *Pestana v Nedbank Ltd* 2008 (3) SA 466 (W), which followed upon the single-judge decision in *Pestana v Nedbank Ltd* [2006] ZAGPHC 113 (29 May 2009).

⁶⁸ Paragraphs 10–16.

⁶⁹ Schulze (2009) 400.

⁷⁰ Paragraph 17.

3.5 Developments in case law subsequent to *Pestana*

After the *Pestana*-cases the issue regarding reversal of a credit transfer served before the Supreme Court of Appeal again in.⁷¹ In this case an erroneous payment was made by means of a credit transfer from the customer's account. It was not clear exactly whose fault caused the error- i.e. whether it was the client or the bank who was at fault. In the *Nissan*-case the court distinguished the obiter statement in the *Take & Save*-case referred to above, on the basis that the *Take & Save*-case was concerned with a *valid* transfer of funds in payment of a debt. The court in the *Nissan*-case agreed that in such a situation the payment could not be reversed without the consent of the beneficiary who received the money (even, for example, if there was a dispute between the parties as to whether the money was indeed owing because the customer alleged that the beneficiary did not complete the work in terms of the contract that the money was paid for).⁷² However, the court stated that in the case where stolen money was paid into an account to the credit of a thief, the thief "had as little entitlement to the credit representing the money paid into the account as he would have had were actual notes and coins paid into the account." The court indicated that this also applies where money is merely erroneously transferred into the account of a person not entitled thereto.⁷³ In the aforementioned instances of fraudulent (and thus erroneous) or mere erroneous transfer, the court held that the credit transfer could be reversed without first having to obtain the consent of the beneficiary.⁷⁴ That this is the position was subsequently confirmed in *ABSA Bank Ltd v Lombard Insurance Co.*⁷⁵

The court in the *Nissan*-case however also made the following cautionary statement: "If a third party claims to be entitled to the money deposited with the bank, the bank need not investigate the matter but may adopt the stance of a stakeholder. It would be well advised to adopt such a stance. Should the bank in such an event unilaterally reverse the credit to the customer's account, it would be doing so at its peril."

⁷¹ 2005 (1) SA 441 (SCA).

⁷² Paragraph 23.

⁷³ The court indicated that this position applies not only where payment is made by cheque but also where payment is effected by cash or electronic funds transfer.

⁷⁴ See further Schulze (2004(1)) 683.

⁷⁵ 2012 (6) SA 569 (SCA).

Comte remarks that it is clear that the court made this cautionary statement to ensure that banks do not whimsically reverse credit transfers, mistaken or otherwise.⁷⁶ However it appears that in practice banks generally appear to take the stance advocated in practice with the result that in cases of erroneous credit transfers they generally tend to avoid getting involved and require the originator to seek legal recourse against the beneficiary. As a general rule a bank, that has not been the party who caused the error regarding the transfer but was merely acting on the originator's (apparent) instructions, will not unilaterally reverse a credit transfer on the mere allegation of the originator that the fraud or theft was involved and they generally require more concrete proof such as a court judgment in favour of the originator.

3.6 The problem revealed in the *Lombard Insurance*-case

Where the originator's bank has effected payment by means of a credit transfer without the necessary authorisation from its client absent negligence on the part of the client, the bank will not be able to rely on the common law or the bank–customer agreement for protection. This means the bank cannot debit the customer's account and will have to bear the loss that may result from such erroneous transfer. The bank may however, on the basis of unjustified enrichment of the person who was not validly entitled to the payment, seek to recover the money it paid from the beneficiary or the person who defrauded the bank. Where the bank has acted correctly according to the customer's mandate but the customer was to blame for the erroneous credit transfer, the position will be that the bank is absolved from liability and the customer will have to bear the loss. In such an instance the customer can also use the principle of unjustified enrichment to claim the money back from the beneficiary or other person who was enriched by the payment. However, as pointed out, payment by credit transfer serves to pay the underlying debt (if there is one) and this aspect has in some instances served to complicate recovery of funds that were erroneously transferred.

That the principle that a credit transfer may serve to extinguish a debt can be problematic for purposes of recovery of funds erroneously transferred clearly appears from the case of *ABSA Bank Ltd v Lombard Insurance Co Ltd*.⁷⁷ In this case an employee of Lombard Insurance fraudulently caused money belonging to a customer

⁷⁶ Comte at 42.

⁷⁷ 2012 (6) SA 569 (SCA). See also Pretorius (2013(3)) 589.

of Lombard Insurance to be transferred electronically into the employee's bank account. The money was thereupon transferred to various other accounts. One of these accounts was the employees overdrawn current account with ABSA. The transfer of the money into the overdrawn account had the effect of extinguishing the employee's overdraft and leaving the account with a considerable credit balance.⁷⁸ Lombard Insurance subsequently sought to recover the full amount credited to the employee's current account from the Absa. For this purpose it instituted an enrichment action based on the *condictio ob turpem vel iniustam causam*. It was contended that, following the *Nissan*-case, a development had taken place in our law in terms of which a bank that had credited a thief's account with the proceeds of stolen money is liable to the owner of the money for the full amount because the bank would be unjustly enriched given that it had no obligation to account for the money to its customer (the thief who had no enforceable claim against the bank).

The Supreme Court of Appeal however took a different view. The court indicated that the basis on which the bank could resist the claim for recovery of the moneys on the alleged grounds of unjustified enrichment, was the defence of *suum recipit*. In simple terms *suum recipit* means that the debtor suffers no loss by making the payment because although the recipient is enriched, such enrichment is justifiable. The reason why it is justifiable is because of the recipient's (in this case the bank who gave the overdraft) entitlement to the payment of the debt owed to it (i.e the overdrawn credit).⁷⁹

The court further softened the effect of this statement by indicating that in order to discharge a debt it must be paid in the name of the true debtor and that generally the discharge of a debt requires an agreement between the parties to that effect.⁸⁰ It also indicated that for payment by electronic means to be effective the payee must acquire the 'unfettered or unrestricted right to the immediate use of the funds in question'. According to the court this requires the parties to be in agreement as to the debt to be paid. Such debt-extinguishing agreement may be concluded expressly or tacitly by conduct.⁸¹

⁷⁸ At 571H–572I.

⁷⁹At 577E–578D.

⁸⁰ At 597A.

⁸¹At 579B.

The court stated that, in a case like that of *Lombard Insurance*, notification of the acceptance of an offer to enter into a debt-extinguishing agreement would be "impractical and superfluous" and that the acceptance was evidenced by the corresponding credit and its non-reversal.⁸² The court further held that a debt-extinguishing agreement may not be *contra bonos mores*. It also pointed out that such an agreement will be invalid where both parties knew that the debt would be discharged with stolen money. However, the court indicated that none of the cases referred to in its judgment suggest that the same result follows where the creditor is in good faith and unaware of the fact that the debt is to be discharged with stolen funds.⁸³

The court consequently stated as follows:

'[A]ny suggestion that the validity of the payment may be questioned for this reason would lead to a series of payment transactions being declared invalid *ex post facto* after discovery of the theft. Nor is it required that the law be developed any further. The common law has already imposed a duty of care on a collecting bank. Extensive legislation aimed at prevention of money laundering applies to banks. Any further development along the lines suggested ... which, to my mind is neither necessary nor desirable, should be by way of legislation'."

The court further indicated that payments made into the customer's account extinguish any debt on the account and that it made no difference that the payment in the *Lombard Insurance*-case was made by electronic transfer.⁸⁴

3.7 Final remarks

From the aforementioned discussion it is clear that erroneous credit transfers, whether they result due to a lack of authorisation by the customer or whether they have been effected as a result of an erroneous instruction by the customer himself, are problematic. The possibility that fraud be perpetrated relatively easily in the context of electronic credit transfers are not helped by the fact that these transfers are generally effected instantaneously thus leaving very little "response time" within which to try and

⁸²At 579C.

⁸³At 579D.

⁸⁴At 80D–E. The court stated that the legal effect of an electronic funds transfer is that no physical money changes hands but that the account holder obtains a claim against his bank for the credit against the account. Where the effect of the transfer is that there is no credit because the entire amount transferred was used to extinguish the debt on the account, the customer acquires no claim against his bank, but he is enriched to the extent that the debt is no longer due.

stop the transfer before it reaches the wrong account. Even despite the principles laid referred to obiter in the *Take & Save*-case and subsequently expressly confirmed in the *Nissan*-case it may still happen that banks rather take a neutral stance and refuse to reverse the credit transfer without a court order. Also, the *Lombard Insurance* –case demonstrates the difficulty that may follow should it happen that the money was paid into an overdrawn account that the thief or fraudster had with the beneficiary bank where the transferred is received.

Chapter Four Guidance from Australia

4.1 Introduction

Australia adopted a framework for dealing with electronic funds transfers in 1986 when they issued the Electronic Funds Transfer Code of Conduct which has been under regular review. This framework for dealing with electronic fund transfers is currently captured in the new Australian ePayments Code that came into effect on 29 March 2016. The Australian market conduct regulator, ASIC, is responsible for administering and reviewing the EPayments Code. The Code is a voluntary Code of practice to which banks, credit unions, building societies and other providers of electronic payment facilities in Australia subscribe. The Code inter alia sets out the rules for determining who pays for unauthorised transactions.⁸⁵

4.2 The ePayments Code

For purposes of the Code the following definitions are relevant:⁸⁶

- A “holder” means “an individual in whose name a facility has been established, or to whom a facility has been issued.”
- A “subscriber” means “an entity that subscribes to this Code” for example a bank.
- A “user” means “a holder or an individual who is authorised by a subscriber and a holder to perform transactions using a facility held by the holder.”

Important to note is that subscribers must warrant that they will comply with the Code in relation to the terms and conditions they impose on consumers. This means that compliance with the ePayments Code must be a term of the agreement entered into between the subscriber and the holder. Holders can complain about a breach of the Code and can first do so to the subscriber. If the holder is not satisfied with the outcome he can complain to an external dispute resolution scheme such as the Financial Services Ombudsman.⁸⁷ Chapter C of the Code provides rules for allocating the liability for losses from unauthorised transactions and system or equipment

⁸⁵ ePayments Code available at <https://www.asic.gov.au> (accessed on 29 December 2019) at 1 .

⁸⁶ Clause 2 of the ePayments Code.

⁸⁷ Ibid.

malfunction. Insofar as the application of the Chapter to unauthorised transactions is concerned its scope is limited by stating that it does not apply to any transaction that is performed by a user or by anyone who performs a transaction with the user's knowledge and consent.⁸⁸

4.3 When the holder is not liable

Clause 10.1 of the ePayments Code then deals with the situation where the holder (customer) is *not* liable for loss flowing from an unauthorised electronic payment transaction and *inter alia* lists the following instances:⁸⁹

- (a) fraud or negligence by a subscriber's (bank's) employee or agent;
- (b) a transaction that is incorrectly debited more than once to the same facility;
- (c) an unauthorized transaction performed after the subscriber (bank) has been informed that a device has been misused, lost or stolen, or where the security of a pass code has been breached.

A holder is also not liable for loss arising from an unauthorized transaction made by using an identifier without a pass code (PIN) or device (for example, a card). Where a transaction can be made using a device (card) but a pass code is not required, the customer will not be liable for loss. Where a transaction can occur using a device (card), or a device (card) and an identifier, but a pass code is not required, the holder is liable only if the user unreasonably delays reporting the loss or theft of the device.⁹⁰

A holder is also not liable for loss arising from an unauthorized transaction where it is clear that the user has not contributed to the loss.⁹¹

In a dispute about whether a user received a device (card) or pass code a presumption exists that the user did not receive the device (card) or pass code- unless the subscriber can prove that the user did receive it. In this scenario the subscriber can prove that the user received a device (card) or pass code by obtaining an acknowledgement from the user.⁹²

⁸⁸ Clause 9.1 of the ePayments Code.

⁸⁹ Clause 10 of the ePayments Code. Only those instances relevant to the topic of this dissertation are mentioned.

⁹⁰ Clause 10.2 of the ePayments Code.

⁹¹ Clause 10.3 of the ePayments Code.

⁹² Clause 10.4(a) and (b) of the ePayments Code.

Subscribers are not allowed to have any terms or conditions in their agreements with their customers to the effect that a card or PIN sent to a user at the user's correct mailing or electronic address is deemed to have actually been received by the user.⁹³

4.4 When the holder will be liable for loss

If clause 10 of the Code does not apply, a holder can be made liable for losses arising from unauthorized transaction only in the instances listed in clause 11 that comprise the following:

Where the bank can prove on a balance of probabilities that a user contributed to a loss through fraud, or as a result of breaching the pass code (PIN) requirements as set out in clause 12 of the Code; then:

(a) the holder is fully liable for actual losses that occur before the loss, theft or misuse of a device or breach of the pass code security is reported to the subscriber.

However, the holder is not liable for the portion of losses that are incurred on any one day that exceeds any applicable daily transaction limit. The holder is also not liable for the portion of losses that are incurred in any period that exceeds any applicable periodic transaction limit; or that exceeds the balance of the facility or that was incurred on any facility that the subscriber and holder had not agreed that it could be accessed using the device or identifier and/or the pass code used to perform the transaction.⁹⁴

Where more than one pass code is required to perform a transaction and a subscriber proves that a user breached the pass code security requirements in clause 12 of the Code in respect of one or more of the required pass codes but not in respect of all the required pass codes then the position is as follows: the holder will be liable under clause 11.2 only if the subscriber also proves on a balance of probability that, when assessed together with all the contributing causes, the breach of the pass code security requirements under clause 12 was mostly (more than 50%) responsible for the losses.⁹⁵

Clause 11.4 of the Code provides that the holder is liable for losses arising from unauthorized transactions that take place because a user contributed to such losses

⁹³ Clause 10.5 of the ePayments Code.

⁹⁴ Clause 1.2 of the ePayments Code.

⁹⁵ Clause 11.3(a) and (b) of the ePayments Code.

by leaving an ATM card in an ATM machine, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM.⁹⁶

Where a subscriber can prove, on a balance of probabilities, that the user contributed to the losses resulting from an unauthorized transaction by delaying to report the misuse, loss or theft of a device, or to report that the security of all pass codes has been breached the position is as follows:⁹⁷

(a) The holder is liable for the actual losses that occur between when the user became aware of the security compromise or should actually have become aware thereof in the case of a lost or stolen device, and such security compromise was reported to the subscriber.

(b) The holder will however not be liable for any portion of the losses incurred on any one day that exceeds any applicable daily transaction limit; or incurred in any period that exceeds any applicable periodic transaction limit; or that exceeds the balance of the facility, including any pre-arranged credit, or incurred on any facility that the subscriber and the holder had not agreed could be accessed using the device and/or pass code used to perform the transaction.⁹⁸

Clause 11.6 deals with the "effect of charges" and states that in deciding whether a user has unreasonably delayed reporting the misuse, loss or theft of a device, or a breach of pass code security, the effect of the charges imposed by the subscriber for making the report or for replacing a device or pass code must be taken into account.⁹⁹

Clause 11.7 deals with instances of limited liability. It provides that where a pass code was required to perform an unauthorized transaction, and clauses 11.2 to 11.6 does not apply, the holder is liable for the least of:

(a) 150 Australian Dollars, or a lower amount if determined by the subscriber;

⁹⁶ The Code contains a note after clause 11.4 which states: "Reasonable safety standards that mitigate the risk of a card being left in an ATM include ATM's that capture cards that are not removed after a reasonable time and ATM's that require a user to swipe and then remove a card in order to commence a transaction."

⁹⁷ Clause 11.5 of the ePayments Code.

⁹⁸ A note is included to clause 11.5 that states: "A holder may be liable under clause 11.5 if they were the user who contributed to the loss, or if a different user contributed to the loss."

⁹⁹ The note to clause 11.6 states: "For example, the reasonableness of a fee a subscriber charges for replacing a device must be taken into account."

(b) the balance of the facility or facilities agreed by the subscriber and holder to be accessed using the device and/or any pass code, including pre-arranged credit; or

(c) The actual loss at the time that the misuse, loss or theft of a device or breach of a pass code security is reported to the subscriber. (This is excluding those portions of losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.)

The Code also specifically deals with the burden of prove in the case of unauthorized electronic payment transactions. In this regard clause 11.8 provides that in deciding whether a subscriber has proved on a balance of probabilities that a user has contributed to losses under clause 11.2 and 11.5:

“(a) all reasonable evidence must be considered, including all reasonable explanations for the transactions occurring,

(b) the fact that a facility has been accessed with the correct device and/or pass code, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in clause 12, and

(c) the use or security of any information required to perform a transaction that is not required to be kept secret by users (for example the number and expiry date of a device) is not relevant to a user’s liability.”

4.5 Pass code (PIN) security requirements

The Australian ePayments code also contains some provisions on pass code (PIN) security requirements. In this regard clause 12 provides that the said clause applies where one or more pass codes are needed to perform a transaction. It states that a user must not:

(a) voluntarily disclose one or more pass codes to anyone. (This includes family members and friends.);

(b) where a device is also required to perform a transaction the user must not write or record pass codes on a device or keep record of the pass code on anything that is carried with the device or that may get stolen or lost together with the device, unless the user makes a reasonable attempt to protect the security of the pass code.

(c) where a device is required to perform a transaction, keep a written record of all pass codes required to perform transactions on one or more articles that may be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the pass code.

It is subsequently explained that a "reasonable attempt" to protect the security of the pass code entails making any reasonable attempt to disguise the pass code when it is recorded or by preventing access to the record of the pass code. This can inter alia be done by hiding or disguising the pass code record among other records; by hiding or disguising the pass code record in a place where it is not expected to be found or by keeping it in a securely locked container; or by preventing unauthorised access to an electronically stored record of the pass code.¹⁰⁰

Clause 12.4 further provides that a user must not act with extreme carelessness in failing to protect the security of all pass codes of his devices. In this context "extreme carelessness" refers to a degree of carelessness that "greatly exceeds what would be considered normal behavior."

A user must also not select a numeric pass code that represents their date of birth or an alphabetical pass code that is recognized as part of their name if the subscriber has specifically instructed the user not to do so and has warned the user of the consequences of doing so.¹⁰¹

In terms of clause 12.6 a subscriber is required to give the specific instruction and warning referred to in clause 5 at the time of selecting a pass code and in a way that is designed to focus the actual user's attention specifically on the instruction and consequences related to breach of the said instructions and warnings. This must be done whilst taking into account the actual user's capacity to understand the instruction and warning.

Clause 12.7 stipulates that the onus is on the subscriber to prove, on a balance of probability, that the subscriber indeed complied with clause 12.5. The Code further provides that where a subscriber expressly or implicitly promotes, endorses or

¹⁰⁰ Clause 12.3 (a) to (d). The note to clause 12.4 explains that: "An example of extreme carelessness is storing a user name and pass code for internet banking in a diary, Blackberry or computer that is not password protected under the heading 'internet banking codes'."

¹⁰¹ Clause 12.5.

authorises the sue of a service accessing a facility (such as by hosting an access service on the subscriber's electronic address, a user who discloses, records or stores a pas code that is required or recommended for the purpose of using the device, does not breach the security pass code requirements indicated in clause 12.¹⁰²

Clause 13 of the Code sets out various provisions relating to pass word security guidelines that a subscriber may give to a user to ensure the security of devices and pass codes. Clause 14 further deals with the situation where liability is caused by a system or equipment malfunction and clause 17 contains provisions detailing how to go about with reporting unauthorized transactions, loss and theft.

4.6 Conclusions and recommendations

It is clear that it is problematic that South Africa does not have legislation or at least a code, dedicated to governing electronic fund transfers and especially the liability of the parties for unauthorized or otherwise erroneous credit transfers. The result is that the banks tailor the bank customer agreement to apportion the greatest risk of loss to the customer and the customer bears the brunt of the liability for erroneous credit transfers. One would have thought that the Nissan-case would have made it easier for customers from whose accounts erroneous transfers were made due to theft or fraud to recover their monies but banks grasped at the cautionary statement made by the court in the Nissan-case to "justify" merely taking a neutral stance and not intervening to do a reversal of the problematic credit transfer. And if customers thought things may get better the *Lombard Insurance*-case lays another stone in their path by using the principle of *suum recipit* to justify refusal to allow the credit transfer and thus allowing the money transferred to be kept as payment to the bank by the thief in respect of his overdrawn account at his bank.

It is therefore submitted that South Africa is in urgent need of at least a code dealing with various aspects of electronic fund transfers. A code, although it is sift law, will be a good mechanism because it can be amended easily without the need for long parliamentary processes and as we know, electronic payments is a fast-changing area of the law. It is suggested that such a code could follow the example of the Australian

¹⁰² Clause 12.9 of the ePayments Code.

code and specify the instances in which the bank will be liable for losses and those where the customer will have to bear the loss for unauthorized or erroneous transfers. It can then also contain some guiding principles to help consumers to understand better how to take precautions to prevent fraud or the loss of their cards through theft. Most importantly though the code should be designed to achieve a fair outcome for consumer instead of just piling all the liability for losses onto them like the Code of Banking Practice currently does. The new code should also indicate that banks must not tailor the terms and conditions in the bank-customer agreement unfairly in their favour.

Bibliography

Books

- Sharrock (ed) *The Law of Banking and Payment in South Africa*
- Havenga (ed) *Commercial Law* (2014)
- Malan , Pretorius & Du Toit *Bills of Exchange , Cheques and Promissory Notes*(5th ed)
- Comte *Reversal of credit transfers* (LLM-dissertation UJ 2012)

Journal articles

- Pretorius 'Aspects of the collection of a cheque cleared through an Automated Clearing Bureau' (1998) 10 *SA Merc LJ* 326
- Pretorius 'Codeline clearing' (2001) 13 *SA Merc LJ* 260
- Schulze 'Countermanding an electronic funds transfer: The Supreme Court of Appeal takes a second bite at the cherry' (2004) 16 *SA Merc LJ* 668
- Schulze 'Electronic funds transfers and the bank's right to reverse a credit transfer: one small step for banking law, one huge leap for banks' (2007) 19 *SA Merc LJ* 379
- Schulze 'The sources of South African Banking Law - A Twenty-First Century Perspective (Part 11)' 2002 *SA Merc LJ* 601 621
- Schulze 'Duty of a Bank to Act with Necessary Skill and Care when Issuing an Automated Teller Machine Card' (2007) *De Jure* 371 372-377
- Schulze ' Depositum, Deposit and Deposit-taking Institutions – Birds of a Feather? Not Quite' (2001) 13 *SA Merc LJ* 78
- Visser 'The evolution of electronic payment systems' (1989) 1 *SA Merc LJ* 189

Cases

- *Absa Bank Ltd v Hanley* [2014] All SA 249
- *Absa Lt d v Lombard Insurance Co Ltd* 2012 (6) SA 569(SCA)
- *B&H Engineering v First National Bank of SA Ltd* 1995 (2) SA 279 (A) 293
- *Diners Club Ltd v Singh* 2004 (3) SA 630 (D)
- *Ex parte Kelly* 1943 OPD 76
- *Gilbeys Distillers and Vintners v ABSA Bank* unreported case no 12698/94 (C)

- *Pestana v Nedbank Ltd* 2008 (3) SA 466 (W)
- *Pestana v Nedbank Ltd* [2006] ZAGPHC 113 (29 May 2009)
- *Nedbank Ltd v Pestana* [2009] 2 All SA 58 (SCA)
- *Nissan South Africa (Pty) Ltd v Marnitz (Stand 186 Aeroport (Pty) Ltd Intervening)* 2005 (1) SA 471 (SCA)
- *Take & Save Trading CC v The Standard Bank of SA Ltd* 2004 (1) SA 597 (SCA)

Codes

- South African Code of Banking Practice (2012)
- Australian ePayments Code (2016)