The liability of banks in respect of unauthorised digital payments: Is there adequate legislative protection afforded to consumers in South Africa?

By

1865365

Submitted in partial fulfilment of the requirements for the degree of

Master of Laws by Coursework and Research Report

at the University of the Witwatersrand, Johannesburg

Date: 18 February 2025

DECLARATION

I, **1865365** declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements for the degree of Master of Laws (by Coursework and Research Report) at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in any other university.

I have submitted my final Research Report through TurnItIn and have attached the report to my submission.

Word Count: 9111

1865365

DATE: 28 February 2025

ABSTRACT

As the payment landscape evolves to keep up with new trends in technology, there has been a shift towards the creation and use of digital payment solutions. The rise in financial technology (Fintech) has provided consumers with faster and more convenient ways to pay. The efforts to create a contactless and cashless society are helping to drive financial inclusion and to close the digital divides. However, the shift has also meant that there has been an increase in fraudulent activities.

The rapid expansion of digital banking in South Africa has led to a significant rise in unauthorised digital transactions. Similar to other countries, South Africa is grappling with the challenges posed by unauthorised digital payments and the subsequent responsibilities of banks in ensuring consumer protection. Currently, South Africa does not have dedicated legislation for digital payments. A key problem with this is the lack of explicit provisions detailing the extent to which banks are liable for unauthorised digital payments, particularly in cases where consumers fall victim to cyber fraud. While some common law principles, such as contractual and delictual liability may be applicable, there remains uncertainty regarding the circumstances under which banks are required to reimburse affected consumers. This research examines the liability of banks in cases of unauthorised digital payments, assessing whether the existing legislative framework provides sufficient safeguards for consumers. The analysis explores key legal provisions, including the *Banks Act,* the *Electronic Communications and Transactions Act (ECTA),* the *National Payment System Act*, the *National Credit Act* and the *Code of Banking Practice,* alongside relevant case law. It also considers the role of regulatory bodies such as the Prudential Authority and the Financial Sector Conduct Authority in enforcing consumer rights. The study identifies gaps in the current regulatory framework, particularly concerning liability allocation between banks and consumers, and evaluates the effectiveness of dispute resolution mechanisms. This research further explores how the EU's PSD has contributed towards making payments safer and more secure, in the hope that South Africa may draw lessons from the EU. The study concludes by proposing legal and policy reforms to enhance consumer protection and ensure a balanced approach to bank liability in the digital era.

TABLE OF CONTENTS

I. INTRODUCTION

Technology is transforming the world around us at an accelerated rate. The evolution is allowing people and economies to become more and more interconnected.[1] In Africa, technology has been recognised as one of the most powerful drivers of economic growth – to revitalise industries, create employment and bridge the divides between the rich and the poor.[2] A central part of this includes reinventing the financial services sector to better serve the needs of the people.[3] Developments in technology have meant that banks are increasingly able to enter new markets and territories and expand without physical infrastructure.[4] This is particularly true since digitalisation has enabled 'branchless banking' through Internet and mobile banking, as well as through digital terminals.[5] This has become important with the rapid shift to a contactless ecosystem that is helping accelerate the de-cashing of the economy.[6] The efforts to create a contactless and cashless society are helping drive financial inclusion and close the digital divides.[7] However, the shift has also meant that there has been an increase in fraudulent activities.

The pervasive growth of the Internet and smartphones has fundamentally altered the landscape of commercial transactions, fostering the creation of innovative payment methodologies.[8] These methods enable consumers to execute remote transactions without the necessity of being physically present at the point of sale.[9] In this evolving scenario, local and international payment service providers have introduced alternatives to the conventional payment methods.[10] Some provide platforms for fund retention within a designated payment account, commonly known as mobile banking.[11] Others present diverse payment solutions, including applications that leverage personal identifiers for authenticating the payer's

[1] Ozow 'Fraud within the payment industry in South Africa' available at *https://ozow.com/white-paper/fraud-within-the-payment-industry-in-south-africa*, accessed on 07 January 2024.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ruth Plato-Shinar 'Regulating liability for unauthorised digital payments: Insights for South Africa' (2020) *Annual Banking Law Update* 1-5.
[9] Ibid.
[10] Ibid.
[11] Ibid.

identity.[12] The fundamental goal driving these advancements is to facilitate seamless, rapid, and secure payment processes for all stakeholders involved.[13]

Advanced payment methods offer various advantages such as: increased competition in payment services through an expanded customer choice; a reduction in transaction costs; speedy transactions resulting in convenience for the customer; and a reduction in money laundering and tax evasion.[14] However, along with the aforementioned benefits, using advanced payment methods also bears a severe risk – the accessibility and ease of use may impair the security of the payment transaction and expose the consumer to fraud and misuse, either by the payee or by a dishonest third party.[15] In order to enjoy the benefits of advanced payment instruments and reduce the risks involved, the existing legal infrastructure needs to adapt to technological developments and the advancing payment methods.[16] In some countries, the provision of payment services was perceived as requiring separate regulation, leading to the establishment of a designated regulator to supervise the provision of payment services.[17]

The experience in South Africa, like in other countries, shows that unauthorised use of payment instruments is a common occurrence, a phenomenon that has evolved with increasingly sophisticated methods over the years.[18] Techniques such as cracking secret codes or passwords, fraudulently extracting the information from the instrument's user (such as through phishing), or employing the intricate hacking strategies on computer systems, all aim to gather the necessary information for the misuse of third party payment instruments.[19] Furthermore, the upsurge in the use of online trading and transactions conducted through the payee's website or designated applications raises concerns that individuals associated with the payee, or those operating on their behalf, who were exposed to the details of the payer's payment instrument, might engage in unauthorised transactions using these payment instruments.[20] From a consumer perspective, one of the most problematic areas of digital payments is the electronic funds transfer (EFT) – which is what this research mainly focuses on.[21]

---

[12] Ibid.
[13] Ibid.
[14] Ibid at 2.
[15] Ibid.
[16] Ibid.
[17] Ibid at 2-3.
[18] Ibid.
[19] Ibid 3-7.
[20] Ibid.
[21] Ibid.

In contrast to countries that have addressed the issue of unauthorised digital payments through legislative measures like the European Union's Payment Services Directive, which is legislation that is dedicated to the payments market in the EU, South Africa stills lacks a comprehensive legislation that specifically deals with the matter.[22] The National Credit Act only minimally covers unauthorised payments, primarily related to credit cards, within a concise section.[23] However, a more expansive framework governing various digital payment methods exists within the Code of Banking Practice[24] established by the Banking Association of South Africa (the Code).[25] Under this Code, a bank becomes contractually bound by the Code where its provisions are incorporated into the agreement with its customer (compliance to the Code is voluntary and does not necessarily bind all banks).[26] One significant aspect of the Code involves banks recognising the authority of the National Finance Ombuds, which is composed of various Ombuds, including the Ombudsman for Banking Services. This body operates in three capacities: mediating disputes; making binding determinations based on the Code and on the law where appropriate; and offering recommendations in situations not explicitly covered, including those based on the principles of fairness and equity.[27] Should a bank refuse to abide by the Ombudsman's recommendation, the Ombudsman reserves the right to publish the recommendation and the bank's refusal to comply with it.[28] It is also possible for the Ombudsman to make a determination, and such a determination may be made an order of court.[29]

Based on the arrangement set forth in the Code, it is quite apparent that the protection afforded to consumers in instances of unauthorised digital payments is significantly more limited when compared to the legislative framework established in other jurisdictions.[30] In certain countries[31], the payment service provider assumed the majority of the financial loss, whereas, under the South African Code, the consumer is responsible for bearing the largest portion of the associated risk.[32] If the primary objective is to foster greater adoption of digital payment instruments by enhancing public confidence in the system, there is considerable doubt

[22] Ibid at 4.
[23] Section 94(2) of the National Credit Act 34 of 2005.
[24] Code of Banking Practice of South Africa.
[25] Ruth Plato-Shinar op cit note 8 at 4.
[26] *Code of Banking Practice* supra note 24, cl 1 (preamble).
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ruth Plato-Shinar op cit note 8 at 5.
[31] Examples being Australia (ePayments Code) and the United Kingdom (the Payments Services Regulation 2017 (which implements the EU's PSD2)).
[32] Ruth Plato-Shinar op cit note 8 at 5.

as to whether the current approach in South Africa will successfully achieve this aim.[33] Moreover, the Code is exclusively applicable to banking institutions, thereby excluding non-bank financial service providers.[34] As the usage of digital payment methods continues to expand, with both domestic and international non-bank entities entering the market, it will be imperative to implement a more comprehensive solution that extends beyond the confines of the banking sector.

This research looks at the liability of banks with respect to unauthorised digital payments (or rather the lack of) – which has inevitably led to an inadequate consumer protection framework in South Africa in respect of unauthorised digital payments. This research begins by providing an analysis of digital payments under South African law; followed by a discussion of the nature of the bank-customer relationship and the reciprocal duty of reasonable care and skill; and lastly, a case is made for regulating unauthorised digital payments in South Africa by looking at the European Union's Payment Services Directive 2015/2366 (PSD2) which is legislation that is dedicated to the payments market in the EU.

II. THE TREATMENT OF UNAUTHORISED DIGITAL PAYMENTS UNDER SOUTH AFRICAN LAW

(a) *The nature of unauthorised digital payments in South Africa*

The advancement and expansion of technology over the years has led to the development of innovative payment methods that allow consumers to make remote payments.[35] One of the latest technological advancements are digital payments, which are sometimes referred to as electronic payments. An electronic payment refers to a payment method which is largely or completely effected by electronic techniques and technology.[36] This includes payments made with bank transfers, transfers effected through an automated teller machine (ATM), mobile money, QR codes, payment instruments such as credit, debit and prepaid cards, and transfers effected by way of a personal computer whereby the consumer is a registered user of Internet-banking services or through magnetic material such as magnetic tapes.[37]

Electronic fund transfers are effected by means of payment orders by a customer to his bank pursuant to the general bank and customer agreement or general mandate in terms of

[33] Ibid.
[34] Ibid.
[35] Ruth Plato-Shinar op cit note 8.
[36] WG Schulze 'The Reversal of Electronic Payments under South African Law: Possible Guidance from Recent Developments in European Union Law' (2020) 32(1) South African Mercantile Law Journal 24.
[37] Ibid.

which the bank is obliged to give effect to payment orders of the customer.[38] The common law of *mandatum* requires banks to exercise reasonable care and skill in the exercise of their mandate, and such mandate must be carried out within a reasonable time and without negligence.[39] The mandatary also has the duty to perform its mandate in good faith.

Moreover, the bank is obliged to install and maintain a reasonably efficient security system and to ensure that the system is operating efficiently.[40] The customer's common law duty is to draw his or her payment instruction with reasonable care, so that he or she does not facilitate fraud or deception.[41] Furthermore, the customer must ensure that the payment order is clear and unambiguous.

The risk of forgery and unauthorised payment[42] presents itself where a customer gives an oral or written instruction to his or her bank to effect an electronic transfer.[43] Where the payment instruction is expressed in a computer language, an electronic key is used to authenticate the message. This instruction or message can, in the absence of sufficient security measures, be altered, erased or transferred to another medium without this fact becoming known by examination of the medium.[44] A customer's bank card can also be lost or stolen and a third party who has knowledge of the PIN for the card will be able to use the card to make withdrawals or effect electronic transfers.[45] The ease with which fraud can be perpetrated where a bank card is used to effect an electronic transfer is one of the reasons why banks generally seek to protect themselves in the bank-customer agreement against liability for unauthorised payments.[46]

(b) *The regulatory framework governing unauthorised digital payments*

(i) Banks Act

Previously, the Banks Act[47] provided for the regulation and supervision of the business of public companies taking deposits from the public – this did not include the products and services (i.e. payment intermediary services) that banks offer to their consumers. This section

[38] Sharrock Robert *The Law of Banking and Payment in South Africa* 1st ed (2016) 368.
[39] Ibid.
[40] Ibid.
[41] Ibid.
[42] An unauthorised digital payment is one that has been executed without the consumer's (authorised user's) consent.
[43] Sharrock op cit note 38 at 370.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Section 3 of the Banks Act 94 of 1990.

of the Banks Act was repealed by the Financial Sector Regulation Act[48] (FSR Act) which introduced a new regulatory regime[49] that provides for the creation of a prudential and market conduct regulator. In terms of the FSR Act, the objective of the Prudential Authority is to promote and maintain safe and sound financial institutions that provide financial products and securities services, and to protect financial consumers from the risk of those institutions not being able to meet their obligations.[50] In order for the Prudential Authority to achieve its objective, it needs to regulate and supervise financial institutions that provide financial products or securities services in accordance with the financial sector laws.[51] A similar obligation is placed on the Financial sector Conduct Authority.[52] Thus, it can be inferred that the FSR Act has the overall function of regulating and supervising financial institutions, which includes digital payment service providers. However, it must be noted that these two regulators are not primarily concerned with the regulation of the intricate details of the contractual relationship between banks and their consumers – there are no detailed provisions regarding digital payments.[53]

(ii) Electronic Communications and Transactions Act (ECTA)

The Electronic Communications and Transactions Act[54] (ECT Act) provides a wide and general framework for the regulation and facilitation of electronic communications and transactions, which includes digital transactions for financial services. However, it does not extensively cover electronic banking services.[55] An "automated transaction," as defined by the ECT Act involves the use of data messages to execute a transaction without direct human review in normal business operations.[56] Typically, an 'electronic agent', 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, is involved in an automated transaction.[57] Thus, one could argue that a digital payment can be seen as a form of an automated transaction, as the platform used to make the payment functions automatically

[48] The Financial Sector Regulation Act 9 of 2017.
[49] This makes reference to the 'Twin Peaks' model of regulation.
[50] Section 33 of the FSR Act 9 of 2017.
[51] Section 34(1)(a)(i) of the FSR Act 9 of 2017.
[52] Section 5891)(a) of the FSR Act 9 of 2017 states that 'in order to achieve its objective, the Financial Sector Conduct Authority must regulate and supervise, in accordance with the financial sector laws, the conduct of financial institutions.
[53] Schulze op cit note 36 at 28.
[54] Electronic Communications and Transaction Act 25 of 2002.
[55] Schulze op cit note 36 at 28; there are many aspects pertaining to electronic payment methods that have not been dealt with.
[56] Section 1 of the ECT Act 25 of 2002.
[57] Ibid.

after being initiated by an electronic payment instruction.[58] Furthermore, the consumer protection provisions contained in the ECT Act primarily target consumers who buy goods or services by way of electronic transactions.[59] In particular, section 43(5) of the ECT Act requires suppliers to use a secure payment system aligned with technological standards at the time and specific transaction types. Section 43(6) outlines a supplier's liability for consumer damages resulting from non-compliance with subsection (5). Accordingly, bank consumers may enjoy protection from fraudulent activities encountered during an electronic transaction – subject to a bank qualifying as a supplier in terms of the ECT Act, considering that the term is not defined.

(iii) The National Payment Systems Act

The National Payment Systems Act[60] (NPS Act) provides for the management, administration, operation, regulation and supervision of payments, clearing and settlement systems in South Africa. Moreover, it provides a broad framework for payment and related systems – it too does not concern itself with the detail and operation of individual methods and instruments of payment.[61] There are no provisions that directly deal with digital payments or instruments.[62]

However, in terms of the NPS Act, the South African Reserve Bank may recognise a payment management body, established with the object of organising, managing and regulating the participation of its members in the payment system.[63] The Payments Association of South Africa (PASA) has been recognised by the South African Reserve Bank in this regard.[64] PASA is responsible for the management, regulation and organisation of its members, who are clearing participants.[65] PASA fulfils its mandate through its regulatory framework, issuance of rules, compliance monitoring and enforcement.[66] According to the PASA clearing rules, the processing of EFT transactions and other non-card transactions

[58] Section 20 of the ECT Act goes on to set out the provisions relating to automated transactions and the formation of agreements by using electronic agents.
[59] Section 43 of the ECT Act 25 of 2002 provides for the duties of suppliers who offer goods or services online, as well as the rights of consumers to cancel transactions in the event of non-compliance by suppliers.
[60] Act 78 of 1998.
[61] Ibid.
[62] Ibid.
[63] Section 3 of the National Payment System Act 78 of 1998.
[64] South African Reserve Bank Consultation Paper 'Processing of Payments in South Africa' available at *https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight-and-supervision/document-for-comments/Domestic%20Processing%20-%2014%20Nov%202018%20-publication.pdf*, accessed on 04 January 2024.
[65] Ibid.
[66] Ibid.

must be effected through an authorised processor – the issuing participant decides which authorised processor will process their transaction in accordance with the PASA rules.[67] Part of the reason for this, is to combat fraudulent activities that may be perpetuated through non-card transactions, by ensuring that only authorised processor's (i.e. Mastercard) can process such transactions.

(iv) The National Credit Act

The National Credit Act (NCA)[68] insofar as it deals with the issue of unauthorised digital payments, only applies to credit cards. Section 94(1) of the NCA states that if a credit facility allows for access to that facility by use of a card, personal identification code or similar identification device, the credit agreement must set out a contact telephone number at which the consumer may report the loss or theft of that card. Additionally, section 94(2) of the National Credit Act prohibits a credit provider from holding a consumer liable for any use of a credit facility after the time that the consumer has reported the loss or theft of the associated card, personal identification code or number or similar device. Furthermore, unless the consumer's signature appears on the voucher, sales slip, or similar record evidencing that particular use of the credit facility, or the credit provider has other evidence sufficient to establish that the consumer authorised or was responsible for that particular use of that credit facility, they cannot be held liable.[69]

(v) The Code of Banking Practice

The Code of Banking Practice is viewed as an important source of 'soft law' in the sphere of banking, focusing on managing the interactions between banks and their personal[70] and small business customers.[71] It is voluntary and has been collectively adopted by most banks operating in South Africa.[72]

In terms of the Code, a bank undertakes, *inter alia*, to: act fairly, reasonably and ethically towards its customers; make available information that is easy to understand concerning the bank's products; and to explain the financial implications and impact of the products and services offered. A bank must ensure that its staff: attends to transactions and

[67] Ibid.
[68] Act 34 of 2005.
[69] Ibid.
[70] A personal customer is defined in the Code as any individual who maintains an account or who receives other services from a bank.
[71] The Code came about as the result of a common perception that the banks in South Africa took advantage of the smaller customer.
[72] Schoeman Heidi *An Introduction to South African Banking and Credit Law* 2nd ed (2013) ch 2.

enquiries promptly; provides affordable and accessible basic banking services to all South Africans; and treats customer information as private and confidential. Moreover, a bank must ensure the compliance of its products and services with laws and regulations, and be guided by four key principles – fairness, transparency, accountability and reliability. Banks have a duty to provide customers with details of the Ombudsman for Banking Services if the customer is not satisfied with the resolution of any dispute between the bank and the customer.[73]

The Code covers various aspects relating to electronic payment services – it includes provisions in terms of which bank customers are required to take reasonable care when utilising digital payment methods as well as provisions pertaining to banks' responsibility for losses.[74] The Code states that the consumer will be liable for all losses if they have acted fraudulently – they may also be liable for losses if they have acted negligently or without reasonable care, which has caused or contributed to losses – this may apply if the consumer has failed to follow the safeguards set out in the Code.[75]

Furthermore, the consumer will be liable for losses if they have not informed the bank as soon as reasonably practicable after they discover or believe that their secret codes or devices, if any, for accessing the electronic banking services have been compromised, lost or stolen, or that unauthorised transactions have been conducted on their accounts.[76] Unless the bank can show that the consumer has acted fraudulently, negligently or without reasonable care, they will refund the consumer the amount of any transaction together with any interest and charges associated with the disputed transaction. This is particularly the case in specific circumstances and after consideration of all the facts. For example: (1) where the consumer has not received their card and it is misused by someone else; or (2) for all transactions not authorised or effected by the consumer after they have reported loss or theft of their card or chequebook or that their PIN may be compromised; or (3) if additional money is transferred from the customer's account to their electronic purse after they have informed the bank of its loss or theft and that someone else knows their PIN, password or unique means of personal identification; or (4) where system malfunctions have occurred in ATMs, or associated systems, which were not obvious or subject to a warning message or notice at the time of use;

[73] Ibid.
[74] Ibid.
[75] The South African Code of Banking Practice, cl 7.8.
[76] Ibid.

or (5) where a credit card transaction is disputed (the bank accepts the burden of proving fraud or negligence).[77]

However, the bank will not be liable for any losses caused by circumstances that are beyond their reasonable control. This includes situations such as: (1) a malfunction of any equipment (including telecommunications equipment) which supports ATMs and Internet, telephone or cell phone banking service; (2) the consumer's inability to access telephone or cell phone banking, or any other application associated or reliant on telephone or cell phone banking, at any time, or any failure or delay in providing a service via telephone or cell phone; or (3) a disruption of services caused by political actions or natural disasters.[78]

The Code provides a valuable set of safeguards for consumers in that it details how the banks, as members of the Banking Association of South Africa, are expected to deal with consumers.[79] However, the provisions of the Code are not enforceable in a court of law, and the Code cannot be used to interpret the legal relationship between and a bank and its consumer.[80] The Code also does not give rise to a tacit contract between a bank and its consumer, or to a banking custom.[81]

III. THE LIABILITY IMPOSED ON BANKS IN RESPECT OF UNAUTHORISED DIGITAL PAYMENTS

(a) The bank's liability in terms of the bank-customer contract

A person becomes a customer of the bank when they approach the bank with a deposit, request the bank to open an account in their name and the bank agrees.[82] This then results in a contractual relationship that is mainly one of debtor and creditor.[83] The customer is the creditor, and the bank the debtor, in relation to any amount standing to the credit of the customer's account.[84] As such, a deposit by the customer into his or her account is effectively a loan to the bank, which the bank can use immediately for its own purposes.[85] The bank-customer relationship is not solely based on contract – it further imposes additional duties on banks and

[77] Ibid.
[78] Ibid.
[79] Schoeman op cit note 72.
[80] Ibid.
[81] Ibid.
[82] Schoeman Heidi op cit note 72 at ch 1.
[83] Ibid.
[84] Ibid.
[85] Ibid.

customers alike.[86] These duties are established by banking practice and custom, legislation and court decisions.[87] The bank-customer relationship can thus be described as a contract *sui generis*, or a unique type of contract.[88]

The contractual relationship between a bank and its customer is mutually dependent and involves a shared duty of care.[89] Under common law, a duty of care is owed to any persons whom one can reasonably anticipate may suffer harm as a result of ones actions or inaction.[90] However, this duty only applies to harm that is foreseeable.[91] In *Absa Bank Ltd v Hanley*[92] Malan JA, in dealing with the reciprocal duties of a bank and its client, highlighted the unique nature of the bank-customer relationship, which functions as a debtor-creditor arrangement governed by contractual agreements. These agreements often involve multiple accounts and require the bank to provide specific services. When a bank processes transactions on behalf of a customer, it acts as a mandatary and is obligated to fulfil its duties promptly, in good faith and without negligence.

Where a bank enters into a formal agreement with a customer - such as for a 'smart banking account' - the relationship is governed by various legal and regulatory frameworks, including international banking standards and domestic laws.[93] Banks have both ethical and legal responsibilities to prevent financial crimes such as fraud, theft, money laundering and corruption.[94] These regulations make it clear that banks must neither participate in nor allow unlawful transactions under their supervision.[95] As a result, the contract between a bank and its customer plays a crucial role in defining their rights and obligations.[96]

With the increasing reliance on mobile and Internet banking, there has been a heightened emphasis on mitigating the risk of fraudulent activities in financial transactions. Both banks and their customers are subject to a duty of care in this regard.[97] This duty of care has long been recognised, with numerous cases outlining the respective obligations of each

---

[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] 2014 (2) SA 448 (SCA) para 25.
[93] *FirstRand Bank Ltd v Kgethile* (M370/2018) [2021] ZANWHC 63 (31 August 2021) para 41.
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Oliver Abel Smith 'Duties not to facilitate fraud' available at *https://www.fieldfisher.com/en/insights/duties-not-to-facilitate-fraud*, accessed on 17 March 2024.

party.[98] The scope of the duty of care owed by banks and their customers is primarily determined by the terms and conditions governing the bank account.[99] However, contractual terms that create a significant imbalance in the rights and obligations of the parties, to the detriment of the customer, are considered unfair and contrary to the principle of good faith.[100] As a result, a bank cannot entirely exempt itself from liability by unduly limiting its duty of care towards its customer.[101] The common law upholds this principle, affirming that both banks and their customers share a responsibility to prevent fraudulent activities.[102]

The case of *FirstRand Bank Ltd v Kgethile*[103] exemplifies the approach commonly adopted by banks in disputes involving unauthorised digital transactions, where liability is predominantly attributed to the customer, often to the exclusion of the bank's own negligence.[104] This judgment critically evaluates the contractual obligations between banks and their customers, the standard of care expected from both parties and the bank's responsibility in preventing financial crimes such as fraud and cybercrime.[105]

In this case, the respondent opened a Smart Account with the bank in terms of a written agreement, which provided that the respondent would use a debit card linked to the account to transact.[106] During October 2015, the respondent, believing he had a won a cash prize from an international entity, disclosed his banking details to a third party via a phishing scam.[107] Disputed transactions, amounting to R2.9 million, were purportedly executed over a period of two days, notwithstanding the fact that the customer's daily transaction limit had been set to R5000 - leading the bank to institute legal proceedings for repayment, alleging that the respondent fraudulently misused bank funds.[108]

The respondent denied liability, asserting that he was the victim of cybercrime and had not instructed the bank to process the transactions.[109] The bank relied on contractual terms that purported to shift liability onto the customer, arguing that the respondent's negligence in

[98] Ibid.
[99] Ibid.
[100] Ibid.
[101] Ibid.
[102] Ibid.
[103] *FirstRand* supra note 93.
[104] Ibid.
[105] Ibid.
[106] Ibid at 4 - 5.
[107] Ibid at 21 - 22.
[108] Ibid at 7 - 9.
[109] Ibid at 25.

disclosing his banking details made him responsible for the loss.[110] Furthermore, the bank asserted that its computer software, which is ordinarily designed to prevent unauthorised or unlawful payments, had a malfunction during the relevant period, thereby failing to detect and block the contested transactions.[111]

A crucial aspect of the agreement was the customer's obligation to review all account statement entries and promptly notify the bank of any discrepancies.[112] In accordance with the express, alternatively tacit and implied, material terms of the agreement, failure to report such discrepancies within 30 days of the statement date would result in the transactions being deemed accurate and authorised.[113] Consequently, the bank placed significant reliance on this contractual provision to substantiate its claim, asserting that the customer's conduct constituted a material breach of the agreement due to his failure to exercise due diligence.[114]

However, it is important to note that the bank itself contravened the terms of the agreement by extending a credit or overdraft facility to the customer, despite the account's explicit designation as a debit account.[115] Moreover, the bank failed to ensure that the contested transactions were executed with the requisite authorisation from the account holder.[116] Under the terms of the agreement, the only funds that should have been available for utilisation were those deposited into the account either by the customer or third party.[117]

While it is undisputed that the customer acted negligently by disclosing his personal and banking details, the bank failed to discharge the burden of proving that he had, in fact, authorised the transactions.[118] Furthermore, the bank's failure to detect and prevent the transactions due to an alleged system malfunction cannot be characterised as a mere technical failure but rather constitutes a material act of negligence.[119] Financial institutions bear an inherent duty to maintain secure and robust security systems to prevent fraudulent transactions.[120]

[110] Ibid at 30 - 31.
[111] Ibid at 14.
[112] Ibid at 5.
[113] Ibid.
[114] Ibid 8.
[115] Ibid at 7.
[116] Ibid at 33.
[117] Ibid at 32.
[118] Ibid at 53 - 54.
[119] Ibid at 41.
[120] Ibid.

In its determination, the court ultimately found that both the bank and the customer had been negligent and/or careless in the performance of their respective contractual obligations.[121] By holding the bank accountable for its system failures, this case reinforces the fact that banks must actively mitigate risks rather than shifting responsibility onto customers. This decision underscores the necessity of a balanced assessment of liability in such cases, rather than an approach that disproportionately attributes fault to the customer while disregarding deficiencies on the part of the financial institution.

(b) The bank's duty to exercise reasonable care and skill

The bank is under a general obligation to the customer to exercise reasonable care and skill in the performance of its duties.[122] The duty extends to a wide range of banking business within the bank-customer contract.[123] Banks are required to adhere strictly to their customers' payment instructions by issuing corresponding payment orders that accurately reflect those provided by the customer. The circumstances under which a bank may lawfully refuse to execute a payment order are limited. In such instances, the bank is obligated to notify the customer at the earliest possible opportunity and, where feasible, provide a rationale for its refusal.[124] Additionally, banks are entitled to decline a payment order if the customer has contravened the agreed-upon terms and conditions governing the account. Examples of such breaches include the failure to provide the requisite two signatures for a joint account transaction or instances where executing the payment would constitute an unlawful act.[125]

However, a bank's duty to comply with a customer's payment instructions may at times conflict with its obligation to exercise reasonable care and skill in protecting the customer from fraudulent acts committed by third parties.[126] This conflict arises when a bank receives what appears to be an authorised payment order, but which, in reality, has been executed as a result of fraudulent activity. Such situations raise critical questions regarding the extent of the bank's duty of care in verifying the authenticity of payment instructions.[127] A bank is only authorised to process a payment or debit a customer's account if it can demonstrate that the customer's consent was obtained.[128] The method and procedure for granting such consent must be clearly

[121] Ibid at 60.
[122] Schoeman Heidi op cit note 72 at ch 1.
[123] Ibid.
[124] Oliver Abel Smith op cit note 97.
[125] Ibid.
[126] Ibid.
[127] Ibid.
[128] Ibid.

outlined in the information provided to the customer prior to the execution of any transaction.[129] If the bank is unable to establish that consent was given, the transaction must be classified as unauthorised.[130] Consequently, if a third party were to gain access to a customer's electronic payment device or circumvent authentication measures to issue payment instructions to the bank, the bank's duty to determine whether it had the requisite consent to process the transaction would depend on the specific terms of the contract governing the relationship between the parties.[131]

Relevant considerations in deciding whether the bank has breached this duty are the practices customarily adopted by banks in similar circumstances, the time available to the bank for making a decision, and the extent to which the particular task or operation was unusual or out of the ordinary course of business.[132] In *Mccarthy Ltd v Absa Bank Ltd*[133] Nugent JA articulated the duty of care incumbent upon banks, stating that a bank is obligated to honour cheques drawn by its customer, provided that they are authentic, complete in all respects and that the customer's account contains sufficient funds or an available line of credit to cover the payment. Furthermore, in executing such transactions, the bank is required to adhere strictly to the customer's instructions and to discharge its duties with the requisite standard of care. This obligation necessitates that the bank acts in good faith and without negligence in the processing of payments.

(c) The customer's duty to exercise reasonable care and skill

A customer also has a duty of care towards their bank, which encompasses several obligations, including: the duty to avoid issuing cheques or other payment instructions in a manner that could facilitate fraud or forgery; and the duty to promptly notify the bank if they become aware of any forgery involving a cheque.[134] Although these duties were initially articulated in the context of cheque transactions, they are equally applicable to payment orders made through any medium.[135]

---

[129] Ibid.
[130] Ibid.
[131] Ibid.
[132] 'Business Transactions Law' available at *http://jutastat.juta.co.za/nxt/gateway.dll/btrl/99/217/222?f=templates$fn=default.htm*, accessed on 18 March 2024.
[133] [1972] 1 W.L.R 602, (1972) All ER 1210 para 22.
[134] Oliver Abel Smith op cit note 97.
[135] Ibid.

In *Absa Bank Ltd v Hanley*, Malan JA addressed the duty of care owed by a customer to their bank, stating that the customer must exercise reasonable care in issuing payment instructions, in order to prevent forgery or alterations, and must notify the bank of any known or suspected fraud or forgery. This duty extends beyond cheques to include telegraphic transfers, with the same principles governing both. The same obligations apply when the payment instruction involves an application for an overseas credit transfer, as in this case. The court further emphasised that a customer owes a duty to his banker to draw his cheques with reasonable care in order to prevent forgery. However, the customer's duty is limited - apart from ensuring that documents presented to the bank are properly drawn and alerting the bank to known or suspected forgeries, the customer has no responsibility to supervise employees, manage their business operations carefully or detect fraud. This customer's negligence or carelessness must be the proximate cause of the bank being misled, and this negligence must be evident in the transaction itself, in the manner the cheque or payment instruction was drawn. If circumstances justify, a bank is obligated to make inquiries before processing a payment. Should a bank choose not to inquire into unusual circumstances for fear of offending the customer, it assumes the risk of liability for failing to make such inquires.[136]

IV. THE EXTENT TO WHICH BANKS ARE HELD LIABLE IN CASES OF UNAUTHORISED DIGITAL PAYMENTS

Given the fact that the use of electronic transfers and other forms of digital payments (including Internet payments) are not regulated by legislation, banks are able to unilaterally determine the rules and conditions that apply to these types of transactions.[137] They are thus able to curtail their liability for unauthorised payments through certain provisions in the bank-customer contract (in terms of which the risk for loss due to an unauthorised payment as a result of theft or fraud is largely allocated to the customer) as long as these provisions are not in conflict with the legislation as discussed above.[138]

This is also evident in the Code where most of the liability is placed on the consumer, but for a few exceptions where the payment service provider bears the loss. The Code was

[136] *Absa* supra note 92 para 26.
[137] Sharrock op cit note 38 at 370.
[138] Ibid.

inspired by the fault model[139] imposing liability on the consumer wherever he or she acted negligently (and not, necessarily, grossly negligently). Similarly, it imposes liability on the service provider where the loss may be attributed to its own negligence.[140] The Code impliedly reinforces the measures taken by banks to protect themselves against liability in the context of electronic funds transfers – however, the extent to which these provisions will be binding in a court of law is uncertain. Generally, if a bank transfers funds from its consumer's account without the consumer's authorisation, it breaches its mandate and can be held contractually liable.[141]

However, given the lack of governing legislation, the bank-customer agreement will generally govern the liability of the bank for unauthorised digital payments and will have to be consulted in order to determine whether it indemnifies the bank regarding such payments or otherwise allocates the risk of loss to the consumer.[142]

V. THE EUROPEAN UNION'S APPROACH TO E-PAYMENTS

(a)The nature and treatment of digital payments in the European Union

The European Union (EU) has introduced legislation that forms the legal basis for a unified payments market, with the goal of fostering safer and more innovative payment services across the EU.[143] The primary objective was to make cross-border payments as seamless, efficient and secure as possible.[144]The Payment Services Directive 1 (PSD1) laid the legal groundwork for payment services across the EU, aiming to enhance transparency and information for consumers, bolster refund rights and clarify the rights and obligations of both consumers and payment institutions.[145] However, under PSD1, significant segments of the payments market - particularly card, Internet and mobile payments - remained fragmented along national borders. Many innovative payment products and services did not fall entirely within the scope of

[139] According to the fault model, the loss is borne by the party whose negligence caused the damage. If several parties have been negligent, the damage is apportioned among them according to the degree of their negligence. The fault model is based on civil procedure and it involves issues such as contributory negligence, the duty to mitigate loss, the validity of liability exemption clauses.
[140] Ruth Plato-Shinar at 8.
[141] Sharrock op cit note 38 at 373.
[142] Ibid.
[143] European Commission available 'Payment Services Directive: frequently asked questions' at *https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5793*, accessed 12 April 2024.
[144] Ibid.
[145] Papadopoulos, S 'A consumer's case for regulating electronic credit and debit transfers in South Africa' (2018) International Journal of Private Law 46.

PSD1.[146] Additionally, the scope of PSD1, and particularly the areas excluded from its coverage, such as certain payment-related activities, proved to be vague, overly broad or outdated.[147] This inevitably led to legal uncertainty, potential security risks within the payment chain and a lack of consumer protection in some areas.[148] Furthermore, it became challenging for payment service providers to introduce innovative, secure and user-friendly digital payment services, as well as to offer consumers and retailers effective, convenient and safe payment methods.[149]

(b) EU's current legislative framework governing unauthorised digital payments

Recognising the emerging trends in the payment industry, notably fuelled by the widespread adoption of data-driven technologies, the EU ratified the Second Payment Services Directive (PSD2) on October 8, 2015.[150] This directive establishes the legal framework for advancing and enhancing various aspects of electronic payments within the EU.[151] The primary goals of PSD2 are to promote a more integrated and efficient European payments market, create a level playing field for payment service providers, enhance payment security, protect consumers and encourage reduced costs.[152] To achieve these goals, PSD2 broadens the scope of its application by encompassing new services and expanding the coverage of existing services.[153] Additionally, it revises the telecom exemption under PSD1, restricting it primarily to micro-payments for digital services and includes transactions with third world countries only when the payment service provider is based within the EU.[154] More specifically, the Revised Payment Services Directive aims to:[155]

i. Reduce and manage industry fraud rates without negatively impacting customer experience while increasing consumer trust;
ii. Develop two-factor authentication to improve the process. PSD2 requires SCA for all European e-commerce transactions beginning on December 31, 2020;

[146] Ibid.
[147] Ibid.
[148] Ibid.
[149] Ibid.
[150] Gounari et al "Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards" 2024 *International Cybersecurity Law Review* 80.
[151] Gounari et al 2024 International Cybersecurity Law Review 80.
[152] Papadopoulos op cit note 145.
[153] Ibid.
[154] Ibid.
[155] Gounari et al op cit note 150 at 82.

iii. Provide more online banking and payment options for e-commerce customers as EU payment markets open to new entrants. The emergence of Third Party Providers will drive payment innovation and competition;
iv. Demand greater clarity and transparency in the fine print of e-commerce application licensing agreements;
v. Reduce consumers' liability for unauthorized payments and institute an 8-week unconditional ("no questions asked") refund right for direct debits in euros;
vi. Ensure that when a transaction is completed, card issuers make all banking funds available;
vii. Prohibit surcharging, which is the practice of charging additional fees for payments made with consumer credit or debit cards in stores or online; and
viii. Improve the complaints procedure because it requires organizations to accept and resolve complaints in a timely manner using predefined methods.

In a notable departure from its predecessor, PSD2 broadened the regulatory scope of Internet payment services to include new and innovative market players.[156] Specifically, PSD2 introduced two new types of services: account information services (AIS) and payment initiation services (PIS).[157] Payment initiation service providers (PISPs), such as PayPal, Sofort, iDeal, and Tikkie, are now authorised to initiate payment orders directly from a user's bank account at the user's request.[158] The PSD2 aims to protect consumers against fraud and other abuses with improved security measures in place. The payment service provider (PSP) has to carry out an assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation of measures implemented on a yearly basis.[159] The PSP has to ensure that the personalised security features of a payment instrument are not accessible to parties other than the payment service user (PSU) entitled to use the instrument and as a corollary requirement the PSU must take all reasonable steps to keep security credentials safe.[160]

In addition, the PSP must refrain from sending an unsolicited payment instrument, except if the payment instrument has to be replaced, and they are to ensure that there are appropriate means available at all times for the PSU to notify the PSP of any loss, theft or

[156] Gounari et al op cit note 150 at 81.
[157] Ibid.
[158] Ibid.
[159] Papadopoulos op cit note 145 at 47.
[160] Ibid.

misappropriation of the payment instrument or of its authorised use.[161] This includes an obligation on the PSP to provide the PSU with the means to prove, for 18 months after notification, that he/she has made such notification.[162] Finally, the PSP must prevent all use of the payment instrument once notification has been made under Article 69(1)(b), and carries the risk of sending a payment instrument or any personalised security features to the PSU.[163]

Article 71 allows a PSU to request the rectification of an unauthorised or incorrectly executed payment transaction from a PAP within 13 months of the debit date, provided that the PSU notifies the PSP without undue delay once the issue is identified.[164] Additionally, member states are required to ensure that when a PSU denies authorising a payment or asserts that the transaction was not correctly executed, the PSP bears the burden of proving that the transaction was authenticated, accurately recorded, entered into the correct account and not affected by a technical failure or any other deficiency.[165] The mere use of a payment instrument recorded by the PSP is not, by itself, sufficient to establish that the payment was authorised by the PSU or that the PSU acted fraudulently or with gross negligence.[166] In terms of the potential losses incurred by the PSU, the rules stipulate that, except in cases of fraud or gross negligence, the maximum amount a payer could lose in the event of an unauthorised transaction is €50.[167] The amount must be refunded immediately or, if it is not possible, it must be refunded no later than the end of the following business day, unless the PSP has reasonable grounds to suspect fraud on the part of the PSU, in which case the suspicion must be communicated in writing to the relevant national authority.[168] Furthermore, if the PSP does not require strong customer authentication, the PSU will not bear any loss.[169]

In cases where the transaction amount is not known in advance, PSD2 allows the PSP to block funds on the payer's payment account only if the payer has consented to the exact amount to be blocked.[170] The payer is entitled to a refund from the PSP for an unauthorised transaction initiated by or through a payee, which has already been executed, provided the following conditions are met: (1) the authorisation did not specify the exact amount of the

[161] Ibid.
[162] Ibid.
[163] Ibid.
[164] Ibid.
[165] Ibid at 48.
[166] Ibid.
[167] Ibid.
[168] Ibid.
[169] Ibid.
[170] Ibid.

payment transaction at the time the authorisation was granted; (2) the amount of the payment transaction exceeds what the payer could reasonable have expected, considering factors such as the payer's previous spending patterns, the terms of the framework contract and the relevant circumstances of the case.[171] Upon the PSP's request, the payer must bear the burden of proving that these conditions are satisfied. The refund must consist of the full amount of the executed payment transaction.[172] Additionally, the credit value date for the payer's payment account must be no later than the date on which the amount was debited.

A payment order becomes irrevocable once it is received by the PSP or at the time agreed upon by the parties.[173] According to Article 83, the payer's PSP is required to ensure that, after the receipt time specified in Article 78 has passed, the amount is credited to the payee's PSP by the end of the following business day. If the transaction is initiated by paper, this period is extended by an additional day.[174] Furthermore, the payee's PSP must also make the amount available to the payee immediately after the funds are credited to the payee's PSP.

In the event of incorrect unique identifiers, PSD2 assigns liability to the payer as outlined in Article 88. It states that if a payment order is executed based on a unique identifier, the transaction is considered to have been correctly executed to the payee identified by the unique identifier. If the unique identifier is incorrect, the PSP is not liable under Article 89 for the defective execution. However, the PSP is obligated to make reasonable efforts to assist in recovering the mistakenly transferred funds. If recovery is not possible, the PSP must provide all necessary information to the payer's PSP to enable the payer to pursue a legal claim for the recovery of the funds.[175]

It is clear that PSD2 widens the scope of PSD1 by incorporating new services and participants, as well as by extending the reach of existing services, such as payment instruments issued by payment service providers that do not manage the payment service user's account, thereby allowing their access to pay accounts.[176] Additionally, in order to enhance the safety and security of payments, PSD2 introduces stricter security measures to be implemented by all payment service providers, including banks.[177] PSD2 specifically mandates that payment service providers apply strong customer authentication for electronic payment transactions as

[171] Ibid.
[172] Ibid.
[173] Ibid.
[174] Ibid.
[175] Ibid.
[176] European Commission op cit note 143.
[177] Ibid.

a general rule.[178] In this regard, the European Commission has established rules outlining the application of strong customer authentication.[179]

The Directive clearly reflects a strong effort to harmonise payment principles across the EU, with explicit delineation of the obligations of both PSUs and PSPs. This level of clarity is something that South African regulation currently lacks and is in urgent need of.[180]

The Directive has provided a significant amount of advantages to the European economy by facilitating access for new market participants and payment institutions, thereby fostering increased competition and consumer choice.[181] It has also contributed to economies of scale and supported the practical implementation of the Single Euro Payments Area (SEPA).[182] PSD1 has enhanced transparency and information for consumers, reduced execution times, bolstered refund rights and clarified the liabilities of both consumers and payment institutions.[183] A notable benefit is that payments within the EU are now more efficient and expedited, with transactions typically credited to the recipient's account the following day.[184]

VI. THE LACK OF LEGISLATIVE PROTECTION FOR CONSUMERS: A CASE FOR REGULATING UNAUTHORISED DIGITAL PAYMENTS IN SOUTH AFRICA

The lack of legislation dedicated towards the regulation of digital payments raises serious consumer protection concerns.[185] Where a consumer gives a written instruction for an electronic funds transfer in a manner that facilitates fraud and the manner in which the payment instruction is drawn is the proximate cause of his or her loss, the common law and generally also the bank-customer agreement dictate that the consumer will have to bear the loss.[186] The bank-customer agreement generally also provides that if the proximate cause of the unauthorised payment was that the client lost their card or their card was stolen and they failed to report such loss or theft timeously (that is, before any unauthorised transfers or withdrawals

[178] Ibid.
[179] Ibid.
[180] Papadopoulos op cit note 145 at 49.
[181] European Commission op cit note 143.
[182] Ibid.
[183] Ibid.
[184] Ibid.
[185] Sharrock op cit note 38 at 373.
[186] Ibid.

are made) to the bank, then they bear the risk for the subsequent loss of money.[187] The same applies where the customer does not guard their PIN with the result that a third party who has acquired knowledge of the PIN makes unauthorised transfers or withdrawals from the customer's account.[188] In the aforementioned instances and also where the customer was aware of a forgery or unauthorised payment instruction but failed to warn the bank timeously thereof, the customer will not be able to hold the bank liable for their loss.[189] This will also be the situation where the customer subsequently ratified an unauthorised payment instruction.[190]

Consumers are at a serious disadvantage when it comes to smart cards, electronic money and electronic fund transfers – banks and other service providers have sought to protect themselves against the risks associated with these payment methods, which has left the consumers to carry the burden. The liability for loss incurred as a result of unauthorised digital payments is mainly governed by the Code and the contract that the consumer enters into with the bank – both are drafted by the banks and they offer very little protection to consumers.[191] Banks dictate the terms upon which they will provide these services without any input from their customers or other consumer protection organisations.[192] The customer is therefore left with no choice but to accept these terms if they want to make use of the services, even though a large portion of the risk is allocated to them.

Banks need to counter the increase in fraud and ensure consumers and merchants are protected against cyber and data risks – to achieve this, they need to continuously implement security systems, data integrity and business continuity processes.[193] Examples of processes and security by the banks to protect their consumers against fraudulent and suspicious activities includes: processes that trigger an alert for any suspicious activity; data encryption; and Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA).[194]

There are various safety and security measures to ensure that customer data is protected.[195] This includes: (1) performing regular reverse-image and unique phrase searches to identify any potential rogue website clones; (2) educating consumers about how to spot

[187] Ibid.
[188] Ibid.
[189] Ibid.
[190] Ibid.
[191] Ruth Plato-Shinar op cit note 8.
[192] Ibid.
[193] Ozow op cit note 1.
[194] Ibid.
[195] Ibid.

phishing sites; (3) securing access to platforms via strong password authentication; (4) segregating testing environments from production environments, reviewing any access to systems and components regularly, and logging and auditing actions by users; (5) using data theft protection solutions to detect and prevent confidential and personal information being leaked; and (6) putting mobile device management solutions in place, enforcing encryption and providing remote wiping and monitoring capabilities.[196]

In order to increase public confidence in the modern payment instruments, a broad protection should be afforded to users of these instruments.[197] The law should move towards having the financial institutions absorb the loss because they have a duty to implement a payment system that is secure and they have the means to mitigate/ensure secure systems.[198] South African law needs consumer legislation governing the extent of liability for each party in an electronic fund transfer, and limitations need to be imposed in order to protect the consumer.[199] Digital payments legislation should provide for: detailed duties of disclosure on providers of electronic fund transfer services; liability for unauthorised transactions; the legal nature of a credit transfer, including time of payment; and the balancing of consumer's interests.[200] It is in the banks own best interests to deal with the legal uncertainty around credit transfers – it promotes transparency and is sound business practice.[201] A notable example of specialised legislation governing electronic funds transfers is the European Union's Payment Services Directive 2015/2366 (PSD2). It is recommended that jurisdictions seeking to enhance the security and regulatory framework of digital payment systems consider adopting similar comprehensive legislative measures.

VII. CONCLUSION

The on-going technological advancements have significantly increased the use and benefits of digital payments. As such, the 'traditional payments' legislation, which largely focused on paper-based instruments, has been rendered inadequate to deal with the challenges brought forth by digital payments. Whilst other jurisdictions have combatted this issue by adopting dedicated legislation, South Africa has not done this. This has inevitably led to one-sided

[196] Ibid.
[197] Ibid.
[198] Papadopoulos op cit note 145 at 45.
[199] Ibid.
[200] Ibid.
[201] Ibid.

contracts between banks and consumers, whereby the consumer carries the largest portion of the risk.

In conclusion, the liability of banks for unauthorised digital payments in South Africa is a multifaceted issue that requires a comprehensive understanding of the regulatory landscape, contractual agreements, and the practical aspects of dispute resolution. While the existing legislative framework provides a foundation, continuous efforts are needed to address emerging challenges and adapt to the evolving nature of digital threats. Through a combination of robust regulations, effective enforcement, and collaborative efforts between banks, regulatory bodies, and consumers, South Africa can strengthen its position in safeguarding against unauthorised digital payments and promoting a secure digital financial environment.

Until South Africa adopts legislations dedicated to digital payments, reliance will have to be placed on the common law, as developed by our courts, and the certain parts of legislation that somewhat finds application. It is recommended that South Africa considers implementing legislation similar to the PSD2, that covers all aspects of digital payments.

VIII. BIBLIOGRAPHY

LEGISLATION

National Credit Act 34 of 2005.

Banks Act 94 of 1990.

Financial Sector Regulation Act 9 of 2017.

Electronic Communications and Transaction Act 25 of 2002.

National Payment System Act 78 of 1998.

The South African Code of Banking Practice

CASES

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

FirstRand Bank Ltd v Kgethile (M370/2018) [2021] ZANWHC 63 (31 August 2021)

Mccarthy Ltd v Absa Bank Ltd [1972] 1 W.L.R 602, (1972) All ER 1210.

ABSA Bank Ltd v Hanley [2014] All SA 249.

ABSA Bank Ltd v Lombard Insurance Co Ltd 2012 (6) SA 569 (SCA).

Diners Club Ltd v Singh 2004 (3) SA 630 (D).

Pestana v Nedbank Ltd 2008 (3) SA 466 (W).

Pestana v Nedbank Ltd [2006] ZAGPHC 113 (29 May 2009).

Nedbank Ltd v Pestana [2009] 2 All SA 58 (SCA).

Nissan South Africa (Pty) Ltd v Marnitz (Stand 186 Aeroport (Pty) Ltd Intervening) 2005 (1) SA 471 (SCA).

Take & Save Trading CC v The Standard Bank of SA Ltd 2004 (1) SA 597 (SCA).

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

BOOKS

Schoeman Heidi *An Introduction to South African Banking and Credit Law* 2nd ed (2013).

Sharrock Robert *The Law of Banking and Payment in South Africa* 1st ed (2016).

Malan, Pretorius & Du Toit *Bills of Exchange, Cheques and Promissory Notes* (5th ed) 2009.

ARTICLES

Gounari et al 'Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards' (2024) *International Cybersecurity Law Review*.

S Cornelius 'The legal nature of payment by credit card' (2003) *South African Mercantile Law Journal*.

VA Lawack 'Electronic innovations in the payment card industry' (1998) *South African Mercantile Law Journal*.

Ruth Plato-Shinar ‘Regulating liability for unauthorised digital payments: Insights for South Africa’ (2020) *Annual Banking Law Update.*

WG Schulze ‘The Reversal of Electronic Payments under South African Law: Possible Guidance from Recent Developments in European Union Law’ (2020) 32(1) *South African Mercantile Law Journal*.

WG Schulze 'Countermanding an electronic funds transfer: The Supreme Court of Appeal takes a second bite at the cherry' (2004) 16 *South African Mercantile Law Journal* 668.

WG Schulze 'Electronic funds transfers and the bank's right to reverse a credit transfer: one small step for banking law, one huge leap for banks' (2007) 19 *South African Mercantile Law Journal* 379.

WG Schulze 'Duty of a Bank to Act with Necessary Skill and Care when Issuing an Automated Teller Machine Card' (2007) *De Jure* 371.

WG Schulze 'Smart cards and e-money: new developments bring new problems' (2004) *South African Mercantile Law Journal*.

MD Tuba 'The regulation of electronic money institutions in the SADC region: some lessons from the EU' (2014) *Potchefstroom Electronic Law Journal*.

Papadopoulos, S 'A consumer's case for regulating electronic credit and debit transfers in South Africa' (2018) *International Journal of Private Law*.

Pretorius 'Aspects of the collection of a cheque cleared through an Automated Clearing Bureau' (1998) 10 *South African Mercantile Law Journal* 260.

INTERNET RESOURCES

Ozow 'Fraud within the payment industry in South Africa' available at *https://ozow.com/white-paper/fraud-within-the-payment-industry-in-south-africa*, accessed on 07 January 2024.

South African Reserve Bank Consultation Paper 'Processing of Payments in South Africa' available at *https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight-and-supervision/document-for-comments/Domestic%20Processing%20-%2014%20Nov%202018%20-publication.pdf*, accessed on 04 January 2024.

Oliver Abel Smith 'Duties not to facilitate fraud' available at *https://www.fieldfisher.com/en/insights/duties-not-to-facilitate-fraud*, accessed on 17 March 2024.

'Business Transactions Law' available at *http://jutastat.juta.co.za/nxt/gateway.dll/btrl/99/217/222?f=templates$fn=default.htm*, accessed on 18 March 2024.

European Commission 'Payment Services Directive: frequently asked questions' available at *https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5793*, accessed 12 April 2024.