UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The regulation of electronic payments in South Africa

By

Riana Heunis

(22212362)

Submitted in partial fulfilment of the requirements for the degree
Master of Laws (Mercantile Law)

In the Faculty of Law,
University of Pretoria

October 2021
Supervisor: Prof R Brits

Declaration

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

Riana Heunis
October 2021

Summary

This dissertation analyses the electronic payments industry in South Africa and identifies certain selected shortcomings in our law to regulate new innovations in the payment services market. It focuses on the rights and obligations of parties involved in different methods of electronic payments and analyses how the common law as well as legislation apply to these methods of payment. Consumer protection concerns are also highlighted, which are heightened by the lack of competition in the payment services industry.

International developments are explored in comparison to the South African regulatory model. The conclusion reached is that there is a need for legislation dedicated to the intricacies involved in electronic methods of payment and that new entrants in the market should be welcomed. In this regard, guidance should be taken from the European Union and the United States of America, where detailed directives or codes have been implemented to cater for electronic methods of payment.

Developments in South Africa, as well as abroad, for the regulation of crypto assets, a new innovation in the payment industry, are also explored. It is shown that, due to crypto assets not being utilized widely as a payment method, regulatory intervention is developing at a slow pace.

Acknowledgements

[to be added after the examination process is completed]

Table of contents

Chapter 1:
Introduction

Electronic payments strengthen the effectiveness and speed of payment and provide support to e-commerce, such that retail commerce can occur between remote parties and across borders.[1] The Covid-19 pandemic has furthermore resulted in an increased demand for payment methods that are contactless and that can accommodate online shopping platforms as consumers avoid public spaces.[2]

Whilst electronic payments have solved a number of problems associated with traditional methods of payment such as cash or cheques, they come with their own risks and create legal uncertainty. It is a case of the law not keeping up with the speed at which technology has evolved.

Payment law is multi-dimensional and consists of different components.[3] It involves the regulatory framework for the operation of a payment system, which manages and oversees the clearing and settlement systems between banks as well as the policy setting for the national payment system.[4] The latter subject falls largely outside the scope of this work. Payment transactions law concerns the legal relationship between all participants in an electronic payment transaction, while payment services law has to do with the regulation and licensing of payment service providers as well the rights and remedies of customers making use of such services.[5] The latter aspect also covers the wider contractual relationship between customers and payment service providers.[6]

This dissertation focuses on the latter two aspects of payment law specifically relating to electronic payments. It explores the most pertinent methods of making and receiving payments electronically and how the law in South Africa applies to these methods of payment from an end-user's perspective, that is, the payer and the payee.

---

[1] B Geva "Electronic payments: guide on legal and regulatory reforms and best practices for developing countries" (2020) *Articles & Book Chapters* 2796 viii, available at https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=3796&context=scholarly_works (accessed 27-09-2021) (hereafter Geva (2020)).
[2] Bank for International Settlements, Financial Stability Institute "Fintech and payments: regulating digital payment services and e-money (Jul 2021) 3, available at https://www.bis.org/fsi/publ/insights33.pdf (accessed 17-10-2021) (hereafter FSI Insights).
[3] Geva (2020) viii-ix.
[4] Geva (2020) ix.
[5] *Ibid*.
[6] *Ibid*.

It also highlights certain selected regulatory challenges and explores how other countries have addressed these problems. It concludes that a regulatory regime applicable to electronic payments must be developed in South Africa, preferably by implementing legislation dealing with the matter in detail.

Chapter 2:
Electronic payment methods

2.1 Introduction

In an electronic age, suppliers and consumers are not in each other's presence when trading and physical cash does not change hands.[7] An electronic payment takes place when a payment instruction enters the payment system through the internet or another telecommunications system.[8] Payment by electronic means can be done in various different ways, and technological advancements in the field have made the act of making and receiving payment quick and easy. The most pertinent methods of electronic payments will be highlighted and explored hereinbelow.

2.2 Payment methods

2.2.1 Electronic fund transfers

2.2.1.1 Definition and general nature

As can be deduced from the term "electronic fund transfer" (EFT), it involves the moving of funds, or economic value, by electronic means as opposed to physical delivery thereof.[9] It is a payment method, and not a payment instrument such as a cheque.[10] Such transfer takes place by the originator giving a mandate to the bank resulting in the originator as well as the beneficiary's bank balances being altered.[11] It is not a transfer of funds or property in the true sense of the word, in that no physical money changes hands,[12] but merely an adjustment of the bank balances of the parties involved.[13] Once the transfer is complete, the bank balances of the parties are altered and the money so transferred no longer has a separate identity as a result of

[7] S Cornelius "The legal nature of payment by credit card" (2003) *SA Merc LJ* 153 - 171 153 (hereafter Cornelius).
[8] Geva (2020) 11.
[9] WG Schulze "The reversal of electronic payments under South African law: possible guidance from recent developments in European Union law" (2020) *SA Merc LJ* 22 - 50 24 (hereafter Schulze (2020)).
[10] WG Schulze "Countermanding an electronic funds transfer: the Supreme Court of Appeal takes a second bite at the cherry" (2004) *SA Merc LJ* 667- 684 670 (hereafter Schulze 2004(1)).
[11] R Sharrock *The Law of Banking and Payment in South Africa* (2016) 273 (hereafter Sharrock).
[12] Schulze (2004(1)) 671.
[13] *Ibid.*

commixtio.[14] The transfer then settles the claim of the beneficiary and at the same time extinguishes the debt of the transferor.[15]

It is possible for the originator of an EFT and the beneficiary thereof to be the same person, for instance, where a person transfers funds between accounts held by that person with the same bank.[16] Transfers can also take place between accounts held by two different persons at the same branch of the bank, or different branches of the same bank.[17] Where the originator and the beneficiary have accounts with two different banks, both banks act in completing the transaction.[18] The bank of the person making the payment will pay the bank of the payee, who will then credit the payee's account with the amount of the transfer.[19] In contrast to payment by way of a cheque, an EFT is not a conditional payment method.[20]

EFTs can be used to effect debit or credit transfers.[21] A credit transfer takes place when the originator mandates his or her bank to debit his or her account with a specified amount and to credit the beneficiary's account with such amount. The beneficiary then has a personal right against his or her bank for the amount of the credit.[22] With a debit transfer, the consumer's account is credited with a certain amount in settlement of a debt, by agreement with the debtor.[23] The person who is owed therefore requests payment from the debtor's bank.[24]

EFT systems can be initiated by the consumer or by the bank.[25] The latter involves systems that facilitate settlements between banks.[26] EFTs activated by the consumer can be done by making use of various systems or products, and include an automated teller machine, a telephone or mobile phone, a point-of-sale facility, or internet banking.[27]

---

[14] WG Schulze "Electronic fund transfers and the bank's right to reverse a credit transfer; one small step for banking law, one huge leap for banks" (2007) *SA Merc LJ* 379 - 387 384.
[15] J Moorcroft and ML Vessio *Banking law and practice* (SI 19, Oct 2019) 20-2 (hereafter Moorcroft and Vessio).
[16] Schulze (2004(1)) 671.
[17] *Ibid*.
[18] *Ibid*.
[19] *Ibid*.
[20] *Ibid*.
[21] Sharrock 274.
[22] *Ibid.*
[23] Sharrock 275.
[24] Schulze (2020) 25.
[25] Sharrock 273.
[26] *Ibid*.
[27] Schulze (2020) 24.

2.2.1.2 Legal nature

Payment by way of an EFT is not regarded as legal tender.[28] An agreement must therefore be entered into between the parties involved in the transaction in terms of which the beneficiary agrees to accept payment by the originator's bank to settle the underlying obligation.[29] Such agreement can be expressly or tacitly entered into, but in modern times, it is said that such an agreement can possibly be inferred or implied as a trade usage.[30] Schulze is of the view that an EFT results in a novation of the original debt obligation, in light of the fact that a new agreement is entered into.[31] The possibility of an EFT constituting an assignment of the debt is also considered by Schulze.[32] He states that assignment takes place where an obligation is transferred from the debtor to a third party, with the creditor's consent.[33] In the context of an EFT, the originator's payment obligation will be assigned to the bank, who becomes the new debtor.[34]

An EFT is not a negotiable instrument, as it does not fit into the definition of a bill of exchange as set out in section 2 of the Bills of Exchange Act 34 of 1964.[35] It is therefore an absolute, and not a conditional form of payment.[36]

2.2.2 Debit and credit cards

2.2.2.1 Definition and general nature

There are many different types of payment cards utilised by retailers, banks and other financial institutions. Only the most pertinent of payment cards, namely, the debit and credit card, will be discussed herein.

The electronic funds transfer at point of sale (EFTPOS) system is normally engaged to effect payments with debit or credit cards.[37] By swiping the relevant card and entering a personal identification number (PIN), the bank is authorised to make

[28] Moorcroft and Vessio 20-2; Sharrock 273.
[29] Moorcroft and Vessio 20-2.
[30] *Ibid.*
[31] Schulze (2004(1)) 672.
[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid*.
[35] Schulze (2004(1)) 673.
[36] Schulze (2004(1)) 673-674.
[37] Sharrock 276.

the payment.[38] As with an EFT, by making use of the EFTPOS system, the customer provides his or her bank with a payment mandate by electronic means.

With a debit card, the customer's account is debited immediately with the amount of the payment, as if he or she had paid cash.[39] The customer must therefore have sufficient funds standing to his or her credit in order for the payment to be successful.[40]

Credit cards allow the holders thereof to buy on credit extended to them by the bank and to pay the outstanding balance in instalments.[41] It therefore also involves the granting of credit by the issuer of the credit card to the cardholder.[42]

A credit card can also be used to make payment over the internet.[43] By providing the relevant card's details to the supplier or retailer online, the cardholder issues the payment instruction electronically, and the supplier is authorised to provide details of the payment to the bank.[44]

Credit cards issued by banks or other financial institutions should be distinguished from store cards, which are issued by suppliers to their customers directly and which are referred to as bipartite credit cards.[45] Where a credit card is issued by the bank to its customer to make purchases from third party suppliers, it is referred to as tripartite credit cards as a result of the fact that a minimum of three parties are involved in the scheme.[46] This will be elaborated on in more detail *infra*.

2.2.2.2 Legal nature

As with an EFT, payment by way of a debit or credit card is not legal tender and is therefore done by agreement between the various parties involved. A tripartite credit card generally results in three contractual relationships being established.[47] The first is the contract between the cardholder, or the customer, and the card issuer, normally the bank, in terms of which the bank issues the card to the customer who may make use of the card to make purchases of goods and services up to a specified limit.[48] The

[38] *Ibid.*
[39] Moorcroft and Vessio 20-12.
[40] Cornelius 154-155.
[41] Sharrock 304; WG Schulze "Smart cards and e-money: new developments bring new problems" (2004) *SA Merc LJ* 703 - 715 709 (hereafter Schulze (2004(2)).
[42] *Ibid.*
[43] VA Lawack "Electronic innovations in the payment card industry" (1998) *SA Merc LJ* 233 - 239 233.
[44] 234.
[45] Sharrock 305; Cornelius 153.
[46] Cornelius 154.
[47] Sharrock 277.
[48] Sharrock 307.

bank may claim payment from the customer once the former has paid the supplier for such goods and services purchased.[49] This agreement is usually regulated by standard-form contracts,[50] which will provide for the circumstances under which a transaction can be reversed as well as liability for unauthorised payments.[51]

The second is the contract between the bank and the supplier of the goods or services, which provides that the supplier will accept payment from a customer who presents a credit card issued by the bank, who in turn agrees to pay for the goods or services.[52] This agreement normally provides that the bank may recover a certain percentage of the payment as fees.[53]

The third is the contract between the cardholder, or the customer, and the receiver of the payment or the supplier, which is the underlying contract for the sale of the goods or services.[54] This contract will provide for payment to the supplier for such goods or services by credit card as opposed to legal tender.[55] Moorcroft states that in this instance, the supplier's claim against the customer is ceded to the bank, who in turn recovers payment from the customer.[56] Therefore, in the event of a credit card being used to make payment for goods or services, the supplier of such goods or services agrees that its claim against the customer is ceded to the bank. The bank, in turn, does not acquire any obligations for the supply of such goods or services as a result of the cession.[57]

Cornelius opines that, in actual fact, these agreements are not separate bilateral agreements, and that parties involved in a credit card scheme enter into a "single multilateral contractual relationship".[58] Depending on the terms of the contracts between the bank, the customer and the supplier, the latter may be required, once a credit card is presented for payment, to release the cardholder or customer from his payment obligations and look to the bank for payment, which amounts to a novation of the customer's payment obligation.[59] In English law, payment by way of a credit card

[49] *Ibid*.
[50] Sharrock 277.
[51] *Ibid.*
[52] Sharrock 307.
[53] *Ibid.*
[54] *Ibid*.
[55] Moorcroft and Vessio 20-9.
[56] *Ibid*.
[57] *Ibid*.
[58] Cornelius 164.
[59] Moorcroft and Vessio 20-9.

results in an absolute discharge of the payment obligation unless the agreement provides otherwise.[60] In South Africa, there are no specific provisions that regulate the position and academic writers differ in their views, with some stating that payment by way of credit card is conditional, as with a cheque.[61] According to Cornelius,[62] delegation resulting in novation takes place when a credit card is presented for payment, and the supplier must claim his money from the bank, with the customer being discharged completely.[63]

Moorcroft suggests that, in the event of one of two conditions being fulfilled, the cardholder's payment obligations are discharged when payment is effected by way of a credit card.[64] The first and most obvious is when the bank pays the supplier for the goods or services bought from the supplier by making use of his or her credit card.[65] The second is that, when the amount due to the supplier in terms of the latter's agreement with the bank is paid by the customer to the bank, the customer's debt is discharged and he will not be required to pay a second time.[66] Roestoff,[67] agreeing with Cornelius, states that the position under English law is sound, in that payment by credit card results in novation of the payment obligation and therefore discharges the debt, with the bank becoming liable for the payment.[68] This is, however, subject thereto that all the legal and contractual terms for payment by way of a credit card, are complied with.[69]

A distinction must however be drawn between on- and offline transactions. Where payments are made online, the electronic transfer is made immediately and directly from the cardholder's account to that of the supplier.[70] With an offline transaction however, the transaction is stored and processed at a later stage,[71] which complicates matters. The supplier is unable to ascertain whether the cardholder has adequate funds to settle the supplier's claim.[72] In terms of the supplier's agreement

[60] Sharrock 308.
[61] *Ibid*.
[62] Cornelius 163.
[63] Cornelius 171.
[64] Moorcroft and Vessio 20-9.
[65] *Ibid*.
[66] *Ibid*.
[67] Sharrock 308-309.
[68] Sharrock 309.
[69] Cornelius 171.
[70] Sharrock 277.
[71] *Ibid*.
[72] *Ibid*.

with the bank, the former will have authorisation to accept payments up to a certain amount, whereafter he will have to obtain authorisation from the bank.[73] It is said that an offline payment by using the EFTPOS system will not be a novation of the cardholder's payment obligations.[74] Therefore, if the supplier does not receive payment from the bank, it may claim from the cardholder.[75] Where such a transaction is effected offline, it has been suggested that it constitutes the granting of credit to the customer.[76] This may be determined by looking at the parties' intentions.[77]

2.2.3 Electronic money

Electronic money, or e-money, has been defined as "monetary value represented by a claim on the issuer", "stored electronically and issued on receipt of funds, is generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand".[78] Examples include electronic purses, digital cash and mobile money.[79] An electronic purse is defined in the South African Code of Banking Practice[80] and provides that it is "[a]ny card or function of a card into which money is prepaid and which can be used for a range of purposes. Some purses may also have an 'e-cash' facility for small value transactions, which are not recorded on an audit trail".[81] The electronic purse utilises smart card technology, whereby a microchip, which can store and process information, is implanted on the card.[82] Money or credit is loaded onto the card and can be utilised by the holder to make payments until the funds are finished, whereafter it can be recharged.[83]

Similar to EFTs and card payments, electronic money does not qualify as legal tender and will only be accepted as payment by agreement between the parties.[84]

---

[73] *Ibid*.
[74] Sharrock 278.
[75] *Ibid*.
[76] *Ibid*.
[77] *Ibid*.
[78] The South African Reserve Bank *Position Paper on Electronic Money* (Nov 2009), available at https://www.resbank.co.za/content/dam/sarb/what-we-do/financial-surveillance/general-public/PP2009_01.pdf (accessed 08-08-2021) (hereafter *Position Paper* (2009)).
[79] Sharrock 280.
[80] The Banking Association of South Africa *Code of Banking Practice* (Jan 2012), available at https://www.banking.org.za/code-of-banking-practice/ (accessed 08-08-2021) (hereafter "the Code").
[81] Cl 12 of the Code.
[82] Sharrock 278 & 280; Schulze (2004(2)) 708.
[83] Sharrock 280-281; Schulze (2004(2)) 708.
[84] Sharrock 281.

Depending on the terms of the agreement and the parties' intentions, payment by way of e-money can discharge the cardholder's payment obligation absolutely or conditionally.[85] Electronic money is denominated in fiat currency and is merely another method used to transfer funds electronically.[86]

In South Africa, the issuing of e-money is restricted to registered banks.[87] This is due to the fact that the acceptance of cash in return for issuing e-money may be seen as taking a deposit, which activity is reserved for registered banks.[88] It is however noteworthy that this is not the case in Europe. In terms of the E-money Directive 2009/110/EC[89] of the European Union, the issuing of e-money does not amount to a deposit-taking activity.[90] The licensing and prudential requirements applicable to registered banks will accordingly not apply to issuers of e-money.[91]

2.2.4 Virtual currencies

A further, fairly recent development in the sphere of payment methods, is that of virtual currencies. A virtual currency is a "digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and /or a store of value, but does not have legal tender status".[92] Virtual currencies can take many different forms. The focus of this work will be on virtual currencies that are convertible into real or fiat currency and which are decentralised, in other words, that are not subject to any central administering authority.[93] A further subcategory of virtual currencies are cryptocurrencies, which refer to their use of cryptography for security purposes.[94]

---

[85] *Ibid.*
[86] Financial Action Task Force *Virtual currencies key definitions and potential AML/CFT risks* (June 2004) 4, available at https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed 09-08-2021) (hereafter FATF report).
[87] *Position paper* (2009) 7.
[88] FSI Insights 14.
[89] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN (accessed 26-10-2021) (hereafter E-money Directive).
[90] Article 13 of the E-money Directive.
[91] For a detailed discussion on the regulation of the issuers of e-money in the European Union, see MD Tuba "The regulation of electronic money institutions in the SADC region: some lessons from the EU" (2014(17)6) *PELJ* 2269-2312.
[92] The South African Reserve Bank *Position paper on virtual currencies* (2014) 2, available at https://www.resbank.co.za/content/dam/sarb/what-we-do/financial-surveillance/general-public/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf (accessed 09-08-2021) (hereafter *Position paper* (2014)).
[93] For a full explanation of the different categories of virtual currencies, see FATF report 4-5.
[94] FATF report 5.

Different terms have been ascribed to this phenomenon, including digital currencies, cryptocurrencies and crypto assets.[95] The Intergovernmental Fintech Working Group[96] has adopted the term "crypto assets" to serve as an umbrella term, capturing all its functions, and which they define as "a digital representation of value that is not issued by a central bank, but is capable of being traded, transferred or stored electronically by natural and legal persons for the purpose of payment, investment and other forms of utility; applies cryptographic techniques and uses distributed ledger technology".[97] To provide for uniformity, the term crypto assets will be used throughout this work.

As can be deduced from the above definition, crypto assets do not qualify as money, as it is not issued by the central bank and is therefore not legal tender.[98] It is also clear from the definition of electronic money as alluded to *supra*, that crypto assets do not fall into this category. It is therefore completely new and unique.

The use of crypto assets as a payment method without the intervention of a third party, such as a bank, seems to have been the initial idea behind this innovation.[99] It allows parties to make payments for goods or services directly without the involvement of an intermediary such as the bank. Acceptance of crypto assets is at the discretion of the supplier of such goods or services.[100] According to the Crypto Assets Regulatory Working Group, the acceptance of crypto assets as payment for goods or services is not too common, but there are certain physical and online stores that do accept them.[101] According to the report, it is a method of payment often used for cross-border transfers due to its digital and borderless nature.[102]

---

[95] E Reddy & V Lawack "An overview of the regulatory developments in South Africa regarding the use of cryptocurrencies" (2019) *SA Merc LJ* 1 - 28 2 (hereafter Reddy & Lawack).
[96] A joint initiative formed in 2016 comprising of members from the National Treasury, the South African Reserve Bank, the Financial Sector Conduct Authority and the Financial Intelligence Centre. The National Credit Regulator and the South African Revenue Service joined in 2019, and the Competition Commission in 2020. In 2018, the Crypto Assets Regulatory Working Group was established from this initiative. See Intergovernmental Fintech Working Group, Crypto Assets Regulatory Working Group *Position paper on crypto assets* (June 2021), available at http://www.treasury.gov.za/comm_media/press/2021/IFWG_CAR%20WG_Position%20paper%20on%20crypto%20assets_Final.pdf (accessed 09-08-2021) (hereafter IFWG, CAR WG *Position paper* (2021)).
[97] IFWG, CAR WG *Position paper* (2021) 16.
[98] FATF report 4.
[99] IFWG, CAR WG *Position paper* (2021) 17.
[100] 18.
[101] *Ibid.*
[102] *Ibid.*

2.3 Conclusion

It can be deduced from the above discussion that the many different methods available to effect payment electronically are complex and that many different branches of the law find application. This will be explored in the next chapter.

Chapter 3:
The law as it applies to electronic payment methods

3.1 Introduction

In South Africa, there is no legislation that specifically regulates electronic payments.[103] Certain parts of legislation do find application, but the legal effects of these payment methods are mostly determined by the common law and specifically the law of contract.[104] This chapter sets out the manner in which the law applies to electronic payment methods.

3.2 Common law principles

As stated previously,[105] payment by way of an electronic payment method is done by agreement between the parties involved in the transaction. The legal consequences of the transaction are therefore determined by the express and/or implied terms of the agreement.

Separate from this payment agreement is the bank-customer relationship, which is contractual.[106] The same can be said for the relationship between a payment service provider, such as the issuer of e-money or a crypto asset service provider, and its customer.[107] Standard form contracts between banks and their customers will, for the most part, provide for the rights and obligations of the parties involved in electronic payment transactions.[108]

Whilst electronic payment methods have advanced significantly, the principles governing the bank-customer relationship have remained unaltered.[109] The contract between a bank and its customer can take various different forms,[110] and in the context

[103] WG Schulze "E-money and electronic fund transfers. A shortlist of some of the unresolved issues" (2004) *SA Merc LJ* 50 - 66 57 (hereafter Schulze (2004(3)); WG Schulze "Of credit cards, unauthorised withdrawals and fraudulent credit card users" (2005) *SA Merc LJ* 202-213 210 (hereafter Schulze (2005)); Schulze (2020) 24.
[104] Schulze (2020) 24-25.
[105] See Chapter 2.
[106] *Standard Bank of SA Ltd v Oneanate Investments (Pty) Ltd* 1995 (4) SA 510 (C) 530G*; Strydom NO v ABSA Bank Bpk* 2001 (3) SA 185 (T) 192H; *DA Ungaro & Sons (Pty) Ltd v ABSA Bank Ltd* [2015] 4 All SA 783 (GJ) 796 paras 25 - 26; Moorcroft and Vessio 15-1.
[107] Schulze (2004(3)) 58-59.
[108] Schulze (2020) 30; Sharrock 305.
[109] Schulze (2020) 24.
[110] Sharrock 115.

of electronic payment services, it is generally one of mandate.[111] As explained *supra*,[112] an EFT transaction can involve different branches of the same bank or two different banks altogether. The bank of the person originating the transfer will act as mandatary and the originator as mandator. Schulze states in this regard that, where a bank provides electronic payment services which, it is submitted, include EFT, e-money and payment card services, the rights and obligations of the bank and its customer will be determined by the contract of mandate.[113]

A contract of mandate imposes certain duties on the mandatary, including the duty to carry out its mandate with reasonable care, skill and diligence,[114] and not to act outside of its terms.[115] If the bank acts without the necessary mandate from its client, for instance, where the payment instruction is forged or unauthorised, it would be in breach of its contract with that client.[116] Unlike payment by way of a cheque, the person who gives a payment instruction by electronic means is not identified by his or her signature.[117] Therefore, an unauthorised payment instruction can easily occur. In this regard, it is said that strict liability should not be imposed on the bank, but that its liability should rather be based on negligence, and further that the client should also have the responsibility of preventing unauthorised payments.[118] To this end, the client has the common law duty to take reasonable care when giving a payment mandate to the bank, to prevent fraud and to ensure that the mandate is drafted in clear terms.[119]

Closely linked to the mandatary's duty to act strictly within the terms of its mandate, is its duty to act with reasonable care and skill.[120] A mandatary can be held liable for loss suffered by the mandator due to the former's negligent failure to do so.[121] Where the specific mandate requires specialised skills or expertise, the mandatary will be negligent if the mandate was accepted whilst the mandatary did not possess the necessary skills to perform the mandate.[122] Schulze argues that a bank should

---

[111] Schulze (2004(3)) 59; 62; Moorcroft and Vessio 15-5.
[112] See paragraph 2.2.1.1
[113] Schulze (2005) 211.
[114] Schulze (2004(3)) 62-63; Sharrock 282; DH Van Zyl "Mandate" in *LAWSA* vol 28 3ed part 1 45 (hereafter *LAWSA* "Mandate").
[115] Sharrock 282-283; *LAWSA* "Mandate" 42.
[116] Schulze (2004(3)) 60.
[117] Sharrock 283.
[118] *Ibid.*
[119] Sharrock 372 - 373.
[120] *Op cit* note 114.
[121] *LAWSA* "Mandate" 45.
[122] 45-46.

generally not be found to have acted negligently if it complied with established banking practices.[123] He states that banking practices can be implied in a contract between a bank and its customer, provided that such practices comply with the requirements for a trade usage.[124]

The beneficiary of an electronic payment, where such beneficiary is with a different bank to that of the originator, does not stand in a contractual relationship with the originator's bank.[125] Therefore, the originator's bank has no duty of care towards the beneficiary, either contractually or of a kind which, if breached, could lead to delictual liability.[126] There is, similarly, also no contractual relationship between the beneficiary's bank and the originator.[127] The question of whether the beneficiary's bank owes a duty of care to the originator which, if breached, could result in delictual liability, is an open one.[128]

3.3 Legislation

3.3.1 The Electronic Communications and Transactions Act

The Electronic Communications and Transactions Act 25 of 2002 (ECT Act) states in its preamble that it provides "for the facilitation and regulation of electronic communications and transactions". The ECT Act applies to all electronic transactions and data messages,[129] which include electronic transactions for financial services.[130] A "transaction" is defined as one of "either a commercial or non-commercial nature, and includes the provision of information and e-government services".[131] When regard is had to the definitions of "data" and "data message"[132] respectively, it is clear that it refers to any kind of an electronic representation of information which is sent, stored or received electronically. The ECT Act therefore has general application to any transaction where an electronic transmission of information is involved. Roestoff states

[123] Schulze (2004(3)) 63.
[124] 63-64.
[125] Sharrock 284.
[126] 284-285.
[127] 285.
[128] 285-286.
[129] S 4(1) of the ECT Act.
[130] Schulze (2004(3)) 57; Sharrock 296 with reference to S 42 of the ECT Act.
[131] S 1 of the ECT Act.
[132] *Ibid.*

that a credit card payment is an electronic transaction and therefore the ECT Act will apply to this method of payment.[133]

The ECT Act further makes reference to an "automated transaction", which is a transaction where data messages are used, either wholly or partially, to carry out a transaction, and the data messages or conduct of the parties to the transaction are not reviewed by a natural person in the normal course of his or her business or employment.[134] An "electronic agent" is involved in such an automated transaction, which is defined as a computer programme or any other electronic mode which functions automatically, and which can respond to a data message to initiate an action.[135] From these definitions, it can be said that an electronic payment is an automated transaction, as the platform used to make the payment functions automatically after being initiated by an electronic payment instruction. Section 20 of the ECT Act sets out the provisions pertaining to automated transactions and the formation of agreements by using electronic agents.

Consumer protection provisions are contained in Chapter VII of the ECT Act. A reading of the chapter reveals that it is primarily aimed at consumers who buy goods or services by way of electronic transactions.[136] The duties of suppliers who offer goods or services online are provided for, as well as consumers' rights to cancel transactions in the event of non-compliance by suppliers.[137] Roestoff[138] states that bank clients may enjoy protection from fraud in an EFT transaction in terms of section 43(5) and (6) of the ECT Act. These sections provide that a supplier is obliged to engage secure payment systems which are up to an acceptable technological standard and that failure to do so may render the supplier liable for damage suffered by the consumer. She states that this would be subject to a bank qualifying as a supplier in terms of the ECT Act, as the term "supplier" is not defined. The term "payment system" is also not defined, and the extent to which section 43(5) of the ECT Act applies to online EFT payments to a third party, as opposed to a supplier of goods or services, is therefore unclear.[139]

---

[133] Sharrock 305.
[134] S 1 of the ECT Act.
[135] *Ibid.*
[136] Sharrock 298.
[137] S 43(1) - (4) of the ECT Act.
[138] Sharrock 298.
[139] *Ibid.*

The ECT Act does not contain any provisions that deal exclusively with electronic payment methods, but applies generally to electronic banking transactions.[140] Schulze is of the view that there are many aspects pertaining to electronic payment methods not dealt with by the ECT Act, and that further developments in the field will reveal even more shortcomings in this piece of legislation as a tool to regulate electronic banking.[141]

3.3.2 The Financial Sector Regulation Act

Financial regulation in South Africa falls under the Financial Sector Regulation Act 9 of 2017 (FSR Act). In terms of the FSR Act, two main regulators were established, namely, the Prudential Authority and the Financial Sector Conduct Authority.[142] The Prudential Authority has as its objective the promotion and maintenance of safe and sound financial institutions that provide financial products and securities services, and to protect financial customers from the risk of those institutions not being able to meet their obligations.[143] In order to achieve this, the Prudential Authority must supervise financial institutions.[144] The Financial Sector Conduct Authority is tasked with enhancing and supporting the integrity and efficiency of financial markets, and to protect financial customers by promoting fair treatment and financial literacy.[145] To this end, it must supervise the conduct of financial institutions.[146] Both of these regulatory bodies are required to assist the South African Reserve Bank in maintaining financial stability.[147]

The FSR Act therefore has the overall function of regulating and supervising financial institutions, which include electronic payment service providers. It does however not provide for the intricacies involved in electronic payment transactions.[148]

[140] Sharrock 299.
[141] Schulze (2004(3)) 57.
[142] S 32(1) & S 56(1) of the FSR Act.
[143] S 33 of the FSR Act.
[144] S34(1)(a)(i) of the FSR Act.
[145] S57(a) & (b) of the FSR Act.
[146] S58(1)(a) of the FSR Act.
[147] S33(d) & S57(c) of the FSR Act.
[148] Schulze (2020) 28.

3.3.3 The National Credit Act

The South African credit market is regulated by the National Credit Act 34 of 2005 (NCA). Since a credit card scheme involves the granting of credit to the cardholder,[149] the NCA applies to the agreement. A credit card transaction falls under the definition of a credit facility as defined in the NCA,[150] and therefore qualifies as a credit agreement to which the provisions of the NCA will apply.[151] It should be noted that the NCA will only apply to a credit card transaction where the consumer, that is, the party who receives credit in terms of the credit facility[152] (therefore, the cardholder) is a natural person or a juristic person with an asset value or annual turnover of less than R1 million.[153]

The provisions of the NCA regulate, *inter alia*, maximum interest rates, fees and charges.[154] It requires pre-agreement assessments to be conducted prior to a credit agreement being entered into[155] and contains provisions in terms of which an agreement can be declared reckless.[156] Debt review[157] as well as debt enforcement provisions are also provided for in the NCA.[158]

Of relevance for purposes of this work is the provisions of section 94 of the NCA, which provides that, where a credit facility is accessed by using a card, the agreement in terms of which the credit facility was granted must set out a contact number where the loss or theft of the card can be reported.[159] The credit provider is prohibited from holding the consumer liable for a credit card transaction concluded after such loss or theft has been reported, unless it can be shown that the consumer approved the transaction.[160]

3.3.4 The Consumer Protection Act

As can be deduced from its title, the Consumer Protection Act 68 of 2008 (CPA) is aimed at the protection of consumers. A consumer is defined in the CPA as, *inter alia*,

---

[149] See par. 2.2.2.1 *supra*.
[150] JW Scholtz *Guide to the National Credit Act* (SI 13, Jul 2021) par. 8.2.2.
[151] S8(1)(a) of the NCA.
[152] See the definition of "consumer" in S1 of the NCA.
[153] S4(1)(a)(i) read with S7(1) of the NCA and GN 713 in GG 28893 of 1 June 2006.
[154] S105 of the NCA.
[155] S81(2) of the NCA.
[156] S80 of the NCA.
[157] S86 of the NCA.
[158] Chapter 6, Part C of the NCA.
[159] S94(1) of the NCA.
[160] S94(2) of the NCA.

"a person who has entered into a transaction with a supplier in the ordinary course of the supplier's business" and "if the context so requires or permits, a user of those particular goods or a recipient or beneficiary of those particular services, irrespective of whether that user, recipient or beneficiary was a party to a transaction concerning the supply of those particular goods or services".[161] Transactions where the consumer is a juristic person with an asset value or annual turnover which, at the time of the transaction, is equal to or exceeds R2 million, are exempted from the CPA's field of application.[162] Banking or related financial services are included in the definition of "service" and the provisions of the CPA will therefore apply to electronic payment services where the consumer is a natural person or a smaller juristic person.

Roestoff submits that the CPA can be utilised by banking customers to protect them against unfair contract terms imposed by banks.[163] Further rights of consumers in terms of the CPA include the right to receive, or to be given access to, the terms and conditions of the agreement entered into,[164] and that agreements must be in plain and understandable language.[165]

Similar to the other pieces of legislation previously referred to, the CPA has general application to electronic payment methods in certain circumstances, but does not deal with the matter in any detail.

3.4 Soft law: The South African Code of Banking Practice

Banks that are members of the Banking Association of South Africa (which are all the registered banks in South Africa)[166] have to adhere to the Code of Banking Practice ("the Code").[167] The Code can be described as a set of rules or principles applicable to products or services that banks offer to their clients.[168] It is only applicable to personal and small business customers.[169] A personal customer is defined in the Code as "[a]ny individual, who maintains an account or who receives other services from a

[161] S1 of the CPA.
[162] S5(2)(b) read with the Schedule in GN 294 in *GG* 34181 of 1 April 2011.
[163] Sharrock 299 with reference to S48-52 of the CPA.
[164] S50(2) of the CPA.
[165] S22 of the CPA.
[166] Moorcroft and Vessio 13-1.
[167] Ombudsman for Banking Services Terms of Reference (Feb 2018) par 2.1(c) read with definition of "member bank" in par 30.1, available at: https://www.obssa.co.za/publications/terms-of-reference/ (accessed 28-10-2021).
[168] Cl 1 of the Code.
[169] Cl 1 of the Code.

bank".[170] A small business is "[a]n association of natural or legal persons incorporated in or outside the Republic of South Africa, which has legal personality or enjoys a similar status in terms of which it may enter into contractual relations and legal proceedings in its own name and whose turnover for the last financial year was less than R5 million".[171]

The Code covers aspects relating to electronic payment services rendered by banks. It includes provisions in terms of which bank customers are required to take reasonable care when utilising electronic payment methods as well as provisions pertaining to banks' responsibility for losses.[172]

In terms of the Code, banks undertake to ensure that their systems are secure and reviewed regularly.[173] It also stipulates that banks will provide their clients with information on procedures to be followed in the event of unauthorised or fraudulent transactions[174] and measures to be followed to prevent a security breach.[175]

The enforceability of the provisions of the Code on banks and their customers is a debatable issue and is yet to be tested in our courts. However, it has been argued that its terms can be implied into the bank-customer agreement as a trade usage.[176] The common law principles of the law of contract will therefore apply in this regard.

3.5 What to do with crypto assets

As previously stated, crypto assets do not qualify as legal tender[177] and therefore, laws applicable to the regulation of legal tender do not apply.[178] It is submitted that the agreement between the parties involved in payment transactions by making use of crypto assets will determine their rights and obligations.

With regard to the applicability of existing laws in South Africa to crypto assets, recent developments towards formulating a regulatory framework for the regulation of crypto assets need mentioning. The Intergovernmental Fintech Working Group, through the Crypto Assets Regulatory Working Group, released a position paper on

[170] Cl 12 of the Code.
[171] *Ibid.*
[172] Cl 7.6 - 7.8 of the Code.
[173] Cl 9.3 of the Code.
[174] Cl 9.3.4 of the Code.
[175] Cl 9.3.6 - 9.3.14.
[176] SF Du Toit "Reflections on the South African code of banking practice" 2014 *TSAR* 568-579 570; Moorcroft and Vessio 13-7.
[177] Paragraph 2.2.4.
[178] Reddy & Lawack 18.

crypto assets on 16 April 2020,[179] which followed on the group's consultation paper on policy proposals for crypto assets which was issued in 2019 and which provided an overview of the perceived risks and benefits of crypto assets and a discussion of the available regulatory approaches.[180]

The position paper makes a total of thirty recommendations by focusing on the risks that each crypto asset use case poses. The idea is to accommodate crypto assets within existing regulatory frameworks by making suitable amendments to legislation. The aim is to regulate those entities that provide crypto asset related services instead of regulating the specific crypto asset itself which is not possible due its borderless and anonymous nature. The proposal is for these entities to become accountable institutions as contemplated in the Financial Intelligence Centre Act 38 of 2001 which will make the provisions of the Act applicable to crypto asset service providers.[181]

It is further proposed that crypto asset related services be included in the definition of "financial services" as contemplated in section 3(1)(a) of the FSR Act.[182]This will allow crypto asset service providers to fall under the umbrella of the twin peaks model of financial regulation, where the prudential and market conduct regulation of crypto asset service providers will be undertaken by the Prudential Authority and the Financial Sector Conduct Authority respectively.[183] It is proposed that the Financial Sector Conduct Authority be responsible "for the licensing of 'services related to the buying and selling of crypto assets'",[184] as these services will become a licensing activity under the Conduct of Financial Institutions Bill (CoFI Bill) once it is enacted.[185] The Prudential Authority must consider "the appropriate supervisory and regulatory approach for the treatment of crypto assets, including the reporting on prudential entities' direct exposures to crypto assets and the treatment of

[179] Intergovernmental Fintech Working Group, Crypto Assets Regulatory Working Group *Position paper on crypto assets* (Apr 2020), available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf (accessed 29-09-2021) (hereafter IFWG, CAR WG *Position paper* (2020)).
[180] IFWG, CAR WG "Consultation paper on policy proposals for crypto assets" (2019), available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf (accessed 12-05-2020).
[181] IFWG, CAR WG *Position paper* (2020) 25.
[182] 27; 31.
[183] See paragraph 3.3.2.
[184] IFWG, CAR WG *Position paper* (2020) 28.
[185] 27.

the prudential and accounting practices for crypto assets".[186] In doing this, they must take guidance from the Basel Committee on Banking Supervision.[187]

It is furthermore stated that the National Payment System Act 78 of 1998 is being reviewed and it is recommended that an enabling provision for the regulation of crypto asset related payment services be included.[188]

On 11 June 2021, the Crypto Assets Regulatory Working Group released a further revised position paper on crypto assets,[189] in terms of which it is confirmed that the implementation of some of its previous recommendations have already commenced.[190] The position paper reiterates that crypto assets can no longer remain unregulated and provides a roadmap for implementing its recommendations.[191] Apart from the recommendations in the previous position paper, it is also recommended that, as a temporary measure until the CoFI is enacted, the Financial Sector Conduct Authority should declare crypto assets as a financial product for purposes of the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS Act) so as to provide for a legal framework within which crypto asset related advisory and intermediary services can be regulated.[192]

3.6 Conclusion

From the above discussion it is clear that many of the rights and obligations of parties involved in electronic payment methods are left up to the parties themselves to regulate in terms of their agreements. Common law duties are applicable, but will in certain instances have to be interpreted and there are no clear rules and regulations. Regulatory problems posed by electronic payments are traversed in the chapter to follow.

---

[186] *Ibid*.
[187] 54.
[188] 29.
[189] IFWG CAR WG *Position paper* (2021).
[190] IFWG CAR WG *Position paper* (2021) 3.
[191] 7.
[192] 36.

Chapter 4:
Regulatory challenges

4.1 Introduction

South Africa is in dire need of dedicated legislation for the regulation of electronic payment transactions.[193] The reasoning behind this concern lies in numerous uncertainties and unresolved issues pertaining to electronic payments. Some of these will be explored herein.

4.2 Fraudulent, unauthorised or unintended electronic payments

As explained previously,[194] an electronic payment is effected by means of a payment order given by the customer to the bank. This order can be given electronically, orally or in writing.[195] Where the payment order is given orally or in writing, the risk of fraud is quite obvious.[196] Where it is given electronically, no signature is added to such an order and it is verified by electronic means.[197] In the absence of adequate security measures, the electronic message can be intercepted and modified.[198] A payment card or an electronic purse can also be lost or stolen and used by someone who has knowledge of the PIN to make payments or withdrawals.[199] In addition, credit card details can be seized before it reaches the payee and used for improper purposes, or the payee itself can abuse its client's credit card details.[200] Also, where payment instructions are drafted or dispatched electronically, errors can occur, such as duplicated payment instructions, the entry of incorrect amounts or incorrect details for the beneficiary.[201]

The risk of fraud or unauthorised electronic payments is further augmented by the fact that they are cleared on an account number only, as opposed to payment by

---

[193] Schulze (2020) 39.
[194] See Chapter 1.
[195] Sharrock 371.
[196] *Ibid.*
[197] *Ibid.*
[198] *Ibid*.
[199] *Ibid.*
[200] VA Lawack-Davids and FE Marx "Consumer protection measures for erroneous or unauthorized internet payments: some lessons from the European Union?" (2010) *Obiter* 446 - 458 446 (hereafter Lawack-Davids and Marx).
[201] Geva (2020) 60.

way of a cheque, where the beneficiary's name and account number are verified to ensure that they match.[202]

The liability of the bank and its customer for a loss suffered due to fraudulent or unauthorised payments is informed by the common law and the terms of the bank-customer agreement. As discussed in chapter 3, the common law principles of mandate govern the legal relationship between the bank and the customer when it comes to electronic payment instructions, which places certain duties on the bank.[203] In this regard, the originator is not represented by the bank, but the latter merely acts as mandatary.[204] Where the bank acts contrary to the terms of the mandate or without authorisation, it will be liable for any consequent loss.[205] The customer, in turn, has a duty to take reasonable care when the payment instruction is given.[206]

The bank-customer agreement normally provides for circumstances under which the bank will be liable for unauthorised or fraudulent payments and banks will no doubt seek to assign as much of the risk as possible to the customer.[207] The terms of the bank-customer agreement will, however, have to survive the provisions of the CPA where it applies.[208]

In the instance of an unauthorised or unintended payment, the bank's right to reverse such payment, or for the payment instruction to be countermanded or revoked, seems to be somewhat of a grey area. Here, one can distinguish between the situation where the customer instructs the bank not to proceed with the transfer (or a countermand) and where the bank unilaterally reverses a transfer due to a fault on their part.[209]

In terms of the common law, a mandate can be revoked before it has been completed or executed.[210] It is thus obvious that, once a payment has been completed, it cannot be countermanded.[211] The moment a payment is complete is therefore an essential determination when considering the possibility of a countermand.[212] Such

---

[202] Sharrock 370-371.
[203] See paragraph 3.2.
[204] Sharrock 368.
[205] 377.
[206] *Ibid.*
[207] Sharrock 371 - 372.
[208] See paragraph 3.3.4.
[209] Sharrock 375-376.
[210] Sharrock 374; Schulze (2007) 383.
[211] Sharrock 292.
[212] 289.

moment can be determined by the rules of the electronic system used or, in the absence of such a rule, banking practice will be considered to make the determination.[213] It has been argued that the moment the creditor obtains an unconditional right to payment against his or her bank, the payment is complete.[214] Other arguments refer to the moment the beneficiary's bank decides to credit the beneficiary's account unconditionally as the moment of payment.[215]

Where the payer and the payee are customers of the same bank, the payment is instant and the instruction to countermand must reach the beneficiary's bank before payment into the latter's account.[216] Where two different banks are involved, it can be said that the countermand is possible until the beneficiary's bank has received the payment instruction.[217]The bank-customer agreement may also contain provisions that regulate the circumstances in which a payment instruction can be countermanded or the payment reversed.[218]

Of relevance in the context of countermanding a credit transfer is the *obiter* comment by the court in the matter of *Take and Save Trading CC v Standard Bank of South Africa Ltd*[219] to the effect that funds transferred cannot be reversed unless the beneficiary has agreed to the reversal.[220] The matter concerned a request by the client to reverse or countermand certain electronic fund transfers made to the account of a third party, after the cheques that were deposited in the client's account were dishonoured due to a lack of funds, resulting in his account becoming overdrawn.[221] Evidence was presented by a bank employee that the provisions of an agreement between banks prohibit the reversal of a transfer without the beneficiary's consent.[222] The court stated that, once a credit transfer has been effected, it belongs to the beneficiary and must be held by the bank for such beneficiary's credit.[223] This dictum has been criticized as an unfair rule in all circumstances concerning the reversal of an electronic payment, especially where fraud has been committed against the payer.[224]

---

213 290.
214 *Ibid*.
215 290-291.
216 375.
217 *Ibid.*
218 Sharrock 374-375.
219 2004 (4) SA 1 (SCA).
220 Paragraph 17.
221 Paragraphs 8-9.
222 Paragraph 12.
223 Paragraph 17.
224 Schulze (2004(1)) 677; Schulze (2020) 32.

It should however be noted that in *Take and Save Trading*, the payment instruction was not fraudulent or unauthorised, or even unintended. The court's *obiter* comment was also not qualified or contextualised.[225]

An erroneous payment instruction was the issue to be decided in *Nissan South Africa (Pty) Ltd v Marnitz (Stand 186 Aeroport (Pty) Ltd Intervening)*.[226] In this matter, the originator, Nissan, gave the bank a payment instruction, but the bank used the incorrect bank account for the beneficiary, with the result that the money was transferred into the wrong account.[227] The facts in *Nissan* were distinguished from that of *Take and Save Trading* on the basis that the latter case concerned a valid transfer as payment for goods delivered and could therefore not be reversed without the beneficiary's consent.[228] The court stated that "[p]ayment is a bilateral juristic act requiring the meeting of two minds" and therefore, in the event of a payment being made by mistake, the beneficiary, being aware of the mistake, is not entitled to the funds, as ownership did not pass.[229] In the event of the beneficiary appropriating the funds, it would amount to theft.[230] Although the decision in *Nissan* clarified the obiter comment of the court in *Take and Save Trading*, Schulze states that the situation is still unclear for a number of reasons, which will be referred to *infra*.[231]

The issue of the bank's right to unilaterally reverse a credit transfer without the beneficiary's consent, again came up for decision in *Nedbank Ltd v Pestana*.[232] In this matter, Nedbank's head office received a notice in terms of section 99 of the Income Tax Act 58 of 1962, appointing the bank as agent for the account holder (Pestana) and requiring the bank to pay over to the South African Revenue Service any amounts standing to the credit of Pestana.[233] Later on the same day, a branch office of the bank received an instruction from Pestana to transfer an amount of R480 000.00 from his account to another account held by another Pestana with the same bank.[234] The bank, unaware of the section 99 appointment, heeded the instruction and the other Pestana's

[225] Schulze (2004(1)) 681.
[226] 2005 (1) SA 441 (SCA).
[227] Paragraphs 2-3.
[228] Paragraph 22.
[229] Paragraph 24.
[230] *Ibid*.
[231] Schulze (2004(1)) 683-684.
[232] 2009 (2) SA 189 (SCA).
[233] Paragraph 3.
[234] *Ibid*.

account was credited with the amount.[235] When the branch became aware of the appointment, it reversed the transfer and made the payment to the South African Revenue Service.[236] The second Pestana, the beneficiary of the initial transfer, then instituted action against Nedbank. The matter was presented by way of a stated case and the court was asked to answer a question of law, namely, whether the bank was entitled to unilaterally reverse the transfer without the beneficiary's consent, in light of the section 99 appointment.[237] The court *a quo* decided in favour of the bank,[238] and on appeal to the full bench, the decision was overturned.[239] The matter then went to the Supreme Court of Appeal, where the decision by the full bench was confirmed.[240] The court found that, once an unconditional payment was completed and the beneficiary's account credited, and the bank had the intention of doing so, it cannot be reversed without the concurrence of the beneficiary.[241] The court accepted that, on the facts before it, the transfer was valid.[242] The court commented that "[i]t 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".[243] The court mentioned that, in cases where money was transferred as a result of fraud or theft, the funds can be validly reversed.[244] Schulze states that this decision has left it open to future courts to allow the unilateral reversal of a credit transfer.[245]

Van Heerden[246] concludes, with reference to the decisions as discussed, that a bank may reverse an unauthorised credit transfer with the consent of the beneficiary or without such consent where an invalid transfer occurred.[247] She states that banks may reverse unauthorised or fraudulent payments so as not to be in breach of their obligations in terms of their mandate, but their decision will depend on the terms of the

[235] *Ibid*.
[236] *Ibid*.
[237] Paragraph 4.
[238] Paragraph 2.
[239] *Ibid.*
[240] Paragraph 17.
[241] Paragraphs 10-16.
[242] Paragraph 10.
[243] Paragraph 8.
[244] Paragraph 9.
[245] Schulze (2020) 35.
[246] Sharrock 381.
[247] Ibid.

bank-customer agreement which can provide that the customer bears the risk of fraudulent or unauthorised payments, in which instance banks will not employ reversal.[248]

In the more recent case of *Ixocure (Pty) Ltd v FirstRand Bank Ltd*,[249] the court was faced with a provisional credit transfer that was reversed after allegations of fraud were brought to the bank's attention. In this matter, the plaintiff company, controlled by one Lombard, had a business relationship with a company by the name of Likhanyile Trading Enterprises (Pty) Ltd (L), in terms of which Lombard was a signatory to the account of L held with the defendant bank.[250] Both the plaintiff and Lombard also held accounts with the defendant bank. The dispute pertained to a transfer by Lombard from L's account into that of the plaintiff, and the subsequent transfer of almost the same amount from the plaintiff's account into Lombard's personal account.[251] Sometime before this transfer took place, L had removed Lombard as a signatory to the account.[252] The day after the transfer, L became aware of it and reported suspected fraud to the bank, who then reacted by putting a "hard hold" on the account of L, with the result that the transfer from L to the plaintiff was not completed but reversed.[253] The bank relied on the provisions of the bank-customer agreement for placing the hold on the account and to stop the transfer.[254] Lombard was then left with the credit in his personal account, but a large debit in the plaintiff's account with the transfer made from L's account not showing.[255] The plaintiff claimed the amount of the transfer from the bank on the basis that the bank unilaterally and without its consent transferred the amount out of the plaintiff's account.[256]

On behalf of the bank, it was confirmed that the transfer was provisional and not finally completed in terms of the bank's processes due thereto that the payment instruction was done after 8pm on the online banking platform.[257] When the hold was placed on the account, the transfer was stopped, redirected into a suspense account

[248] Sharrock 381-382.
[249] Unreported case no 19618/2014 (WCC), 30 November 2017.
[250] Paragraph 4.
[251] Paragraph 6.
[252] Paragraph 14.
[253] Paragraph 16-17.
[254] Paragraph 2.
[255] Paragraph 7.
[256] Paragraph 1.
[257] Paragraph 19.

and transferred back into L's account.[258] The court found that, because the transfer was not completed, the findings in *Pestana* were not applicable.[259] The plaintiff also relied on the doctrine of estoppel on several grounds, the details of which are not relevant for current purposes, but suffice it to say that the court did not uphold any of these claims. The plaintiff's claim was ultimately dismissed.[260]

Schulze states that the finding in *Ixocure* is correct, but comments on certain aspects of the judgment.[261] He states that, in this case, the parties involved were all customers of the same bank, which will not necessarily always be the case. Where the parties are with different banks, one must assume that the inter-bank agreement will provide for a situation such as the one in *Ixocure*, but because that agreement is confidential, it remains pure speculation.[262] He also states that the court did not specify which standard agreement was relied on, whether it was the one with L or with the plaintiff.[263] In circumstances where the parties are clients of different banks, the issue can become even more complicated.

Schulze opines that, even though the decisions referred to above have brought some measure of clarity, there are still a number of unresolved aspects pertaining to the reversal of electronic payments.[264] He argues that the provisions of the confidential inter-bank agreement referred to by the bank's witness in *Take and Save Trading* to the effect that an EFT cannot be reversed are problematic.[265] Furthermore, although the court in *Nissan* clarified the comments made in *Take and Save Trading* on the basis that the bank should be allowed to unilaterally, without the beneficiary's consent, reverse an invalid payment, no clear guidance was given on what will qualify as an invalid or a valid payment.[266] He further states that the decision in *Ixocure* does not provide much clarity on the question whether an electronic transfer can be reversed without the consent of the beneficiary, as the transfer in that matter was never

[258] Paragraph 20.
[259] Paragraph 25.
[260] Paragraph 38.
[261] Schulze (2020) 38.
[262] *Ibid*.
[263] *Ibid*.
[264] Schulze (2020) 38.
[265] *Ibid.*
[266] *Ibid.*

completed and therefore, a reversal thereof was not relevant.[267] The issue of when a payment is finally credited to the beneficiary is also not finally resolved.[268]

4.3 Consumer protection

The lack of legislation dedicated to the regulation of electronic payments raises consumer protection concerns. It has been pointed out previously[269] that consumer protection legislation has general application to electronic banking in certain limited instances but it does not cover all aspects of consumer protection in this context. Lawack-Davids and Marx opine that consumer protection laws are inadequate to sufficiently protect consumers against losses suffered as a result of erroneous or unauthorised internet payments.[270]

Schulze points out that consumers are at a serious disadvantage when it comes to smart cards, electronic money and electronic fund transfer technology, as banks or other service providers have sought to protect themselves against the risks pertaining to the use of these payment methods, which has left the user of this technology with a large portion of the risk.[271] Banks and other payment service providers dictate the terms upon which they will provide these services without any input from their customers or other consumer protection organisations.[272] The customer is therefore left with no choice but to accept these terms if he wants to make use of the service, even if a large portion of the risk is allocated to the customer.[273] Schulze also reasons that, because there is only a limited number of banks operating as such in South Africa, competition between banks is almost non-existent.[274] This exacerbates consumer protection concerns.

The absence of a regulatory framework is in contrast to the position pertaining to cheques, the use of which is regulated by the Bills of Exchange Act 34 of 1964 and principles developed in the courts over the years.[275] It thus seems as if the user of an

[267] Schulze (2020) 39.
[268] *Ibid*.
[269] See Chapter 3.
[270] Lawack-Davids and Marx 457.
[271] Schulze (2004(3)) 57.
[272] 58.
[273] *Ibid*.
[274] *Ibid*.
[275] Schulze (2004(3)) 59.

electronic payment method could be worse off than those select few who still make use of cheques.

4.4 Risks associated with the use of crypto assets

Crypto assets exist in the virtual arena and cannot be associated with any particular jurisdiction, as it cannot be said that a crypto asset or virtual wallet is in any particular place at any given time.[276] Due to its use of cryptography, it is also completely anonymous.[277] A crypto asset can therefore not be said to be subject to the law of any particular country, which makes the regulation thereof almost impossible.

Crypto assets are not seen as money or legal tender, but they can function as money, and they do so in a regulatory lacuna.[278] Payment system laws are therefore bypassed by the use of alternative systems.[279] Widespread use of crypto assets to make payments also poses risks to the efficiency of the national payment system.[280]

It has also been stated that crypto assets are not suitable to be used as an everyday method of payment.[281] This is due to "their high price volatility, restricted scalability, limited throughput of transactions, and lack of payment finality".[282] The use of crypto assets as a payment method also raises consumer protection concerns. For example, it is uncertain whether a payment made in error, an overpayment or even fraudulent payments can be reversed.[283]

4.5 Conclusion

Based on the above analysis, the need for regulatory intervention in the field of electronic payments should be explored. In the next chapter, developments in other countries are investigated in comparison to the position in South Africa.

[276] S Eiselen "What to do with bitcoin and blockchain" (2019 (82)) *THRHR* 632-640 636.
[277] *Ibid*.
[278] IFWG, CAR WG *Position paper* (2021) 12.
[279] 24.
[280] 25.
[281] FSI Insights 22.
[282] *Ibid*.
[283] IGFW, CAR WG *Position paper* (2021) 25.

Chapter 5:
International developments

5.1 Introduction

Unlike the position in South Africa, other countries have enacted legislation dealing specifically with the rights and obligations of parties involved in electronic payment transactions.[284] The position in the European Union and the United States of America will be explored herein to serve as good examples.

5.2 European Union

5.2.1 Payment Services Directive

The regulation of electronic payments in the European Union is informed by the Payment Services Directive (EU) 2015/2366, also referred to as PSD2 on account of the fact that it replaced the previous payment services directive.[285] Member countries were required to implement the rules of the directive into national law by 13 January 2018.[286] It sets out rules applicable to payment services within the EU. The aim of PSD2 is to lay a legal foundation for a more consolidated internal payment services market within the European Union.[287] Enhanced security requirements for electronic payments, transparency of information as well as the rights and obligations of payment service providers and their users are catered for in PSD2.[288] It also accommodates new market entrants in the payment services arena, taking into account new innovations, thereby promoting competition in the market.[289] A wide scope of payment services are covered by PSD2 and includes EFTs, payment cards and electronic money.[290]

---

[284] Sharrock 250.
[285] Schulze (2020) 40; Directive (EU) 2015/2366 of the European Parliament of the Council of 25 November 2015, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366 (accessed 25-09-2021) (hereafter PSD2).
[286] European Commission, implementing measures for Directive (EU) 2015/2366 on payment services, available at https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/implementation/implementation-eu-countries_en (accessed 25-09-2021).
[287] PSD2 Summary, available at https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366 (accessed 26-09-2021) (hereafter PSD2 summary).
[288] PSD2 Summary.
[289] *Ibid*.
[290] Annex 1 of PSD2.

New services are provided for, referred to as payment initiation services, which are defined as "a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider".[291] Account information service is "an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider".[292]

PSD2 contains, *inter alia*, provisions regulating the rights and obligations of parties in the event of unauthorised payment transactions. It provides in article 71 that an unauthorised or unintended payment must be rectified if the customer notifies the payment service provider of the transaction without undue delay but no longer than thirteen months after becoming aware of the payment. The time period of thirteen months does not apply if the payment service provider did not provide information on the transaction in line with Title III.[293] The customer will also enjoy the same right of recourse where a payment initiation service provider is involved.[294] Schulze states in this regard that the provisions of article 71 cover both provisional and final credit transfers and that the consent of the receiver of the funds is not a requirement.[295] If a customer claims that a payment was not authorised or executed correctly, the payment service provider or the payment initiation service provider has to prove the contrary.[296] To this end, the payment instrument used is not by itself sufficient proof that the payment was authorised or that the customer acted fraudulently or with gross negligence.[297]

Parties' respective liabilities for unauthorised payments are also comprehensively provided for in articles 73 and 74. It provides that the amount of the unauthorised payment shall be refunded to the customer immediately but in any event no later than the end of the business day following the day of notification.[298] If a payment initiation service provider is involved, the same rule applies and the account servicing payment service provider must refund the money.[299] The refund can be held

[291] Article 4(15) of PSD2.
[292] Article 4(16) of PSD2.
[293] Article 71(1) of PSD2.
[294] Article 71(2) of PSD2.
[295] Schulze (2020) 44.
[296] Article 72(1) of PSD2.
[297] Article 72(2) of PSD2.
[298] Article 73(1) of PSD2.
[299] Article 73(2) of PSD2.

back if the payment service provider suspects fraud, provided the authorities are notified in writing.[300] The customer must on account of the refund be placed in the same position as he would have been, had the unauthorised payment not taken place.[301] The payment initiation service provider must compensate the account servicing payment service provider if the former is responsible for the unauthorised payment.[302] Any additional financial compensation will be determined by the contract between the parties and the law applicable thereto.[303]

Article 74 limits the liability of payment service providers for unauthorised payments, as provided for in the preceding article. It provides that the payer, or the customer, can be held liable for losses to the maximum amount of EUR50 where the loss occurred as a result of a lost or stolen payment instrument or the misappropriation thereof.[304] This limit is not applicable if the loss or misappropriation was not detectable to the payer before the payment took place, provided no fraud was committed by the payer or where the loss was caused by an act or omission on the part of the payment service provider, its branches, employees or agents.[305] Where the payer committed fraud or intentionally or through gross negligence failed to adhere to its obligations in terms of article 69, the limit will also not apply.[306] If such fraud or failure to adhere to the article 69 requirements is not present, member states may reduce the payer's liability, taking into account the circumstances of the loss or misappropriation of the payment instrument and the specific personalised security credentials.[307] Article 74(2) further provides that "[w]here the payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider".[308] Where sufficient means of notification of a lost or stolen payment instrument are not furnished by the payment

[300] Article 72(1) of PSD2.
[301] Articles 73(1) & (2) of PSD2.
[302] Article 73(2) of PSD2.
[303] Article 73(3) of PSD2.
[304] Article 74(1) of PSD2.
[305] *Ibid*.
[306] *Ibid*.
[307] *Ibid*.
[308] Article 74(2) of PSD2.

service provider, as set out in point (c) of article 70(1), the payer will not be held liable for any losses, except where fraudulent behaviour is involved.[309]

Articles 75 to 77 further regulate certain instances of authorised payments, such as instances where payment is made by making use of a payment card and the amount of the transaction is not provided when authorisation is given,[310] and where double payment was made on payments initiated by the payee.[311]

In the instance of an erroneous payment instruction, article 88 provides that a payment order shall be deemed to have been executed correctly where it was done on account of a unique identifier provided by the payment service user, and that, if the latter provided an incorrect unique identifier, the payment service provider will not be liable for any deficiencies in the payment transaction.[312] An example of a unique identifier is an account number.[313] It further provides that the payment service provider will make a reasonable attempt to recover the funds with the cooperation of the payee's payment service provider.[314] The payer will, however, have to institute its own claim in the event of the funds not being recoverable. If so agreed, the payment service provider may charge the payment service user for recovering the funds.[315]

With regard to the cancellation of a payment order, article 80 states that, once a payment order has been received by the payment service provider, it may not be revoked.[316] It provides further that, where a payment initiation service provider is involved or where the payment is initiated by the payee, the payment order may not be cancelled after the payer has given consent for the payment to the payment initiation service provider or to the payee.[317] If a payment is to be made on a day agreed to between the payment service user and the payment service provider, the payment order may be revoked by the latest on the business day preceding the agreed day.[318] After these cut-off times, the payment order may only be cancelled by

[309] Article 74(3) of PSD2.
[310] Article 75 of PSD2.
[311] Articles 76 and 77 of PSD2.
[312] Article 88(1) - (2) of PSD2.
[313] Geva (2020) 60.
[314] Article 88(3) of PSD2.
[315] *Ibid*.
[316] Article 80(1) of PSD2.
[317] Article 80(2) of PSD2.
[318] Article 80(3) - (4) of PSD2.

agreement between the payment service provider and the payment service user as well as the payee if the latter initiated the payment.[319]

To conclude, and as stated by Schulze, the provisions of PSD2 are detailed and provide much needed certainty in the sphere of payment services in the European Union.[320]

5.2.2 Regulatory response to crypto assets

The European Commission issued a proposal in September 2020, referred to as the Markets in Crypto-assets Regulation (MICAR).[321] The proposal is part of a broader digital finance package aimed at supporting the opportunities presented by digital finance whilst mitigating the risks.[322] The European Commission noted that existing regulation in the European Union will not include all types of crypto assets and therefore MICAR serves to cover these shortcomings.[323]

In terms of MICAR, crypto assets are broken down into different categories, including crypto assets in general, asset-referenced tokens, e-money tokens and significant tokens.[324] Crypto asset service providers are defined and include services pertaining to the custody and administration of crypto assets, the running of trading platforms and crypto asset related advice.[325]

It proposes, *inter alia*, that crypto asset service providers be required to comply with rules preventing market abuse, as well as organisational and prudential requirements.[326] It further proposes that crypto asset issuers be required to comply with consumer protection rules, which includes the issuance of a crypto asset white paper and notification to the relevant authorities.[327] Further consumer protection rules to be complied with include consumers' rights to withdraw once a token has been attained, the provision of information that is fair and unambiguous, the requirement that issuers of crypto assets should always act in a manner that is fair, honest and in the best interest of their clients as well as procedural requirements for dealing with

[319] Article 80(5) of PSD2.
[320] Schulze (2020) 48.
[321] FSI Insights 35.
[322] *Ibid*.
[323] *Ibid*.
[324] *Ibid.*
[325] *Ibid*.
[326] FSI Insights 36.
[327] *Ibid*.

complaints.[328] It also contains provisions pertaining to good governance in respect of crypto asset service providers.[329]

5.3 United States of America

5.3.1 The Uniform Commercial Code

There are various pieces of legislation in the United States of America that cover electronic payments.[330] Suffice it to mention only one. The Uniform Commercial Code (UCC) is a comprehensive set of rules and principles that each state has to incorporate into state law.[331] Article 4A of the UCC regulates credit transfers by non-consumers.[332] In terms of section 4A-102 of the UCC, the article applies to a "funds transfer", which is defined in section 4A-104 as a "series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator's bank or an intermediary bank intended to carry out the originator's payment order. A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order".[333]

Section 4A-103 of the UCC provides that a "payment order" is an instruction by a sender to a receiving bank, given orally, electronically or in writing, to pay, or cause to be paid, an amount of money to the beneficiary. Article 4A of the UCC excludes a fund transfer that falls under the Electronic Fund Transfer Act of 1978.[334]

Article 4A of the UCC contains, *inter alia*, provisions pertaining to the verification of payment orders by making use of reasonable security procedures, agreed upon between the bank and its customer to prevent unauthorised payment orders.[335] If such security procedure is followed by the bank and its agreement with the customer is complied with, it is entitled to regard a payment order as effective against the customer, even if the payment order was unauthorised.[336] If the customer can prove that the

---

[328] *Ibid*.
[329] *Ibid*.
[330] FR Malan and JT Pretorius "Credit transfers in South African law (1)" 2006 (69) *THRHR* 594-612 607 (hereafter Malan and Pretorius (2006)).
[331] *Ibid*.
[332] Geva (2020) 48.
[333] Article 4A-104(a) of the UCC, available at https://www.law.cornell.edu/ucc/4A (accessed 17-10-2021) (hereafter UCC).
[334] Geva (2020) 48; Article 4A-108 of the UCC.
[335] Section 4A - 202 of the UCC.
[336] Section 4A-202(b) of the UCC.

order was not authorised or that another person obtained information facilitating a breach of the security procedure, the bank is not entitled to enforce or retain the payment order, regardless of how the information was obtained or whether the customer was at fault.[337]

Section 4A-204 of the UCC provides for refunds in the event of unauthorised payment orders. It states that, if the bank accepts a payment order that is unauthorized, ineffective as against the customer in terms of section 4A-202 or unenforceable in terms of section 4A-203, the bank shall refund any payment of the payment order and be liable for interest on the refundable amount calculated from the day the bank received payment to the date of the refund. It further states that the bank will not be liable for such interest if the customer does not, by exercising ordinary care, establish that the payment was unauthorized and notify the bank within a reasonable time but at least within 90 days after the bank notified that customer of the payment or after the customer's account was debited.[338] The bank does, however, not have any right of recovery against the customer as a result of the latter's failure to notify the bank in terms of the section.[339] The bank and the customer may agree to vary the 90 day period, but the bank's duty to refund the customer may not be contracted out of.[340]

Erroneous payment orders are provided for in section 4A-205 of the UCC. It deals with payment orders to an incorrect beneficiary or for an incorrect amount, or instances where a payment order is erroneously duplicated.[341] It states that where the sender proves that the security procedure was complied with by such sender and that the bank could have detected the error by complying with such procedure, the sender is not obliged to pay for the order and the bank is entitled to recover any erroneous or overpayment from the beneficiary to the extent allowed by the law governing mistake and restitution.[342] The customer is obliged to notify the bank of the error within a reasonable time but at least within 90 days after receiving notification from the receiving bank that the payment order was accepted and that the customer's account has been debited.[343] If the bank proves that the customer failed to comply with this duty, the bank may recover any proven losses from the customer on account of such

[337] Section 4A-203(2) of the UCC.
[338] Section 4A-204(a) of the UCC.
[339] *Ibid*.
[340] Section 4A-204(b) of the UCC.
[341] Section 4A-205(a) of the UCC.
[342] Section 4A-205(a)(1) - (2) of the UCC.
[343] Section 4A-205(b) of the UCC.

failure, but the customer's liability may not exceed the amount of the erroneous payment order.[344]

UCC article 4A also contains provisions pertaining to the beneficiary bank's liability in the event of the latter receiving a payment order where the beneficiary's name, account number or other identification of the beneficiary does not exist or is unidentifiable.[345] It provides that, in such a case, no person has rights as a beneficiary of the order and it cannot be accepted.[346] It further contains provisions dealing with a situation where the beneficiary's name and bank account number do not match.[347] It provides that the beneficiary's bank is under no obligation to determine whether the name and account number match. If it is unaware of the discrepancy, it may rely on the account number in executing the payment order.[348] If the bank relies on the name only or where it is aware of the discrepancy between the name and the account number, no person has rights as a beneficiary except where such person was entitled to receive funds from the originator.[349] If not, the payment order cannot be accepted.[350] In the event of the originator's payment order describing the beneficiary inconsistently by name and number and the payment order is accepted by the bank by relying on the account number, the originator is liable to pay its payment order if it is a bank.[351] If the originator is a non-bank, and if it can prove that the beneficiary who received the payment was not entitled to such payment, the originator is not compelled to pay its order, "unless the originator's bank proves that the originator, before acceptance of the originator's order, had notice that payment of a payment order issued by the originator might be made by the beneficiary's bank on the basis of an identifying or bank account number even if it identifies a person different from the named beneficiary. Proof of notice may be made by any admissible evidence. The originator's bank satisfies the burden of proof if it proves that the originator, before the payment order was accepted, signed a writing stating the information to which the notice relates".[352] The section further contains provisions dealing with the parties' right of recovery.[353]

---

[344] *Ibid*.
[345] Section 4A-207(a) of the UCC.
[346] *Ibid*.
[347] Section 4A-207(b) of the UCC.
[348] Section 4A-207(b)(1) of the UCC.
[349] Section 4A-207(b)(2) of the UCC.
[350] *Ibid*.
[351] Section 4A-207(c)(1) of the UCC.
[352] Section 4A-207(c)(2) of the UCC.
[353] Section 4A-207(d)(1) & (2) of the UCC.

Further sections deal with the situation where the intermediary or beneficiary banks are described incorrectly.[354]

The provisions of section 4A-211 of the UCC cover the cancellation and amendment of a payment order. It provides that such communication should be verified pursuant to the security procedure in effect between the sender and the receiving bank, failing which it is not effective.[355] It further provides that the request will only be effective if it is received by the receiving bank at such a time and manner to allow it sufficient time to act on the request before the payment order is accepted.[356] After acceptance, a payment order can no longer be cancelled or amended unless the bank agrees to it or where a funds-transfer system rule provides for such cancellation or amendment without the bank's consent.[357] If the receiving bank other than the beneficiary's bank consents to the cancellation or amendment after acceptance, a conforming cancellation or amendment issued by the receiving bank must be made for it to be effective.[358] Where a payment order is accepted by the beneficiary's bank, it can only be cancelled or amended if the payment order was unauthorized or issued by mistake by the sender, which resulted in a payment order being duplicated or issued to an incorrect beneficiary or for an incorrect amount.[359] If the beneficiary had already been paid and the payment order is subsequently cancelled or amended, the beneficiary's bank may recover such an amount from the beneficiary to the extent allowed under the law of mistake and restitution.[360]

Although the field of application of the UCC is not as broad as the PSD2, its provisions are clear and detailed, and will regulate at least all non-consumer credit transfers.

5.3.2 Regulatory response to crypto assets

In the United States of America, financial regulators have adopted different regulatory responses to crypto assets.[361] The Federal Reserve System, which is the central bank

[354] Section 4A-208 of the UCC.
[355] Section 4A-211(a) of the UCC.
[356] Section 4A-211(b) of the UCC.
[357] Section 4A-211(c) of the UCC.
[358] Section 4A-211(c)(1) of the UCC.
[359] Section 4A-211(c)(2) of the UCC.
[360] *Ibid*.
[361] FR Edwards, K Hanley, R Litan and RL Weil "Crypto assets require better regulation: statement on the financial economists roundtable on crypto assets" (2019) *Financial Analysts Journal* 14-19 16 (hereafter Crypto assets (2019)).

of the United States of America, has taken the stance that it does not have authority to regulate crypto assets.[362] Rulings made by the Internal Revenue Service indicate that crypto assets are treated as property for tax purposes.[363] The Treasury Department, through the Financial Crime Enforcement Network, monitors criminal activities by making use of crypto assets.[364] It issued a guideline on 18 March 2013 to clarify the application of the Bank Secrecy Act to virtual currencies.[365] Two bills aimed at creating a special regulatory regime for crypto assets were introduced in the House of Congress in 2019.[366] It appears that, at this stage, the Federal Reserve has taken a monitoring approach towards crypto assets.[367]

[362] IFWG, CAR WG *Position paper* (2020) 52.
[363] *Ibid*; Crypto assets (2019) 16.
[364] Crypto assets (2019) 16.
[365] ST Middlebrook and SJ Hughes "Virtual uncertainty: developments in the law of electronic payments and financial services" (2013) 69(1) *Business Lawyer* 263 - 273 264.
[366] Crypto assets (2019) 16.
[367] IGFWG, CAR WG *Position paper* (2020) 52.

Chapter 6:
Conclusion

The conclusion to the above analysis can be summed up in the words of Geva:[368]

> "Briefly stated, in the modern era, on-going technological enhancements significantly increased the use and benefits of credit transfers. In turn, traditional payment instrument legislation, which focused on the paper-based negotiable instruments used in debit transfers, has become inadequate to deal with electronic payment transactions. General principles of law, though available, are slow to develop, such that reliance on them does not secure certainty and predictability. A contract is not an effective mechanism to provide for the rights of third parties; the same is true for interbank payment system rules. As well, a series of bilateral contracts is unlikely to produce harmonisation. Finally, between bank and customer, contracts can be one-sided, unfair to customers and thus, in some cases, risk lack of enforceability on public policy grounds."

Whilst other jurisdictions have adopted comprehensive rules to cater for most electronic payment methods, South Africa has taken a hands-off approach. The position pertaining to crypto assets is much different, in that the development of regulatory approaches to answer to the risks posed by this new innovation is ongoing.

In the interest of legal certainty, it is clear that the rights of parties in all electronic methods of payment should be regulated by dedicated legislation or industry codes. The case law discussed herein demonstrates the existing uncertainties in instances of fraudulent, unauthorised or erroneous payments as well as the circumstances in which a payment instruction can be countermanded. Closely linked to this problem is that of consumer protection and competition in the payment services market, which are lacking. For this, international developments can provide valuable guidance. The Second Payment Services Directive applicable in the European Union is comprehensive and covers most electronic payment methods. It contains detailed provisions pertaining to the rights of parties involved in electronic payment transactions, including instances of unauthorised or fraudulent payments as well as erroneous payment instructions. The directive also regulates the specific circumstances when a payment order can be revoked. It also accommodates new

[368] Geva (2020) 35-36.

entrants in the payment services industry, thereby enhancing competition in the market and embracing new innovations.

Although limited to non-consumer credit transfers, article 4A of the Uniform Commercial Code applicable in the United States of America similarly covers parties' rights when it comes to unauthorised, fraudulent or erroneous payments. It sets out in detail a beneficiary bank's liability in the event of a beneficiary's details being incorrect or non-existent. A payment originator's right to cancel a payment order is also regulated.

Until such time as South Africa follows the international standard, reliance will have to be placed on the common law, as developed in our courts, and those parts of legislation that do find application. It is recommended that legislation similar to that of PSD2, that covers all aspects of payment, be implemented.

-o0o-

Bibliography

Literature

Cornelius, S "The legal nature of payment by credit card" (2003) *SA Merc LJ* 153 - 171.

Du Toit, SF "Reflections on the South African Code of Banking Practice" 2014 *TSAR* 568-579.

Edwards, FR, Hanley, K, Litan, R and and Weil, RL "Crypto assets require better regulation: statement on the financial economists roundtable on crypto assets" (2019) *Financial Analysts Journal* 14-19

Eiselen, S "What to do with bitcoin and blockchain?" (2019) 82 *THRHR* 632-640.

Lawack, VA "Electronic innovations in the payment card industry" (1998) *SA Merc LJ* 233 - 239.

Lawack-Davids, VA and Marx, FE "Consumer protection measures for erroneous or unauthorized internet payments: some lessons from the European Union?" (2010) *Obiter* 446 - 458.

Malan, FR and Pretorius, JT "Credit transfers in South African law (1)" 2006 (69) *THRHR* 594-612.

Middlebrook, ST and Hughes, SJ "Virtual uncertainty: developments in the law of electronic payments and financial services" (2013) 69(1) *Business Lawyer* 263 - 273.

Moorcroft, J and Vessio, ML *Banking law and practice* (SI 19, Oct 2019)

Reddy, E & Lawack, V "An overview of the regulatory developments in South Africa regarding the use of cryptocurrencies" (2019) *SA Merc LJ* 1 - 28.

Sharrock, R *The Law of Banking and Payment in South Africa* (2016) Cape Town: Juta.

Scholtz, JW *Guide to the National Credit Act* (Service Issue 13, Jul 2021) Durban: LexisNexis.

Schulze, WG "The reversal of electronic payments under South African law: possible guidance from recent developments in European Union law" (2020) *SA Merc LJ* 22 - 50.

Schulze, WG "Countermanding an electronic funds transfer: the Supreme Court of Appeal takes a second bite at the cherry" (2004) *SA Merc LJ* 667- 684.

Schulze, WG "Electronic fund transfers and the bank's right to reverse a credit transfer: one small step for banking law, one huge leap for banks" (2007) *SA Merc LJ* 379 - 387.

Schulze, WG "Smart cards and e-money: new developments bring new problems" (2004) *SA Merc LJ* 703 - 715.

Schulze, WG "E-money and electronic fund transfers. A shortlist of some of the unresolved issues" (2004) *SA Merc LJ* 50 - 66.

Schulze, WG "Of credit cards, unauthorised withdrawals and fraudulent credit card users" (2005) *SA Merc LJ* 202-213.

Schulze, WG & Eiselen, GTS "Die terugskryf van 'n elektroniese oordrag en die rol van estoppel" (2020) *TSAR* 837-846.

Tuba, MD "The regulation of electronic money institutions in the SADC region: some lessons from the EU" (2014(17)6) *PELJ* 2269-2312.

Van Zyl, DH "Mandate" in *LAWSA* vol 28 3ed part 1.

Legislation

Electronic Communications and Transactions Act 25 of 2002

Financial Sector Regulation Act 9 of 2017

National Credit Act 34 of 2005

Consumer Protection Act 68 of 2008

Case law

DA Ungaro & Sons (Pty) Ltd v ABSA Bank Ltd [2015] 4 All SA 783 (GJ).

Ixocure (Pty) Ltd v FirstRand Bank Ltd Unreported case no 19618/2014 (WCC), 30 November 2017.

Nedbank Ltd v Pestana 2009 (2) SA 189 (SCA).

Nissan South Africa (Pty) Ltd v Marnitz (Stand 186 Aeroport (Pty) Ltd Intervening) 2005 (1) SA 441 (SCA).

Standard Bank of SA Ltd v Oneanate Investments (Pty) Ltd 1995 (4) SA 510 (C).

Strydom NO v ABSA Bank Bpk 2001 (3) SA 185 (T).

Take and Save Trading CC v Standard Bank of South Africa Ltd 2004 (4) SA 1 (SCA).

Online sources

Geva, B "Electronic payments: guide on legal and regulatory reforms and best practices for developing countries" (2020) *Articles & Book Chapters* 2796 viii, available at https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=3796&context=scholarly_works (accessed 27-09-2021).

Bank for International Settlements, Financial Stability Institute "Fintech and payments: regulating digital payment services and e-money (Jul 2021), available at https://www.bis.org/fsi/publ/insights33.pdf (accessed 17-10-2021).

The South African Reserve Bank *Position Paper on Electronic Money* (Nov 2009), available at https://www.resbank.co.za/content/dam/sarb/what-we-do/financial-surveillance/general-public/PP2009_01.pdf (accessed 08-08-2021).

The Banking Association of South Africa *Code of Banking Practice* (Jan 2012), available at https://www.banking.org.za/code-of-banking-practice/ (accessed 08-08-2021).

Financial Action Task Force *Virtual currencies key definitions and potential AML/CFT risks* (June 2004), available at https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed 09-08-2021).

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN (accessed 26-10-2021).

The South African Reserve Bank *Position paper on virtual currencies* (2014), available at https://www.resbank.co.za/content/dam/sarb/what-we-do/financial-surveillance/general-public/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf (accessed 09-08-2021).

Intergovernmental Fintech Working Group, Crypto Assets Regulatory Working Group *Position paper on crypto assets* (June 2021), available at http://www.treasury.gov.za/comm_media/press/2021/IFWG_CAR%20WG_Position%20paper%20on%20crypto%20assets_Final.pdf (accessed 09-08-2021).

Ombudsman for Banking Services Terms of Reference (Feb 2018), available at: https://www.obssa.co.za/publications/terms-of-reference/ (accessed 28-10-2021).

Intergovernmental Fintech Working Group, Crypto Assets Regulatory Working Group *Position paper on crypto assets* (Apr 2020), available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf (accessed 29-09-2021).

IFWG, CAR WG "Consultation paper on policy proposals for crypto assets" (2019), available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf (accessed 12-05-2020).

Directive (EU) 2015/2366 of the European Parliament of the Council of 25 November 2015, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366 (accessed 25-09-2021).

European Commission, implementing measures for Directive (EU) 2015/2366 on payment services, available at https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/implementation/implementation-eu-countries_en (accessed 25-09-2021).

PSD2 Summary, available at https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366 (accessed 26-09-2021).

Article 4A of the Uniform Commercial Code, available at https://www.law.cornell.edu/ucc/4A (accessed 17-10-2021).