COUNTERFEIT CARD FRAUD: IS THERE A NEED TO INTRODUCE LEGISLATION TO FACILITATE THE PROSECUTION OF RELATED CRIMINAL ACTIVITIES?

by

GERDA FERREIRA

A dissertation submitted as partial fulfilment for the MAGISTER LEGUM

in

Banking Law

in the

Faculty of Law

at the

University of Johannesburg

Supervisor: Prof. D.S. de Villiers

2012

SUMMARY

Despite payment cards being of a fairly recent origin,[1] these instruments of payment play an increasingly significant role in commerce. With reference to credit cards, Cornelius already in 2003 stated: "They fulfil various functions that are increasingly important at a time that e-commerce is taking off at a tremendous pace."[2] Similarly criminals continuously use more inventive and technologically advanced methods to commit fraud, including counterfeit card fraud. Is the South African criminal law, however, keeping up?

The aim of this study is to investigate whether the various activities which form part of the criminal business value chain relating to counterfeit card fraud, with specific reference to bank payment cards, are sufficiently criminalised in South Africa or whether the inability of our criminal law to address the challenges posed by this crime type necessitates the introduction of further legislation.

In the first part of the dissertation the South African common and statutory criminal law is investigated in some depth to establish the applicability thereof on the activities forming part of the criminal business value chain relevant to counterfeit card fraud. The appropriateness of certain statutory provisions is questioned and recommendations are made to amend current legislation. An argument is also advanced for further development of the common-law offence of theft to include identity theft and the unlawful copying and subsequent use of data. Brief reference is made to the international situation.

Chapter 2 is an introduction to bank payment card fraud in South Africa focusing on the most prevalent forms thereof being card-not-present fraud and counterfeit card fraud. Reference is made to the manner in which offences related to counterfeit card fraud are currently approached in our criminal courts and the limited impact prosecutions has on the prevalence of this fraud type.

[1] See Otto "Credit card transactions and a spouse's consent in terms of the Matrimonial Properties Act" 1997 *TSAR* 216.
[2] Cornelius "The legal nature of payment by credit card" 2003 *SA Merc LJ* 153.

Finally the criminal business value chain related to counterfeit card fraud is set out and analysed with the objective to identify the different key activities which ought to be criminalised.

It is concluded that prosecutions of counterfeit card fraud related matters could be facilitated by either the introduction of specific legislation or the amendment of current statutory provisions. However, appropriate use of the current South African criminal law would already result in convictions and sentences with a deterring impact.

TABLE OF CONTENTS

CHAPTER 1

THE SOUTH AFRICAN CRIMINAL LAW

1 *Introduction*

The South African criminal law offers a variety of common-law and statutory offences which could be applied to prosecute a number of the activities involved in the business value chain of counterfeit card fraud.[3]

Unlike some overseas' jurisdictions, there is, however, no specific or dedicated legislation in South Africa covering credit card or other payment card schemes.[4] All the criminal activities related to this crime type are also not currently catered for in our criminal law.

During his presentation at the opening of the academic year at the University of Port Elizabeth on 3 February 1984 Eksteen argued as follows in favour of the application, and where appropriate the adaptation, of the common law when dealing with technology-driven offences:

> "It seems to me that it is eminently desirable that these novel problems posed by the advent of computers to which I have referred should, so far as is possible, be resolved by the application or adaptation of the principles of our Roman-Dutch law rather than by resorting to legislation which almost invariably presents problems of its own."[5]

As we will argue later, however, the introduction of further legislation should be considered to criminalise the remaining activities not sufficiently catered for and to simplify the related prosecutions.

---

[3] For a discussion of the business value chain of counterfeit card fraud see ch 3 below.

[4] Schulze "Of credit cards, unauthorised withdrawals and fraudulent credit-card users" 2005 *SA Merc LJ* 202 210. In the United States card fraud, including counterfeit card fraud, is covered by s 916 of the Electronic Fund Transfer Act of 1978 (15 USC 1693 *et seq*). The United Arab Emirates enacted the Cybercrimes Act, Law no 2 of 2006, which *inter alia* prohibits credit card fraud. In this regard see Cassim "Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study" 2009 *PER* 36 53. Although the African Union Commission *Draft African Union convention on the establishment of a credible legal framework for cyber security in Africa* 2011 contains various provisions aimed at combating cybercrime, including a number of suggested offences specific to information and communication technologies, no recommendations are made specific to payment card fraud. The recommendations include suggestions that the use of information and communication technology to commit common law offences such as theft and fraud should be considered as aggravating circumstances. The convention has not been adopted yet.

[5] "Die bydrae van akademici tot die regspleging" 1984 *Obiter* 1 4.

2 *Common law offences*

2.1 Theft

Theft is the most basic crime against property. Burchell describes theft as "an unlawful appropriation with intent to steal of a thing capable of being stolen".[6]

The essential nature of theft has evolved from the original secretive "taking" and "carrying away" of property from the possession and control of the owner, to a wider notion of depriving an owner of his or her interests in the property, whether by carrying it away or by other devices.[7]

In Roman law theft was not limited to the actual taking of property (*furtum rei*), but included the unauthorised use of a thing (*furtum usus*) and the unauthorised acquiring of the possession of a thing (*furtum possessionis*).[8]

The South African law of theft is based on a mixture of Roman-Dutch law and English law. English law not only determined our law relating to the theft of trust money, but is also the source of the definition of the fault element of the crime, namely the intention to steal.[9]

Snyman differentiates between four different forms of theft, one of which is the theft of credit.[10] The essential elements of theft, applicable to all forms of the crime, are appropriation, property, unlawfulness and intent.[11]

2.1.1 The elements of theft and counterfeit card fraud

2.1.1.1 Conduct (appropriation)

Roman and Roman-Dutch law defined this element essentially as the mere handling (*contrectatio*) of the property without it necessarily being removed from the control of the

---

[6] Burchell *Principles of Criminal Law* (2005) 782. For a more involved definition of theft and a discussion of the different ways in which the crime has been defined in case law and legal literature, see Snyman *Criminal law* (2008) 483 ff.
[7] Burchell (n 6) 782.
[8] Burchell (n 6) 783.
[9] Burchell (n 6) 785.
[10] Snyman (n 6) 486 and 487.
[11] Burchell (n 6) 785 and Snyman (n 6) 484.

owner.[12] This very wide concept was interpreted so strictly that it would have excluded incorporeal things like shares and data, since such property could not be touched or handled.

In the South African law the *contrectatio* concept was also adopted as the definition of the "taking" element of theft requiring the assumption of control of property belonging to another.[13] Through judicial interpretation the concept acquired a wider content than it had in the Roman and Roman-Dutch law. Although our courts yet have to clearly define what amounts to an "assumption of control", our law has developed to the stage where *contrectatio* is possible in respect of an incorporeal thing, such as shares,[14] and in respect of money the *contrectatio* condition would be met if a computer is instructed to transfer the money to an account other than that of the owner.[15]

One can only welcome the development of the common law to a stage where our courts explicitly recognised the appropriation of personal rights as constituting theft.[16] As correctly pointed out by Burchell,[17] the highly restrictive earlier interpretation does not meet the requirements of a modern industrialised capitalist economy where wealth is increasingly found in incorporeal things and where the transfer of property is more often achieved by instructions to computers and book-entries than by the physical handing over thereof.

In 1975 Snyman already expressed the following view:

> "*Contrectatio* was miskien 'n bevredigende maatstaf in die samelewing van 'n paar eeue gelede met sy byna primitiewe ekonomie wat hoofsaaklik op die landbou geskoei was. In die moderne samelewing met sy ingewikkelde ekonomiese struktuur is die meer abstrakte toe-eieningsbegrip veel beter as die *contrectatio*-begrip in staat om te beskryf wat presies by die diefstalhandeling gebeur, tensy 'n mens die oorspronklike betekenis van die laasgenoemde term oorboord gooi en dit slegs gebruik as 'n tegniese "geleerde woord" om die diefstalhandeling te beskryf. So 'n metode het egter die nadeel dat dit een van die kernvrae by diefstal, nl die vraag welke handelinge diefstalhandelinge is, omseil en misken. Misdaadomskrywings behoort, veral vir die leek, so helder en verstaanbaar as moontlik te wees en juis daarom is 'n omskrywing van diefstal in die voetspoor van die toe-eieningsbegrip ("die wederregtelike

---

[12] Burchell (n 6) 786.
[13] Burchell (n 6) 786.
[14] *Milne and Erleigh (7)* 1951 1 SA 791 (A).
[15] In *Van den Berg* 1991 1 SACR 104 (T) 106 the court held that "the fact that the misrepresentation was introduced into the computer system electronically differs not one whit from the clerk who, with the intention to deceive, makes a false entry with a pen into a ledger account".
[16] Ebersöhn "A common law perspective on computer-related crimes (1)" 2004 *THRHR* 22 29 -32; *Kearney* 1964 2 SA 495 (A); *Kotze* 1965 1 SA 118 AD; *Harper* 1981 2 SA 638 (D) and *Kimmich* 1996 2 SACR 200 (C).
[17] (n 6) 786.

> opsetlike toe-eiening van sekere soort sake") veel beter as 'n omskrywing van diefstal as "die wederregtelike *contrectatio* van sekere soort sake met die opset om te steel"." [18]

Both Burchell[19] and Snyman[20] are of the view that the South African case law concerning *contrectatio* can be interpreted as having adopted the concept of appropriation as the criterion for the taking element of theft.[21] According to Snyman the act of appropriation in theft consists of any act in respect of property whereby the perpetrator deprives the lawful owner or possessor of his property and exercises the rights of an owner in respect of that property.[22] Depriving the owner of his property rights or benefits flowing from such ownership rights would be to deprive him of the enjoyment of his property.[23]

In the *Boesak* matter the court defined this element as "to deprive the owner permanently of his property or control over his property".[24] Burchell opined that it would be incorrect to argue that it would be sufficient for theft to be committed if there is a mere assumption of control in circumstances where the owner was not deprived of his property.[25]

The South African common law relating to the crime of theft has developed to the extent that the physical handling of property is no longer required,[26] and since control can be exercised over an object without removing it, neither is the removal thereof.[27]

The act of appropriation in respect of money, whether in the format of coins and notes or as the theft of credit, will in effect always amount to the assumption of the power to dispose of or the actual disposing of a certain value or purchasing power quantified as a sum of money, whereby the person entitled to the benefits of such disposal is permanently excluded from those benefits.[28]

---

[18] "Die begrip"toe-eiening" in die omskrywing van diefstal" 1975 *THRHR* 29 34.
[19] (n 6) 787.
[20] (n 6) 487 – 8.
[21] See *Boesak* 2000 1 SACR 633 (SCA) 659, citing *Visagie* 1991(1) SA 177 (A) at 181I, where the supreme court of appeal acknowledged "appropriation" as part of the definition of theft.
[22] (n 6) 488.
[23] See *Premier Western Cape v Parker & Mohammed* 1999 1 All SA 176 (C) 187F – G. See also *Von Elling* 1945 AD 234 236.
[24] *Boesak* (n 21) 659.
[25] (n 6) 489.
[26] *Naryan* 1998 2 SACR 345 (W) 355H – 356H.
[27] *Mlooi* 1925 AD 131 152.
[28] Loubser "The theft of money in South African law" (1977 thesis, University of Oxford) 134. See also Loubser "Sekere probleme in verband met die diefstal van geld" 1978 *De Jure* 86.

There are various means whereby a sum of money can be appropriated and the use of negotiable instruments like cheques for this purpose is an everyday occurrence. Payment cards, including counterfeit cards, can similarly be used by someone other than the lawful card holder to dispose of a certain sum of money, for which the card holder is then debited by the financial institution who issued the card.[29]

Loubser argues that since a thief can employ a variety of means to steal sums of money,[30] the act of theft as far as money is concerned should not be defined in terms of the means employed, but only in terms of the economic effect and therefore, the act must be defined as disposing of or assuming the power to dispose of the value or purchasing power represented by a sum of money resulting in the person entitled to the benefits of such disposal being excluded from those benefits.

Unfortunately our jurisprudence has not yet developed to the stage where the copying of data, causing the owner to be deprived of his exclusive right to the property, is considered to constitute an act of appropriation for purposes of satisfying that element of the common-law crime of theft.[31]

The notion of appropriation as currently interpreted by our judiciary and by academia, does not cater for the phenomena (and increasing threat) of identity theft and theft of data found in modern society and business. The essence of these criminal activities is that the owner at all times remains in possession of the incorporeal assets, which get copied for the intrinsic value thereof for the facilitation of various subsequent dishonesty related offences. Whilst the owner furthermore does not immediately get deprived of the ability to exercise related rights, the criminal obtains a similar "right" (ability) which is exercised simultaneously and to the prejudice of the owner, often leading to the owner subsequently being excluded from the benefits of those rights due to the eradication of whatever credit facilities the owner had.

When data on the magnetic strip of a payment card is for instance "stolen" or personal card data is "stolen" via hacking or phishing to facilitate the manufacturing of a counterfeit

---

[29] In such cases the offender's conduct will usually also involve fraud and he will thus not necessarily be charged with theft.
[30] (n 28 1977) 139.
[31] Watney "Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 1)" 2003 *TSAR* 56 60.

payment card intended for use in card-not-present fraud,[32] proving the element of appropriation in its current definition would be problematic, since the data is in reality only copied to provide the perpetrators with the ability to access and steal the money and/or credit of the owner of the original payment card. The owner is thus not deprived of his property (the card and information encoded on it) and neither is he excluded from exercising his rights in respect of that property (the credit in the account to which the card grants access), but his rights in respect of that property (both the data on the card and the funds in the account) are simultaneously being exercised by the criminal. However, due to the use thereof by the criminals in possession of counterfeit payment cards, the legitimate owner of such a card would in most cases be deprived of the use of the property soon after the track date and personal information number (PIN) of his card were compromised due to the funds or credit being depleted.[33] Although the owner is thus not deprived of control over his card, the activity by the fraudsters ultimately causes him to lose control over the funds and facilities for which he had used his card as an instrument to gain access and use.

Predominantly due to the development of technology, the true nature of the act of theft in modern society has changed and there is a dire need for our common law of theft to be developed accordingly. Actual physical handling of the object is not always essential for the "thief" to achieve all the benefits traditionally associated with the completed crime of theft. Thus to satisfy the requirements of the crime of theft in a modern society, obtaining control over the property and depriving the owner from exercising his related rights, should not be essential requirements anymore. Similarly, as a book entry to the financial prejudice of a complainant may amount to theft of the money involved, copying data unlawfully or assuming another person's identity for own future use ought to amount to theft.[34] The act of

[32] "Hacking" could be described as unauthorised access to a computer, whilst "phishing" entails sending out an email purporting to require information from the recipients for some legitimate purpose. "Phishing" has been explained as follows by Van der Bijl "SIM-card swapping, mobile phone banking fraud and RICA 70 of 2002" 2009 *SA Merc LJ* 159 161: "Phishing entails that unsolicited e-mails, purportedly from the bank, are sent to clients requesting them to update and verify details such as their PIN ('Personal Identification Number'), password, cellular phone number and address. The client will then be requested to click on a link and update his personal details. Once the link is clicked on, the client is diverted to a fraudulent website. The fraudsters then gain access to the client's personal details and cellular phone number when the client responds to such phishing e-mails."

[33] For a discussion of ways in which the PIN of payment cards is compromised, see ch 2 par 3 and ch 3 par 2.2 below.

[34] See par 2.1.2 below for further discussion of identity theft.

"appropriation" involved in the modern variation of theft will often be virtually inseparable from the element of intention and the act has to be coloured by the requisite intention for theft to be proven.

2.1.1.2 Property (things capable of being stolen)

Because of the element of *contrectatio* in Roman and Roman-Dutch law, any item of property that did not have an actual physical existence could not be stolen and only corporeal movable things were thus capable of being stolen.[35]

Loubser, in my view correctly, argued that the law of theft in South Africa could not only apply to money in the form of notes and coins or cheques, which is corporeal, but that it had to provide for the unlawful appropriation of credit or of an incorporeal sum of money.[36] His inference was based on the following argument:

> "The underlying reason why the criminal law cannot confine itself to the unlawful appropriation of money in corporeal form is because money, whether in the form of banknotes and coins or in the form of credit, essentially represents a certain intrinsic value or purchasing power, and where a person is unlawfully deprived of the benefits of disposing of this value or purchasing power it makes no difference economically whether this occurred through a loss of banknotes and coins or through a reduction of the credit in his bank account."[37]

Burchell also correctly points out the importance of the commercial and mercantile implications of the proposition that in South African law only corporeal things are capable of being stolen for a modern system of banking where most transactions are dealt with by way of entries in books of accounts, cheques, credit cards, automatic teller machines and electronic transfers.[38] Such a construction would be untenable. The relative wealth of the owners of the respective accounts is impacted upon by the entry of debits and credits in the books of account and money is transferred as incorporeal credits in books of account.

The South African courts gradually abandoned the common-law requirement of a corporeal object of theft and accepted that theft of money cannot be restricted to money in corporeal form. In *Manuel* Greenberg JA explained his finding that the accused had stolen the complainant's money as follows: "Under our modern system of banking and paying by

---

[35] Burchell (n 6) 788.
[36] (n 28 1977) 107.
[37] Loubser (n 28 1977) 107- 108.
[38] (n 6) 789.

cheque or kindred process, the question of ownership in specific coins no longer arises in cases where resort to that system is made". [39]

As early as 1955 Van den Heever JA made the following obiter remark: "nowadays in cases of theft we are apt to look at the economic effect of the act by which a person fraudulently converts money to his own use rather than be hypnotised by the concrete mechanics by means of which the crime is committed."[40]

The appellate division recognised the fact that an incorporeal sum of money could be the object of theft in a number of cases, including *Scoulides*[41]and *Gathercole*.[42] In *Graham*[43] the court held that where theft of a sum of money and theft of a cheque for that sum were charged alternatively, the conviction could be upheld on either of these charges.

In *Kimmich* it was held that the accused not only appropriated the cheques as corporeal objects, but also the proceeds or economic value that the cheque represents, which is incorporeal in nature:

> "Although in terms of the Roman-Dutch law only corporeal things are capable of being stolen (see *S v Graham* (supra at 576E)) our Courts have expanded the concept of theft, in respect of money other than physical notes and coins, and have held that a conviction of theft of an incorporeal in the form of (a) a diminution of a credit balance in a complainant's bank account (see *S v Kotze* (supra)); and (b) the appropriation of the proceeds of a cheque (see *S v Visagie* 1991 (1) SA 177 (A); *S v Graham* (supra at 577B)) is competent in our law. Our Courts furthermore do not appear to have had any difficulty in holding that other incorporeals, such as shares, in contra-distinction to share certificates, are capable of being stolen (see *S v Harper and Another* 1981(2) SA 638 (D) at 664G – 668H)." [44]

Since money in an incorporeal form can be stolen, it follows that money in its credit form could also be stolen. Not only will it thus constitute theft to deposit a cheque drawn fraudulently on another person's bank account, or to instruct a computer to transfer money from one account (without the account holder's knowledge and permission) to another

---

[39] 1953 4 SA 523 (A) 526H.
[40] *Sibiya* 1955 4 SA 247 AD 261 referring to *Solomon* 1953 4 SA 518 AD.
[41] 1956 2 SA 388 AD.
[42] 1964 1 SA 21 (A).
[43] 1975 3 SA 569 AD 575H-576D. For a discussion of the case and related matters see Dreyer "Computer law in South Africa" 1983 *De Rebus* 534 536 and 537. Also see *Kotze* (n 16) where the appellate division concluded that since a valid cheque represents money and is a generally acceptable form of payment, an agent commits theft of a sum of money if he receives cheques for payment of debts owed to his principal and deposits the cheques in payment of his own private debts, instead of applying them for investment on behalf of his principal; Loubser (n 28 1977) 120 criticises this finding and correctly points out that a negotiable instrument like a cheque does not represent money, but embodies a certain right to money.
[44] (n 16) 210e.

account, but it will also constitute theft if a counterfeit card is used at an automatic teller machine to draw money from the legitimate card holder's account.

However, data and information are not legally recognised as property and can thus not be stolen, despite being potentially very valuable.[45] Van der Merwe profoundly stated:

> "…"data" is the real gold ore which needs to be processed intelligently in order to lead to higher forms of information value. For this reason the South African criminal law system urgently needed to formulate crimes which would protect the integrity and inviolability of data, particularly because our criminal law historically focused on protecting intangible assets and money. Any criminal law system which fails to adequately protect one of the most valuable commercial resources, will ultimately fail in its purpose."[46]

2.1.1.3 Unlawfulness

The appropriation of money will generally be unlawful when the person appropriating the money is not in law entitled to that money. It is difficult to think of any possible grounds of justification if a person's money or credit is stolen through the use of a counterfeit card and such conduct would in my view always be considered unlawful.

The theft of a single payment card is sometimes considered to be so trivial that the *de minimis* rule is invoked as grounds not to prosecute.[47] The appellate division has confirmed that this rule is applicable to the crime of theft in appropriate circumstances, since the courts "should not be concerned with such trivialities".[48] This view may be justified if the potential and likely use thereof in cases concerning card-not-present and/or counterfeit card fraud is ignored. Although it should not be difficult to prove the value and potential for fraudulent use of such a stolen card, it may be challenging to convince a court beyond reasonable doubt that the thief had such fraudulent use in mind. Since there is no other obvious reason why

[45] For a discussion of this *lacuna* and possible solutions see Coetzee "Diefstal van onliggaamlike sake" 1970 *THRHR* 369; Van der Merwe "Diefstal van onliggaamlike sake met spesifieke verwysing na rekenaars" 1985 *SACC* 129 130 ff; Kleyn "Dogmatiese probleme rakende die rol van onstoflike sake in die sakereg" 1993 *De Jure* 3 ff and Maat "Cyber crime a comparative law study" (2004 thesis, University of South Africa) 192 ff.
[46] "Information technology crime – a new paradigm is needed" 2007 *THRHR* 309 312.
[47] The *de minimus non curat lex* rule means that a crime may be so insignificant in nature that the law may disregard it as too trivial to warrant criminal liability. For a discussion of this principle see Burchell (n 6) chapter 22 and Labuschagne "*De minimis non curat lex* as strafregtelike verweer in'n regstaat: opmerkinge oor strafsinvolheid en die groeiende rasionele dimensie van geregtigheid" 2003 *THRHR* 455.
[48] See *Kgogong* 1980 3 SA 600 (A) 603H.

somebody would steal a payment card, the court could however be requested to accept such an objective as the only reasonable inference in the circumstances once the actual theft of the card has been proven.

In such cases the decision in *Nedzamba*[49] should be followed, where the court correctly refused to invoke the *de minimis* principle in a case where the accused stole two blank cheque forms. The court considered not only the commercial value of the unused cheque forms, but also the motive of the thief in stealing the article, the effect of the deed on the community and all the circumstances in which the deed was committed. In *Murbane*[50] the court also considered the argument that a cheque form has no value and that the *de minimis non curat lex* principle should be applied and, emphasising the potential fraud that could be committed using a stolen cheque form, held that the argument held no merit. Buys J neatly commented as follows: "Dit sal tot totale chaos in die handelswêreld lei as die diefstal van tjekboeke en tjekblaaie nie as 'n misdaad beskou word nie."[51] With reference to the above cases the court should consider the special nature of a payment card, the purpose for which it is used in the commercial world and the impact of payment card fraud when determining whether the application of the *de minimis* rule will have an adverse impact on the interests of the community.

2.1.1.4 Intent

The form of culpability required for theft is intention. The accused must intentionally effect an appropriation, must intend to deprive the owner permanently of his property or control over his property, must know that the property is capable of being stolen and must know that he or she is acting unlawfully in taking it.[52] The appellate division further held that an accused cannot be convicted of theft unless he intends to deprive the owner permanently of the whole benefit of his ownership.[53]

When property such as a vehicle is removed from the owner's control for temporary use, but with the intention of returning it to the owner at a later stage, the temporary borrowing of the

[49] 1993 1 SACR 673 (V) 676.
[50] 1992 1 SACR 298 (NC).
[51] *Murbane* (n 50) 301.
[52] Burchell (n 6) 792 and *Boesak* (n 21) 659 par 97.
[53] *Sibiya* (n 40) 257; *Van Coller* 1970 1 SA 417 AD 424G – 426A and *Heller* 1971 2 SA 29 (A) 46.

property without the authorisation of the owner thereof will not constitute theft. The legislature attempted to fill the gap in our law by creating a new statutory offence to criminalise the removal of property for use.[54]

If a person picks up lost property, the act of picking up the property does not constitute unlawful taking and does not give rise to the presumption that there was an intention to terminate the owner's enjoyment of his rights. On a subsequent charge of theft, the *onus* remains on the state to prove the *animus furandi*.[55]

Theft can never be committed negligently. However, intent in the form of *dolus eventualis* will suffice. *Dolus eventualis* exists "where the accused does not 'mean' to bring about the unlawful circumstance or to cause the unlawful consequence which follows from his or her conduct, but foresees the possibility of the circumstance existing or the consequence ensuing and proceeds with his or her conduct".[56]

When the data contained on the magnetic strip of a payment card is copied, the owner is not permanently deprived of the relevant information. In such a case the owner will no longer have exclusive use of the data. Ebersöhn argued that in the instance of mere copying of electronic data, the perpetrator appropriates the immaterial property rights of the owner of the data, has the intention to exercise ownership rights over the electronic copy of the original data and although he has the intention to deprive the owner of his control over the data temporarily and not permanently, such conduct should qualify for the offence of theft.[57] He argues as follows:

> "It is submitted that our courts should give effect to the economic reality and hold that the intention to temporarily deprive the owner of the benefits of his ownership rights (control) by making an electronic copy and the intention to exercise control over the electronic copy suffices for the purposes of theft." [58]

[54] s 1(1) of the General Law Amendment Act 50 of 1956. Since one of the requirements of s 1(1) is the removal of property from the control of the owner, it will also not be applicable to the copying of data on a bank payment card when a skimming device is used.
[55] *Luther* 1962 3 SA 506 (A).
[56] Burchell (n 6) 462. For a comprehensive discussion of the various forms of intention see Burchell (n 6) 461 ff.
[57] (n 16) 37 - 41.
[58] Ebersöhn (n 16) 38.

This view is however not supported by our courts.[59] Maat recommended intervention by the legislature and the enactment of a provision in respect of the intentional and unlawful use or copying of data and certain information without authority.[60] She suggested the following text: "A person who intentionally and without authority copies or uses protected data, is guilty of an offence."[61]

2.1.1.5 Conclusion

If a person uses a counterfeit card either at an automated teller machine (ATM) to withdraw money from the account of the legitimate owner of the originally issued payment card or to pay for merchandise, he or she will be guilty of theft.[62] The unlawful access, copying and subsequent use of data to manufacture counterfeit cards, however, do not meet the requirements of the common-law offence of theft.[63]

2.1.2 Identity theft

Watney defines identity theft as "the abuse of personal information to impersonate somebody else with the intent to commit a crime, for example the use of another's banking facilities without the consent of the account holder…."[64] This type of theft is predominantly commissioned through fraud, often in the form of social engineering,[65] phishing or spoofing.[66] Counterfeit card fraud is a fine example of identity theft.[67]

[59] See *Sibiya* (n 40).
[60] (n 45) 201.
[61] Maat (n 45) 201.
[62] See ch 3 par 4 below.
[63] See ch 3 par 2 and 3 below.
[64] Watney "Identity theft – the dangerous imposter" 2004 *De Rebus* 20.
[65] "Social engineering" is the term used to describe where the fraudster engages in social contact with the victim to extract personal or confidential information required to facilitate the planned criminal activity. For examples of this see Augustyn "Identity theft escalation – you may need to change your life" 2005 *South African Journal of Information Management* 1 6.
[66] "Spoofing" in this context takes place when the link to a website in an email seems legitimate, while the underlying hyperlink is to a completely different site used to lure users to provide their personal details under false pretences. Other methods of obtaining the personal information of other persons include interception of mail and retrieving documents from rubbish bins.
[67] The Australian Crime Commission report on card fraud 2011 accessed through http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/card-fraud (30-4-2012).

Although identity theft is not a new threat, the electronic environment makes it significantly easier to access the personal information required to commit this offence.[68] As stated by Atta-Asamoah, "a more complex form of cyber crime has emerged in which cyber criminals focus primarily on assuming the identity of the target. These second-generation types of crimes make extensive use of information technology skills and involve less time…."[69]

Identity theft is a worldwide phenomenon. In 2005 it already cost the United Kingdom £1.3 billion a year with fraudulent credit card purchases accounting for most to these costs.[70]

Internationally legal systems introduced a specific offence of "identity theft" to address the difficulty of punishing misuse or dealing in identity related information under the general criminal law. Since 1998 the United States of America with the promulgation of the Identity Theft and Assumption Deterrence Act, specifically provided on a federal level for the crime of identity theft.[71] This Act which became effective on 30 October 1998 provided for penalties up to 15 years imprisonment and a maximum fine of $250 000.[72] The Identity Theft Enforcement and Restitution Act of 2007 amended title 18 of the United States Code to enable increased federal prosecution of identity theft crimes and to allow for restitution to victims of identity theft. The European Union, through its arm the European forum of organised crime, is also currently considering the introduction of legislation to deal with identity theft,[73] despite the fact that identity theft does not constitute a substantive offence in the member countries of the European Union.[74] In Australia two states already have criminal provisions relating to identity theft.[75] Western Australia also has an amendment to their criminal code that is currently being considered for enactment.[76] Various offences relating to

---

[68] Watney "'Identity theft': the mirror reflects another face" 2004 *TSAR* 511.
[69] "Understanding the West African cyber crime process" 2009 *Institute of Security Studies African Security Review* 106 109.
[70] Augustyn (n 65) 4.
[71] Watney (n 68) 518. Forty states in America also have statutes to address identity theft. See also Snail "Cyber crime in the context of the ECT Act" 2008 *JBL* 63 68.
[72] title 18 USC 1028b.
[73] Watney (n 68) 518.
[74] Watney (n 64) 21.
[75] Clough *Principles of Cybercrime* (2010) 186 208. Through the Criminal Law Consolidation (Identity Theft) Amendment Act 2004, South Australia specifically addressed the criminalisation of identity theft. It provides that assuming a false identity of another person constitutes a "false pretence" and it also criminalises the production or possession of material that enables a person to assume a false identity.
[76] Western Australia Standing Committee on Uniform Legislation and Statutes Review *Criminal Code Amendment (Identity Crime) Bill 2009* Report 44 (2010).

identity crime have also recently been introduced in Canada by Bill S-4 "An Act to Amend the Criminal Code (Identity Theft and Related Misconduct)".[77]

At present the South African criminal law does not provide for the prosecution of this crime type. Identity theft does not fall within the existing definition of theft, since the "identity in the form of personal information relevant to a specific person is not tangible and the owner of that identity is not permanently deprived of his or her identity when it is utilised by another person".[78] The Electronic Communications and Transactions Act 25 of 2002 (ECT Act) also does not specifically provide for the criminalisation of identity theft.[79]

Watney's view that the prosecution of these offences does not pose a problem is not fully supported.[80] The electronic accessing of the relevant personal data is likely to constitute a statutory offence if proven,[81] and the use of such "stolen identity" will constitute fraud and may constitute theft of money. However, a person who is caught copying personal data related to the identity of another or is unlawfully found in possession of the personal information of other persons, either in the form of the "raw data", eg a stolen database in its original format, or in the form of an instrument of crime, such as a counterfeit card or cloned cheque, may go unpunished.[82]

The South African criminal law has a living and developing common-law system, which contains flexible and adaptable general principles as opposed to rigid rules. One would therefore expect it to adapt reasonably easily to new legal phenomena.

> "The Superior Courts have always had an inherent power to refashion and develop the common law in order to reflect the changing social, moral and economic make-up of society. That power is now constitutionally authorised and must be exercised within the prescripts and ethos of the Constitution."[83]

---

[77] Clough (n 75) 208.
[78] Watney (n 68) 512.
[79] See par 3.1.1 below for a discussion of the ECT Act. In 1985 Le Roux in "Diefstal deur middel van die rekenaar" 1985 *De Rebus* 401, already argued in favour of legislation to cater for new crime types created by the use of computers, including theft of information.
[80] Watney (n 68) 513 and 518.
[81] It is likely to be a contravention of s 86 of the ECT Act. See par 3.1.1 below.
[82] This will not be the case if the facts support a prosecution relying on the doctrine of common purpose as set out in par 2.5 below. If the data is copied by means of a handheld skimming device a prosecution under the ECT Act may not succeed as explained in par 3.1.1 below.
[83] *Thebus* 2003 6 SA 505 (CC) 526F. In *Amod v Multilateral Motor Vehicle Accidents Fund* 1998 4 SA 753 (CC) 763F Chaskalson P also confirmed that the "Supreme Court of Appeal has always had an inherent jurisdiction to

Theft is arguably the one common-law crime in respect of which this adaptability was demonstrated best. In Roman law physical handling of the property was a prerequisite and thus only a material thing could be stolen. The Roman-Dutch writers did not require the thing stolen to have been physically handled, but claimed that there should be some handling of a physical object relating to the thing stolen. An example of this would be the physical handling of the book in the case of writing tablets which were allegedly falsified. Although it involved the physical handling of the book, "credit" was stolen and not the book. Finally the courts moved away from the requirement of physical handling, resulting in the recognition of theft of incorporeal things.

However, since the enactment of the South African constitution,[84] the expansion of the definitional scope of common-law crimes has been impaired due to the law-making ability of our courts being reined in.

Although the legality principle, *nullum crimen sine lege*,[85] was one of the inalienable human rights re-confirmed by our constitution,[86] the same constitution places a duty on the judiciary to develop the common law in order to give greater effect to human rights.[87] Thomas states that our "common law is primarily law in action".[88] The inherent power of the constitutional court, supreme court of appeal and high courts to develop the common law, by taking into account the interests of justice (and the constitutional principles) has been constitutionally authorised.[89] In terms of section 39(2) of the constitution, courts developing the common law, should do so in a manner that promotes the "spirit, purport and objects of the Bill of Rights", ensuring that the common law will evolve within the framework of the constitution.[90]

---

develop the common law to meet the needs of a changing society. The circumstances in which it elects to do so and the manner in which it develops the law form part of this jurisdiction".

[84] The Constitution of the Republic of South Africa 108 of 1996 (the constitution).

[85] no crime without (preceding) criminal prohibition.

[86] In terms of s 35(3)(l) an accused's right to a fair trial includes the right not to be convicted for an act that was not an offence at the time it was committed. For a discussion of the principle of legality see Snyman (n 6) 36 ff and Currie and De Waal *The Bill of Rights Handbook* (2005) 787.

[87] s 8(3).

[88] Thomas "The South African common law into the twenty-first century" 2005 *TSAR* 292 293.

[89] s 173 of the constitution.

[90] See *Pharmaceutical Manufacturers Association of SA; In re Ex parte President of the Republic of South Africa* 2000 2 SA 674 (CC) par 46 – par 49; *Carmichele v Minister of Safety and Security* 2001 4 SA 938 (CC) par 33 – par 36; *Brinsley v Drotsky* 2002 4 SA 1 (SCA) 33 par 88 – 89 and *Afrox Healthcare Bpk v Strydom* 2002 6 SA 21 (SCA) par 27 – 29.

In *Carmichele v Minister of Safety and Security*[91] the court determined that a two-stage enquiry was required when considering the development of the common law beyond existing precedent, namely, whether in light of the objectives of section 39(2) of the constitution, the existing common law should be developed in such a manner and if so, how the development would occur and whether it should be the constitutional court or the supreme court of appeal that should embark on that exercise.[92] Moseneke DCJ (as he was then) confirmed that "the common law must be adapted so that it grows in harmony with the 'objective normative value system' found in the Constitution."[93]

In *Masiya v Director of Public Prosecutions, Pretoria*[94] the adaptability of the common law was demonstrated when the common-law crime of rape was extended by the constitutional court to include penetration of a woman by a man's penis through her anus, an offence which had previously been punishable as indecent assault. Taking into account the prevalence of the crime type in our society, the interests of the victim and the need to express the abhorrence with which society regards "these pervasive but outrageous acts",[95] the constitutional court held that the then common-law definition of rape needed to be appropriately adapted because it fell short of the spirit, purport and objects of the Bill of Rights.[96] Based on the principle of legality the constitutional court duly held that the common law could only be developed prospectively and that the extension of the definition of rape did thus not apply to the accused in that case.[97]

Identity theft involves a serious invasion of the constitutionally protected right to privacy. Applying the principles enunciated in *Masiya* the common-law offence of theft ought therefore to be extended to include the theft of personal information relating to the identity of an individual.

In a number of cases our courts however proved their reluctance to extend the common law crime of theft to incorporeal objects.

---

[91] (n 90) par 40.
[92] See *Thebus* (n 83) 524 par 26.
[93] *Thebus* (n 83) 526 par 28.
[94] 2007 5 SACR 30 (CC). This judgement was severely criticised by Snyman (n 6) 46.
[95] *Masiya v DPP, Pretoria* (n 94) par 44.
[96] *Masiya v DPP, Pretoria* (n 94) par 70.
[97] *Masiya v DPP, Pretoria* (n 94) par 51.

In *Augustine*[98] the court commented:

> "There are always people to be found who invite and favour "extensions" by the Court of the existing principles of the common law to encompass situations which they feel "should" be encompassed, even if they have not hitherto been so encompassed. I do not think the Courts should respond too readily to such invitations. Fundamental innovations of this kind are for the Legislature (if so advised) and not the Courts".[99]

In *Mintoor*[100] where the accused was convicted in the magistrate's court of theft of electricity, the high court setting aside the conviction on review *inter alia* held:

> "In die algemeen gesproke, is dit in elk geval juridies ongesond om die trefwydte van ons strafreg deur Hofbeslissings te vergroot. Die uitbouing van strafregtelike sanksies is 'n taak wat normaalweg aan die Wetgewer oorgelaat word om te verrig indien en insoverre hy dit nodig ag."[101]

In light of the reluctance of our courts in this regard, coupled with the dire need for identity theft to be recognised as a criminal offence and the need for legal certainty on the matter, it would be advisable for the legislature to resolve the matter.

2.1.3 Theft is a continuing crime

Our courts accepted that theft is a continuing crime.[102] Theft thus continues to be committed as long as the stolen property remains in the possession of the thief or somebody who has participated in the theft or somebody who acts on behalf of that person.[103]

The rule that theft is a continuing crime has significant consequences.

- The accused may be tried at the place where he is found with the stolen property even though the original appropriation took place outside of the court's jurisdiction and regardless of whether the taking was regarded as theft by the law of the place where the taking occurred.[104]

---

[98] 1986 3 SA 294 (C).
[99] *Augustine* (n 98) 302I – J.
[100] 1996 1 SACR 514 (C).
[101] *Mintoor* (n 100) 517A – B.
[102] *Brand* 1960 3 SA 637 (A) 640H; *Kruger* 1989 1 SA 785 (A) 793C-E and *Cassiem* 2001 1 SACR 489 (SCA) 492h – 493a. For a discussion of a number of cases relating to theft as a *delictum continuum* see Le Roux "Die aard van diefstal as voortdurende misdaad in die Suid-Afrikaanse strafreg" 2005 *THRHR* 472.
[103] Snyman (n 6) 509.
[104] *Kruger* (n 102) 793C-E. In *Dayizana* 1989 1 SA 919 (EC) 921E - F this principle was confirmed, but it was further held that it "does not follow that a person in country (or district) A who assists a thief who has committed a theft in country (or district) B becomes subject to the jurisdiction of the court in B."

- Persons who assist the thief after the initial appropriation, but while the theft "continues", are guilty of theft (as perpetrators) and not merely as accessories after the fact, as they would be if the general principles applicable to other crimes were applied.[105]

2.1.4 Attempted theft

If we assume that the objective of a syndicate employing a skimming device is to use the track data copied from it to produce counterfeit payment cards with the ultimate objective of using such newly created cards to steal the money and/or credit of the original card holder (who for our purposes can be regarded as the owner of such money, credit and payment card),[106] the question arises whether the perpetrators involved in the entire process could successfully be prosecuted of attempted theft based on evidence that they were already in the process of committing acts indicating that they have arrogated to themselves the rights of the owner.

In *B* Schreiner JA held that the test is whether "the accused had already commenced the consummation of the act constituting the offence or had only taken steps leading up to the stage of commencing to carry it out".[107] The appropriate approach was defined by Watermeyer CJ as follows:

> "The time when the consummation begins must necessarily vary with the particular crime and depend upon the circumstances of the particular case. There are, however, certain general considerations which may legitimately be regarded as of assistance in the solution of the problem. One of these is that the question whether or not a man's wrongful conduct should, in law, be regarded as criminal or innocent should not depend entirely upon the time at which an event happens, when such a time may be largely determined by chance. Consequently if a wrongdoer has finally made up his mind to commit a crime and has taken steps to carry out his resolution, the exact moment at which he is interrupted and prevented from fulfilling his intention should not be the sole determining factor in deciding whether his morally wrongful act should be regarded as a crime. Provided always that his acts have reached such a stage that it can properly be inferred that his mind was finally made up to carry through his evil purpose he deserves to be punished because, from a moral point of view, the evil character of his acts and from a social point of view the potentiality of harm in them are the same, whether such interruption takes place soon thereafter or later. Consequently the Court should lean towards giving a wide interpretation to the phrase 'commencement of the consummation' by including in such consummation all the last series of

[105] Burchell (n 6) 796; *Cassiem* (n 102) 492I – 493B.
[106] For a discussion of skimming devices see ch 3 par 2.1 below. For a discussion of track data see ch 2 par 3 and ch 3 par 2.1, as well as n 353 below.
[107] 1958 1 SA 199 (A) 202E.

> acts which would constitute a continuous operation, unbroken by intervals of time which might give an opportunity for reconsideration." [108]

In *Sibuyi*[109] the court held that a theftuous intention without any physical expression cannot amount to theft or attempted theft. The state has to prove that the accused had intent to commit theft and that he or she acted in furtherance of that intent.

A person found in possession of counterfeit cards aimed at being used at some time in future to steal the money available in the legitimate cardholder's account, has not yet commenced the consummation of the crime and can thus not be charged with attempted theft. The mere acquisition or manufacturing of a card with the intent to commit theft or fraud does not amount to attempted theft or fraud.

2.2 Fraud

Fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another.[110]

The Roman and Roman-Dutch law distinguished between *crimina falsi* (different forms of cunning or deceitful practices causing prejudice to the state) and *stellionatus* (so-called private fraud), but the South African courts followed some of the Roman-Dutch writers who amalgamated the two types of fraud and recognised a single crime of "fraud".[111]

Burchell summarises that various forms of deception, swindling and trickery are in the South African law embraced in the single crime of fraud that penalises any misrepresentation that causes another to suffer some form of prejudice.[112] Due to the fact that potential prejudice suffices, the offence of attempted fraud only exists in a few scenarios, such as when a misrepresentation was made but never communicated.[113]

---

[108] *Schoombie* 1945 AD 541 547 as quoted and affirmed in *B* (n 107).
[109] 1993 1 SACR 235 (A) 241H - J.
[110] Snyman (n 6) 531. See also *Gardener* 2011 4 SA 79 (SCA) 86 par 29.
[111] For a discussion on the development of fraud in the SA law, see Burchell (n 6) 834 – 835 and Snyman (n 6) 531 – 532.g
[112] (n 6) 833.
[113] *Heyne* 1965 3 SA 604 (A). An example of attempted fraud would be when the letter containing the misrepresentation was never delivered, due to getting lost or intercepted in the post as the case was in *Isaacs* 1968 2 SA 187 (D). See also *Francis* 1981 1 SA 230 (ZA); *Moodie* 1983 1 SA 1161 (C) and a discussion of the issue in Burchell "Does potential prejudice suffice for fraud?" 1963 *SALJ* 168.

Henning J summarised the legal position as follows:

> "One would look at the mind of the deceiver and, once he has been proved to have gone beyond acts of preparation in making a fraudulent misrepresentation intended to be acted upon, he would be guilty of an attempt to defraud, and he would likewise be guilty and his conduct punishable if thereafter his design is frustrated for whatever reason….once a false representation is proved to have been wilfully made with intention to deceive, and to be acted upon by the representee to his actual or potential prejudice, the crime of fraud has been established; if the representation has not yet been communicated to the mind of the representee, a verdict of an attempt to commit fraud might be proper."[114]

2.2.1 The elements of fraud and in particular counterfeit card fraud

2.2.1.1 Conduct (misrepresentation)

The misleading or attempted misleading of the victim of fraud by way of a misrepresentation is the essence of the crime.

Although the misrepresentation usually takes the form of written or spoken words, it is also often made by conduct.[115] The mere handing over of a counterfeit payment card as instrument to pay for goods or services at a merchant,[116] the use thereof at an ATM to draw money and the capturing of its particulars to effect payment of goods on the Internet will constitute the misrepresentation required. Botha, in my view incorrectly argued that fraud cannot be committed by way of an automated teller machine as it is not possible to make a misrepresentation to a machine.[117] The misrepresentation is in fact made to the bank or more specifically a banker, as was argued by Burchell with reference to the judgment by Boshoff JP in *Myeza*[118] where a parking meter was activated by using a beer-can ring instead of a coin:

> "On this reasoning it would follow that persons who withdraw money from automated teller machines (ATM) in banks by misrepresenting their identity could be convicted of fraud. Since an ATM is nothing but a computer linked to the funds and records of the bank and serves as a conduit for transmitting instructions as to the receiving or withdrawing of funds, the misrepresentation involved is made to the banker."[119]

---

[114] *Isaacs* (n 113) 191A – C.
[115] *Larkins* 1934 AD 91 94 and *Mbokazi* 1998 1 SACR 438 (N) 445F - I.
[116] *Salcedo* 2003 1 SACR 324 (SCA). Botha "Bedrog ten opsigte van die gebruik van tjek- en/of kredietkaarte" 1988 *SACJ* 377 383 expresses the view that such fraud is committed in writing due to the fact that the perpetrator has to forge the signature of the legitimate card holder.
[117] "Sogenaamde 'rekenaarbedrog'" 1990 *SACJ* 231. See also *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) 577 where the court held that a computer is not a person.
[118] 1985 4 SA 30 (T). For a discussion of the case see Botha "*S v Myeza* 1985 (4) SA 30 (T): oor blikringetjies en boetebessies – aspekte van bedrog" 1986 *SACJ* 72.
[119] (n 6) 840.

With reference to the *Myeza* case[120] the writers Carstens and Trichardt argue:

> "the element of misrepresentation with regard to the crime of fraud, in cases of computer crimes by means of the ATM, lies therein that the perpetrator unlawfully and fraudulently represents to the bank by means of his actions channelled through the ATM, that he has sufficient funds, or made sufficient deposits or transfers enabling him to withdraw money. The perpetrator is thus misrepresenting results on his account, results produced by means of the ATM and herein lies the misrepresentation to the bank, inducing the bank to believe that the results were lawfully produced by means of information channelled through the ATM and that he (the perpetrator) is now entitled to withdraw money. It is further submitted that, just as the element of misrepresentation in this case was not considered to be a misrepresentation made to a parking meter, the same argument is valid in the case where money is fraudulently withdrawn, transferred or deposited by means of an ATM, that the misrepresentation is made to the bank and not to the computer."[121]

This view is also supported by *Van den Berg* where a misrepresentation electronically introduced into the computer system resulting in an account falsely being credited, was held to constitute a misrepresentation to the bank, being a legal *persona*.[122]

When cash is withdrawn at an ATM with a counterfeit card, the implied representation to the bank would either be that it is the customer withdrawing the money or that the transaction has been duly authorised by the customer.[123] It is not a requirement that the charge sheet alleges that the misrepresentation was made to a specific person.[124]

The misrepresentation could either be express or implicit. When a counterfeit card is used to pay a merchant for goods or services and the fraudster falsely places what purportedly is the legitimate card holder's signature on the payslip, the fraudster implies that he or she is the authorised card holder and is entitled to present the card for payment, and he or she therefore commits fraud. The situation is similar when somebody else's particulars (ie that of the lawful card holder) are being provided to a merchant to conduct a card-not-present fraud.

---

[120] *Myeza* (n 118).
[121] "Computer crime by means of the automated teller machine – just another face of fraud" 1987 *SACJ* 122.
[122] *Van den Berg* (n 15).
[123] *Mbokazi* (n 115) 445F – 446C.
[124] *Avion Motor Enterprises* 1987 4 SA 692 (T).

2.2.1.2 Unlawfulness

Although there are generally various grounds of justification to be raised on a charge of fraud, such as compulsion, obeying orders and consent, the use of a counterfeit card as an instrument to effect payment or obtain cash is clearly against the *boni mores* and therefore unlawful.[125]

2.2.1.3 Intent

The fraudster must have both the intent to deceive and the intent to defraud. He must thus make the representation knowing or foreseeing that it might be false. Stegmann J confirms that intent in the form of *dolus eventualis* will suffice and defines it as follows:

> "… when one person makes a representation of fact to another whilst not knowing whether his representation is true or false, if the representor knows that his representation may be false and reconciles himself to the risk entailed in suggesting it to be true, to the potential or actual prejudice of that other or of anyone else."[126]

The distinction between an intention to deceive and an intention to defraud was clarified as follows by Buckley J in *Re London and Globe Finance Corporation Ltd*: "To deceive is by falsehood to induce a state of mind; to defraud is by deceit to induce a course of action."[127]

Heher JA in *Gardener* made the following *obiter* remark in this regard:

> "The authorities I have cited support the view that an intention to cause actual or potential prejudice is a necessary element of the crime of fraud. But it may be that proof of deceit which is calculated (likely), in the ordinary course of things, to result in such prejudice is sufficient, without a subjective mental element."[128]

The prosecution of fraud was previously facilitated by section 245 of the Criminal Procedure Act,[129] which provides the following presumption:

> "If at criminal proceedings at which an accused is charged with an offence of which a false representation is an element, it is proved that the false representation was made by the accused, he shall be deemed, unless the contrary is proved, to have made such representation knowing it to be false."

---

[125] For a discussion of unlawfulness as an element and grounds of justification, see Burchell (n 6) 835 – 836 and Snyman (n 6) 539.
[126] *Ex parte Lebowa Development Corporation Ltd* 1989 3 SA 71 T 101 D.
[127] [1903] 1 Ch 728 at 733 as quoted and approved in *Isaacs* (n 113) 191H. See also Makakaba "Rubber cheques" 2007 *JBL* 17 19.
[128] *Gardener* (n 110) 87 par 32.
[129] 51 of 1977. This clause originated from s 280 *bis* of Act 56 of 1955.

The state could only rely on this presumption if the representation pertained to an objectively ascertainable fact and not when it related to the accused's state of mind.[130] This provision was however found to compromise the right to be presumed innocent severely and thus a court can no longer rely on it.[131] Nowadays, in the absence of an admission to the effect that the accused had indeed been aware of the falsity of the misrepresentation, such knowledge mostly has to be inferred from circumstantial evidence.

It is difficult to imagine circumstances under which the user of a counterfeit card would not be making the misrepresentation knowingly or would make it without the intent to defraud. Even in instances where a counterfeit payment card is presented at a so-called "friendly merchant" who provides the fraudster with the merchandise or even cash, knowing that the card being presented for payment is a counterfeit card, fraud has still been committed, since the law only considers the state of mind of the deceiver and not that of the person to whom the misrepresentation is made.[132]

2.2.1.4 Prejudice

The crime is only punishable if the misrepresentation brings about actual or potential prejudice of a proprietary (financial) or non-proprietary nature.[133] Prejudice of a non-proprietary nature would for instance include damage or potential damage to the reputation of a bank whose automated teller machines are continuously targeted by the use of high-technology skimming devices,[134] the risk of negative media publicity and the risk of loss of credibility in the security of ATM transactions.[135]

"Potential" prejudice means that the making of the misrepresentation objectively involved a risk of prejudice and the test is whether it was reasonably possible that prejudice would

---

[130] *Van Niekerk* 1981 3 SA 787 (T) 790 and *Harper* (n 16) 649.
[131] *Coetzee* 1997 3 SACR 527 (CC). See also Makakaba "Credit card holder's conduct and credit limit" 2007 *JBL* 71 73.
[132] *Judin* 1969 4 SA 425 (A).
[133] *Dyonta* 1935 AD 52 55 – 56 and *Myeza* (n 118) 32. Also see *Ressel* 1968 4 SA 224 (A) 232 E – G. For a discussion of the wide sense in which courts have interpreted "prejudice" see Ebersöhn "A common law perspective on computer-related crimes (2)" 2004 *THRHR* 193 193 – 196.
[134] colloquially referred to as "high-tech skimming devices or high-tech skimmers".
[135] Prejudice in the form of the risk of dishonour or loss of reputation was acknowledged in *Seabe* 1927 AD 28 33.

occur.[136] Although the risk of harm should not be too "remote or fanciful", the test is an objective one and it is not necessary to prove that the prejudice was probable.[137] It is thus not relevant that the victim was not misled by the misrepresentation.[138] Negligence on the part of the representee also does not assist the representor.[139]

The prejudice could be suffered by a third party. This will usually be the case when a counterfeit payment card is used, since the misrepresentation will usually be made to a merchant or a bank, whilst the holder of the targeted account and the legitimately issued payment card will suffer the prejudice or potential prejudice if the fraud was detected before the money left the account.[140]

Despite criticism that the concept of potential prejudice creates an excessively wide scope to the South African crime of fraud and the notion that cases of potential prejudice should rather be treated as attempted fraud,[141] the alleged vagueness of the crime passed constitutional muster and the court held as follows:

> "The present definition of fraud is wide, but that does not make it difficult, much less impossible, to ascertain the type of conduct which falls within it….I find nothing objectionable in the approach which punishes fraud not because of the actual harm it causes, but because of the possibility of harm or prejudice inherent in the misrepresentation….The type of prejudice relied upon by the State, and hitherto accepted by the Courts, is not in my view so repugnant to, or so far removed from, what I conceive to be the moral values of the man in the street, that a reappraisal of the common-law definition of fraud is either warranted or necessary."[142]

2.2.1.5 Conclusion

The use of a counterfeit card either at an ATM to withdraw money from the account of the legitimate owner of the originally issued payment card or to pay for merchandise constitutes fraud with the misrepresentation being made to the bank and the merchant respectively.

---

[136] *Seabe* (n 135) 32 and *Kruger* 1961 4 SA 816 (A) 828H – 829A. It is not necessary to proof a probability of prejudice; a possibility of prejudice will suffice.
[137] *Heyne* (n 113) 622 E – 623 A.
[138] See *Dyonta* (n 133) and *African Bank of SA Ltd* 1990 2 SACR 585 (W) 647F.
[139] *African Bank of SA Ltd* (n 138) 647F.
[140] In such a case the card is blocked by the bank and the client will not only be without the facility until the payment card has been replaced, but will also be subjected to the bank processes relating to the application of replacement cards which could be time-consuming and cumbersome.
[141] See De Wet and Swanepoel *Die Suid-Afrikaanse Strafreg* 1985 391-2 and Burchell (n 6) 843.
[142] *Friedman (1)* 1996 1 SACR 181 (W) 194B and H and 195D - E.

When a computer system is hacked and data required for the perpetration of card-not-present fraud or for the manufacturing of counterfeit payment cards, are being accessed and copied, the hacker will commit fraud.[143] A hacker breaking the username and password protection makes a misrepresentation to the system administrator or anybody in control of the computer that he is an authorised user of the computer. The actions of the hacker will at least cause potential prejudice or harm and one should be able to prove his intention to defraud.

2.3 Forgery and uttering[144]

Forgery is a species of fraud and comprises the unlawful and intentional making of a false document to the actual or potential prejudice of another.[145] The misrepresentation in forgery takes place by way of the falsification of a document.

The only difference between forgery and fraud is that the crime of forgery is already completed when the document is falsified,[146] whilst fraud has only been committed once the misrepresentation has come to the attention of the person to whom it is meant to be made. Innes CJ summarised it as follows: "In a case of ordinary fraud, the falsity is contained in the fraudulent misrepresentation made to the person affected. But in forgery there is a fraudulent perversion of the truth as soon as the false document is made, for a false statement is thereby brought into existence."[147]

If the falsified document is presented to another person, the separate offence of uttering is committed. Uttering, another species of fraud, is the unlawful and intentional passing off of a false document to the actual or potential prejudice of another.[148] Uttering of the forged document could be committed by a person other than the person who has forged the document.

---

[143] For a detailed argument on why hacking into computers constitutes fraud, see Ebersöhn (n 133) 196 – 203.
[144] Although "forgery" and "uttering" are two separate offences, they are discussed together due to usually being used together if the forged document was also uttered.
[145] *Muller* 1953 2 SA 146 (T) 148A - B.
[146] *Hymans* 1927 AD 35 38.
[147] *Hymans* (n 146) 38.
[148] Snyman (n 6) 543.

To be forged, a document must tell a lie about itself and it will not suffice if it merely contains a falsehood.[149] Forgery and uttering can only be committed in respect of documents. Although the courts have never formally defined "document" for the purpose of the crime of forgery or uttering, they have acknowledged various types of documents as being the subject of forgery.

In a prosecution on charges of forgery and/or uttering it is advisable to also consider the definitions of "document" in various statutory provisions when determining the ambit of the development of our law in this regard.

In section 221(5) of the Criminal Procedure Act "document" has been defined to include "any device by means of which information is recorded or stored".

The Documentary Evidence from Countries in Africa Act[150] defines "document" as follows: "'document' includes any affidavit, certificate, record, photograph, book, map, plan, drawing and any documentary recording or transcribed computer printout produced by any mechanical or electronic device and any device by means of which information is recorded or stored."

In section 1 of the Counterfeit Goods Act[151] the definition of "document" is equally broad: "'document' includes a tape recording, a photograph and any electronic or magnetic or other medium on, in, or by means or by way of which, images, sound, data or information may be stored, and 'documentary' will be construed accordingly."

The following definition was suggested by Milton: "[A document is] any writing in any form, on any material, which communicates to some person or persons a human statement, whether of fact or fiction."[152]

The substance on which the writing appears does therefore not matter and neither does it matter in which medium the writing is done. Burchell concludes that forgery is committed in

---

[149] *Banur Investments* 1970(3) SA 767 (A).
[150] 62 of 1993.
[151] 37 of 1997.
[152] Milton *South African Criminal Law and Procedure vol II: Common Law Crimes* (1996) 744. The definition also carries the support of Burchell (n 6) 846.

respect of any document containing writing or marks which can be interpreted into the spoken word.[153]

Although negotiable instruments such as cheques and promissory notes definitely meet the definition of "document" for purposes of these offences,[154] no prosecutions on charges of forgery and/or uttering in respect of counterfeit payment cards have been reported to date. Relying on the definition by Milton, coupled with the definitions of "document" in the legislation quoted above, the meaning of "document" would be wide enough to include a bank payment card reflecting the identifying information of the card holder encoded on the magnetic strip on the back of the card. A counterfeit card tells a lie about itself by purporting to be a valid original card, which it is not.

The manufacturing of a counterfeit card as described below,[155] will constitute forgery. Although the presentation thereof will constitute uttering, the perpetrators will usually be prosecuted for fraud.

Since the actual "making of the document" is one of the elements of the crime of forgery, possession of counterfeit payment cards without evidence of the making thereof by the same person,[156] will not meet all the elements of the crime of forgery.

2.4 *Crimen iniuria*

Crimen iniuria is the unlawful, intentional and serious violation of the dignity or privacy of another.[157]

Section 14 of the South African constitution recognises a person's right to privacy, including privacy of a person's home, property, possessions and communications. "Dignity" or

---

[153] Burchell (n 6) 846.
[154] See *Joffe* 1934 SWA 108; *Reynolds* 1924 TPD 607 and *Sedat* 1916 TPD 431.
[155] ch 3, par 3.
[156] In appropriate cases the prosecutor will be able to rely on such an inference as the only reasonable inference in the circumstances.
[157] Snyman (n 6) 469; *Sharp* 2002 1 SACR 360 (Ck) 372A and *Mostert* 2006 1 SACR 560 (N) 571B -C. Neethling "The concept of privacy in South African law" 2005 *SALJ* 18 23 guards against "complete blurring of the distinction between privacy and dignity as independent interests of personality".

"*dignitas*" includes a person's right to freedom from invasion of privacy and in the South African law invasions of privacy are punishable as a violation of dignity.[158]

Our courts have held that listening to somebody's private conversations using a listening-device that was planted in the person's private apartment,[159] intercepting and reading another person's correspondence,[160] taking private documents from a private safe and copying them,[161] telephone tapping and other forms of electronic surveillance all constitute *crimen iniuria*.[162] Individuals as well as juristic persons are the holders of the right to privacy.[163]

Since the mere unwarranted intrusion of a person's privacy is sufficient to constitute *crimen iniuria*, it is not necessary for the person to be aware of the intrusion and neither is it relevant what the nature of the private conversation is that the perpetrator "listened" to.[164]

The right to privacy is not an unlimited right and privacy infringements may thus in certain circumstances be allowed by the law.[165] In deciding whether an intrusion on a person's privacy is allowed, a court will take into account the prevailing *boni mores*.[166] The ultimate criterion for determining whether a person's dignity has been impaired is that of the reasonable person.[167] Unlawfulness of an *iniuria* will thus be determined by the objective standards of the prevailing norms of society (the current values and thinking of the community), determined by the criterion of persons of ordinary sensibilities.[168] One of the factors a court may take into account when determining unlawfulness, is the need to protect the community or sections of the community from the conduct in question.[169] The court will

---

[158] Burchell (n 6) 747 and 748.
[159] *A* 1971 2 SA 293 (T).
[160] *Hammer* 1994 2 SACR 496 (C).
[161] *Reid-Daly v Hickman* 1981 2 SA 315 (ZA).
[162] See Burchell (n 6) 753 and Van der Berg "The criminal act of violation of dignitas" 1988 *SACJ* 351 367 ff.
[163] *Financial Mail v Sage Holdings* 1993 2 SA 451 (A) 462A - F.
[164] *A* (n 159) 298C – D and Snyman (n 6) 474. See Neethling "S v A 1971 2 SA 213 (T)" 1971 *THRHR* 324 for a discussion of the judgment by Botha J.
[165] *I* 1976 1 SA 781 (RA).
[166] Snyman (n 6) 473 and *Financial Mail v Sage Holdings* (n 163) 462F - G. See also Goodburn and Ngoye in Buys (ed) *Cyberlaw @SA II* (2004) 370 ff 173.
[167] Burchell (n 6) 749.
[168] Burchell (n 6) 753 and *Delange v Costa* 1989 2 SA 857 (A) 862B - G.
[169] Burchell (n 6) 756.

furthermore consider whether the conduct is "likely to have results that may detrimentally affect the interests of the state or the community".[170]

Intention must be proved in respect of each element of the crime. *Dolus eventualis* will suffice.[171]

There is no reported case where it was held that hacking into a computer constitutes *crimen iniuria*. Ebersöhn convincingly argues that it does.[172] If copying private documents from somebody's safe satisfies the elements of the crime, then justifying on principle why the same crime is not committed when the accessing and copying of the same or similar documents are done electronically, seems virtually impossible. Data stored on any medium capable of storing electronic content, including a computer, comprises confidential business and/or personal information protected by the right to privacy.[173] The nature of the data so stored will not determine whether intrusion of its privacy will constitute *crimen iniuria* or not.[174] The mere accessing of a computer system by a hacker, regardless of whether the data accessed is read, copied, deleted and/or modified, will constitute *crimen iniuria*.[175] Hacking is to the detriment of the state and the community and an infringement of a computer user's privacy will also be against the conviction of the prevailing norms of the society.[176]

The principle of legality should not come into play, since an extension of the common law offence of *crimen iniuria* is not proposed; the fact that technology enables different ways in which the right to privacy could be invaded, should merely be acknowledged.

2.5 Common purpose

When the business value chain of counterfeit card fraud is considered,[177] it is clear that the commission of the crime involves a number of people. Although different role players will

---

[170] *Momberg* 1970 2 SA 68 (C) 71G. See also *Jana* 1981 1 SA 671 (T) 676A.
[171] *A* (n 159) 299F -G.
[172] "A common law perspective on computer-related crimes (3)" 2004 *THRHR* 375 378 ff.
[173] Ebersöhn (n 172) 378.
[174] *A* (n 159) 298C - D and Ebersöhn (n 172) 379.
[175] Ebersöhn (n 172) 379.
[176] Ebersöhn (n 172) 379.
[177] See ch 3 below.

execute different activities, all of them ultimately contribute to the theft of the money and/or the fraud on the bank or merchant.[178]

In the South African criminal law a distinction is drawn between perpetrators, co-perpetrators and accomplices as participants in the commission of the crime. Whilst a perpetrator and co-perpetrator satisfy all the elements of a crime, an accomplice knowingly associates him or herself with and facilitates or furthers the commission of the crime by the perpetrator.[179] Our law however also recognises the law of association in crime and the English rule of evidence is applied when accused are charged based on a common purpose, making statements and acts of one accused in the furtherance of the common purpose admissible against the other accused.[180] The conduct of the perpetrator is thus attributed or imputed to the other participants in the common purpose and all parties who actively associate in the common purpose are then considered to be co-perpetrators.

The doctrine of common purpose has been defined as follows:

> "Where two or more people agree to commit a crime or actively associate in a joint unlawful enterprise, each will be responsible for the specific criminal conduct committed by one of their number which falls within their common design. Liability arises from their 'common purpose' to commit the crime."[181]

If a number of people with a common purpose to commit a crime act together in order to achieve that purpose, the conduct of each of them in the execution of that purpose is thus imputed to the others,[182] regardless of whether one plays an active role and the other a less active or even passive role,[183] and regardless of whether there is proof of a prior conspiracy.[184]

---

[178] For a discussion of participation before the completion of the crime, see Burchell (n 6) ch 41 and Whiting "Joining in" 1986 *SALJ* 38.

[179] The conduct of an accomplice does not comply with the requirements contained in the definition of the offence. His liability stems from the fact that he furthers the commission of the crime by somebody else by advising or assisting the perpetrator in various ways, eg by giving advice, supplying information or facilitating the commission of the crime.

[180] *Cilliers* 1937 AD 278 285.

[181] Burchell (n 6) 574 as affirmed in *Thebus* (n 83). In *Motaung* 1990 4 SA 485 (A) 509A Hoexter JA described common purpose as "a purpose shared by two or more persons who act in concert towards the accomplishment of a common aim". The doctrine of common purpose have been discussed by many academia, including Matzukis "The nature and scope of common purpose" 1988 *SACJ* 226; Cameron "Inferential reasoning and extenuation in the case of the Sharpeville Six" 1988 *SACJ* 243 and Rabie "Kousaliteit en 'common purpose' by moord" 1988 *SACJ* 234.

[182] *Thebus* (n 83) 521C.

[183] *Shaik* 1983 4 SA 57 (A) 65A.

[184] *Mambo* 2006 2 SACR 563 (SCA) 570F.

In *Shaik*[185] where the prosecution relied on the doctrine of common purpose in a corruption matter, the hearsay evidence contained in a document was held to be admissible against other *socii criminis*,[186] on the grounds that it was in the interest of justice to do so.

If direct evidence of prior agreement, whether express or implied, to commit an offence lacks, the liability requirement is active association and participation in a common criminal design, with the necessary *mens rea*.[187]

When relying on the common-purpose rule, the prosecution is relieved of the burden of proving causation in consequence crimes on the part of the remote parties. It is not necessary to prove that each participant knew or foresaw in detail the exact manner in which the unlawful result would be brought about.[188] It is however still a requirement to prove beyond reasonable doubt that at least one party to the joint venture caused the unlawful consequence, even if it is not possible to establish precisely which party.

It is furthermore only the act of one person which is imputed to the others, not his or her culpability. The liability of every accused is based upon his or her own intention.[189] Once the court has found that the consequence should be imputed to all the accused, the prosecution still has to prove that each participant possessed the requisite *mens rea*.[190]

---

[185] 2007 1 SA 246 (SCA) 295 par 166 ff.
[186] In *Cilliers* (n 180) 285 the definition of a *socius criminis* was affirmed as anybody who "instigates, procures or assists the commission of the deed", while accused are prosecuted as *socii crimins* if they have a common purpose.
[187] In *Mgedezi* 1989 1 SA 687 (A) 705I – 706B with reference to *Safatsa* 1988 1 SA 868 (A) the court identified additional factors from which such agreement could be inferred when relying on "active association", such as presence at the scene of the crime, being aware of the crime perpetrated by somebody else, intention to make common cause with those who were actually perpetrating the crime, some act of association with the conduct of the others and the intention to commit the crime. For a comprehensive discussion of common purpose by active association see Paizes "Common purpose by active association: some questions and some difficult choices" 1995 *SALJ* 561.
[188] *Shezi* 1948 2 SA 119 (A) 128.
[189] *Malinga* 1963 1 SA 692 (A) 694 and *Khumalo* 1991 4 SA 310 (A).
[190] This differs from the felony-murder rule applicable in Canada and some other Anglo-American jurisdiction as explained by Burchell (n 6) p 578 – 9. *Mens rea* will depend on the type of crime involved and could exist in the form of *dolus directus*, *dolus eventualis* or even negligence. See *Geere* 1952 2 SA 319 (A); *Ngobozi* 1972 3 SA 476 (A) 478E – F and *Nkwenja* 1985 2 SA 560 (A) 568F ff.

In *Goosen*[191] the appellate division held that in consequence crimes the accused's intention must have been directed at bringing about the consequence in substantially the same manner as that in which it actually was caused. *Dolus eventualis* will suffice, but Oliver J cautioned:

> "…one should not too readily proceed from 'ought to have foreseen' to 'must have foreseen' and hence to 'by necessary inference in fact did foresee' the possible consequences of the conduct inquired into. *Dolus* being a subjective state of mind, the several thought processes attributed to an accused must be established beyond any reasonable doubt, having due regard to the particular circumstances of the case….In this case, as in many others, the question whether an accused in fact foresaw a particular consequence of his acts can only be answered by way of deductive reasoning. Because such reasoning can be misleading, one must be cautious."[192]

The finding should result from a "logical inferential process".[193]

When it is proved on a charge of fraud that the scheme had been a joint enterprise with a common purpose involving all or some of the accused, the related transactions have to be considered as parts of a single consolidated scheme, in which case it is sufficient to prove any one act of intention to defraud and one act of prejudice; it is not necessary for the "ingredients of fraud to be established afresh at each stage of the scheme".[194] In *Khambule*[195] the judges of appeal inferred an intention on the participants in the common purpose to unlawfully possess a firearm and all the accused were convicted of the offence, despite the fact that the actual possession or control of the firearm stolen was personal to each participant.[196]

Burchell explains the rationale for the common-purpose rule as being invoked in the context of consequence crimes in order to overcome prosecutorial problems of proving the normal causal contribution between the conduct of each and every participant and the unlawful consequence in the interest of crime control.[197]

In a unanimous decision by the constitutional court the common-purpose rule as formulated by the South African courts was affirmed as constitutional.[198] The common-purpose doctrine

---

[191] 1989 4 SA 1013.
[192] *Lungile* 1999 2 SACR 597 (SCA) 602 par 16 – 603 par 17.
[193] *Lungile* (n 192) 603 par 17.
[194] *African Bank of South Africa Ltd* (n 138) 645B and 647J – 648A.
[195] 2001 1 SACR 501 (SCA).
[196] Burchell (n 6) 580 criticises the judgement in *Khambule* (n 195) on the basis that the actual possession or control of the stolen firearm cannot be imputed from one participant to another.
[197] (n 6) 579.
[198] *Thebus* (n 83). Burchell (n 6) 583 ff also criticises this finding and argues that the court should have followed the English law and shifted the imputed co-perpetrator liability under the common-purpose principle to actual accomplice liability to give appropriate weight to the degree of a participant's participation in a common purpose

was held to be rationally linked to a lawful aim, namely the combating of criminal activities by a number of people acting together. The principle object thereof was acknowledged as the criminalisation of collective criminal conduct to satisfy the social need to control crime committed in the course of a joint enterprise.[199] The court furthermore recognised the fact that group, organised or collaborative misdeeds strike more harshly at the fabric of society and the rights of victims than crimes perpetrated by individuals.[200]

When considering the constitutionality of the doctrine of common purpose, Moseneke J observed as follows:

> "Common purpose does not amount to an arbitrary deprivation of freedom. The doctrine is rationally connected to the legitimate objective of limiting and controlling joint criminal enterprise. It serves vital purposes in our criminal justice system. Absent the rule of common purpose, all but actual perpetrators of a crime and their accomplices will be beyond the reach of our criminal justice system, despite their unlawful and intentional participation in the commission of the crime. Such an outcome would not accord with the considerable societal distaste for crime by common design. Group, organised or collaborative misdeeds strike more harshly at the fabric of society and the rights of victims than crimes perpetrated by individuals. Effective prosecution of crime is a legitimate, 'pressing social need'.[201] The need for 'a strong deterrent to violent crime'[202] is well acknowledged because 'widespread violent crime is deeply destructive of the fabric of our society'.[203] There is a real and pressing social concern about the high levels of crime. In practice, joint criminal conduct often poses peculiar difficulties of proof of the result of the conduct of each accused, a problem which hardly arises in the case of an individual accused person. Thus there is no objection to this norm of culpability even though it bypasses the requirement of causation.
>
> ….It may be added that a person who knowingly and bearing the requisite intention, participates in the achievement of a criminal outcome cannot, upon conviction in a fair trial, validly claim that his or her rights to dignity and freedom have been invaded." [204]

Although the common-purpose rule has to date predominantly been applied to violent crime cases,[205] there is no reason why reliance could not be placed on it in the prosecution of members of counterfeit card fraud syndicates on charges of theft and/or fraud.[206] Since it is

---

in determining both verdict and sentence. For a supporting analysis of the findings in *Thebus* see Reddi "The doctrine of common purpose receives the stamp of approval" 2005 *SALJ* 59. Reddi on 66 concluded the article with the following statement: "In a society that is currently reeling from the impact of a pandemic of serious crimes committed by collective individuals acting in concert, the doctrine of common purpose is crucial to the eradication of the ubiquitous threat."

[199] *Thebus* (n 83) par 34.

[200] *Thebus* (n 83) par 40.

[201] See *Zuma* 1995 2 SA 642 (CC) par 41.

[202] See *Makwanyane* 1995 3 SA 391 (CC) par 117.

[203] *Dlamini; Dladla; Joubert; Schietekat* 1999 4 SA 623 (CC) par 67. In par 68 the court however cautions that the alarming level of crime should not be exploited to justify inappropriate invasion of individual rights.

[204] *Thebus* (n 83) par 39 – par 41.

[205] See for instance *Safatsa* (n 187); *Nzo* 1990 3 SA 1 (A) and *Khumalo* (n 189).

[206] See *Mongalo* 1978 1 SA 414 (O); *Del Ré* 1990 1 SACR 392 (W) and *Windvogel* 1998 1 SACR 125 (C).

unlikely that evidence will be available to prove the existence of an expressed previous agreement between the members of the syndicate to commit counterfeit card fraud, the prosecution will have to rely on an implied prior agreement to be inferred from the facts of the matter, including circumstantial evidence.

The acquisition of the "tools of the trade",[207] the placement and/or removal of a skimming device on or from an ATM, the use of a card reader at a merchant to copy the data on the magnetic strip of a payment card, the downloading of the data retrieved from bank payment cards, the fabrication of counterfeit payment cards and the use thereof to pay for goods or services or to draw cash, most of it by different parties, ought to be enough to prove a prior agreement by various syndicate members to commit counterfeit card fraud and to invoke the common-purpose doctrine. The mere fact that an accused was present when the theft was perpetrated and that he walked or ran away with the person who committed the crime, will however not suffice.[208]

Crime control would furthermore be an equally valid argument for the application of the common-purpose rule in such prosecutions. The challenges currently experienced with sentences imposed in respect of lesser crimes not having the desired deterrent effect may well be addressed in this manner.

3 *Statutory offences*

Technology became the "weapon of choice" among white-collar criminals and is also embraced by regular "street criminals".[209] Internationally, legal systems, which developed over decades and longer, are being challenged with the ever-increasing surge of technology and the fast-moving world of information. Like most other countries South Africa introduced various pieces of legislation to address the legal problems brought by the use of technology.[210] At the heart of the legislation related to information and communication

[207] See ch 3 par 3.1 below.
[208] *Windvogel* (n 206) and *Mongalo* (n 206).
[209] Naude "Rekenaarmisdaad: 'n skewe beeld?" 1983 *SACC* 165.
[210] See Barker "Trespassers will be prosecuted: computer crime in the 1990s" 1993 *Computer Law Journal* 61 for a discussions of different ways in which computers are used to commit crime and the US legal response to that.

technology, is often the protection of data. The question is whether the legislation recently introduced in South Africa sufficiently protects the data contained on payment cards.

3.1 Statutory offences specifically aimed at cyber-related crimes

The criminalisation of unauthorised access to and the modification of data was the focus of a discussion paper "Computer related crime: preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects" published on 2 July 2001 by the South African law commission, which has since had its name changed to the South African law reform commission.[211] One of the recommendations made in the discussion paper was that legislation be considered to introduce new cyber offences.[212] The paper highlighted three vulnerabilities of information technology not being addressed by the South African common law at that stage: unauthorised access to any database, unauthorised modification of data and software applications. The unlawful copying and subsequent use of data was seemingly not specifically considered.[213]

The Department of Communications subsequently released a green paper on electronic commerce, which ultimately resulted in the ECT Act, which has been in operation since 30 August 2002.[214]

The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)[215] was assented to on 30 December 2002, but only came into force on 30 November 2005.[216]

---

[211] Discussion Paper 99 Project 108.
[212] The Commission considered the common-law offences of malicious injury to property, housebreaking and trespassing under the Trespass Act 6 of 1959 and concluded that the South African criminal law could not deal with unauthorised modification of computer data or unauthorised access to computers.
[213] This oversight is probably due to it being seen as an extension of unauthorised access to a database.
[214] *GG* 23809 (30 August 2002). For a general discussion of the impact of the ECT Act on electronic commerce, see Coetzee "The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce" 2004 *Stell LR* 501. Before the introduction of the ECT Act a number of authors argued that it was time for legislative action designed to tighten up the law in connection with the abuse of computers and/or technology. Examples include Van der Merwe "Computer Crime" 1983 *Obiter* 124 and Horwitz "Computer abuse – the legal implications" 1986 *De Rebus* 503.
[215] 70 of 2002. For a discussion of the impact of RICA on telecommunication service providers see Van Rensburg "Intercepting communications and providing communication related information" 2003 *JBL* 90.
[216] Van der Merwe *et al Information and Communications Technology Law* (2008) 390.

The nature of the technology and equipment used and the nature of the use thereof will determine the applicability of the available legislation aimed at addressing cyber-crime.[217]

Since credit and debit cards with magnetic strips, as well as chip-and-PIN payment cards contain data that involves some form of computer and information technology, Maat in my view correctly submits that the ECT Act will be applicable to all such cards.[218] RICA will similarly apply if the devices used and the unlawful activities alleged meet the requirements set out in the Act.

3.1.1 Electronic Communications and Transactions Act 25 of 2002 (ECT Act)

One of the stated objects of the ECT Act is to "develop a safe, secure and effective environment for the consumer, business and Government to conduct and use electronic transactions".[219]

The ECT Act is aimed at the protection of "data" or "data messages".[220] "Data" is defined in section 1 as the "electronic representation of information in any form", whilst "data message" is defined in the same section as "data generated, sent, received or stored by electronic means and includes ... (b) a stored record".

Section 86(1) of the ECT Act deals with the unauthorised access and interception of data, whilst section 86(2) deals with the unauthorised modification or destruction of data. Hacking of a system or database with the intention to obtain protected data to facilitate the crimes of counterfeit card fraud or card-not-present fraud, has thus been criminalised by section 86(1) of the ECT Act. The unauthorised access to the data on the magnetic strip of a payment card facilitated by either a handheld skimmer or a ATM-mounted high-tech skimming device will also constitute a contravention of section 86(1).[221]

---

[217] See par 3.1.1 and 3.1.2 below.
[218] (n 45) 15.
[219] s 2(1)(j). For a discussion of the crimes provided for in the ECT Act, see Watney "Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)" 2003 *TSAR* 241 – 245. For a discussion of some of the other objectives of the ECT Act see Coetzee "Incoterms, electronic data interchange, and the Electronic Communications and Transactions Act" 2003 *SA Merc LJ* 1.
[220] Cassim (n 4) 57.
[221] For a discussion of ATM-mounted skimming devices, see ch 3 par 2.1.2 below.

For purposes of counterfeit card fraud section 86(2) is not relevant due to the data on the magnetic strip of a payment card not being modified during the copying of the data with the use of a skimming device, regardless of whether it is a handheld or a high-tech skimmer.

Section 86(3) prohibits a number of unlawful activities and reads as follows:

> "A person who unlawfully produces, sells, offers to sell, procures for use, designs, adepts (*sic*) for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence."

The ECT Act does not provide a definition of "device", but states that it includes a "computer program" or "a component". The ordinary dictionary meaning of "device" is "a thing made or adapted for a particular purpose, especially a piece of mechanical or electronic equipment".[222] In terms of the ECT Act the device must however have been designed primarily to overcome security measures for the protection of data.

According to Ebersöhn security measures can serve one or more of three purposes:

> "the measures may protect data from
>
> - unauthorized access;
> - unauthorized copying, including distribution or printing; or
> - unauthorized modification, deletion, or corruption."[223]

When considering card skimming, the security measures relevant to a payment card would be the track data on the magnetic strip coupled with the PIN when the card is used to transact at an ATM to authorise electronic access to the bank account of the legitimate card holder.[224]

A high-tech skimmer is a purpose built device specifically designed to fit on the card slot of an ATM and for the exclusive purpose of copying and storing the data contained on the magnetic strip of payment cards used to access clients' accounts and thus meet the requirements set out in section 86(3) of the ECT Act. A mould with a built-in pinhole camera, which has been designed and manufactured to be fitted as part of the fascia of an ATM in order to record the PIN when entered by the client of the bank transacting using the ATM, will similarly meet the requirements set out in section 86(3).

---

[222] Soanes and Stevenson "Concise Oxford English dictionary" (2009) 392.
[223] Ebersöhn "Catching hackers" 2004 *JBL* 14 17.
[224] See ch 2 par 3 and ch 3 par 2 below.

Handheld skimmers were however initially primarily designed for use by employers such as factory owners to monitor time and attendance.[225] Although such devices are currently also frequently being used by fraudsters to overcome "security measures for the protection of data", it may be problematic for the prosecution to prove that the device was "designed primarily to overcome security measures for the protection of data".[226] It would have been preferable had the legislature rather used the words "which is used or can be used to overcome security measures for the protection of data".[227] It is recommended the wording of section 86(3) be amended to address the possible or even intended use of the device rather than the purpose of its design.

Counterfeit payment cards are manufactured with the sole purpose of enabling unauthorised access to and utilisation of the money or credit of the legitimate card holder. To achieve this goal it is essential to overcome the security measures created to prevent such unlawful access. An argument that counterfeit payment cards are devices as contemplated in section 86(3) of the ECT Act should thus succeed.

None of the other "tools of the trade" however meets the requirements set out in section 86(3) of the ECT Act.[228]

In terms of section 86(4) a person who utilises any device or computer program mentioned in section 86(3) to unlawfully overcome security measures designed to protect such data or access thereto, is also guilty of an offence. The mere possession of the devices described in section 86(3) thus constitutes an offence, whilst the utilisation thereof constitutes a further offence.

Section 87(2) of the ECT Act criminalises computer related fraud and reads as follows: "A person who performs any of the acts described in section 86 for the purpose of obtaining any

---

[225] Consultation with Fryer: Director Operations, Risk Diversion (Pty) Ltd, a service provider used for the downloading and analyses of skimming devices and other equipment retrieved by the South African Police Service (10-8-2011).

[226] Although perpetrators are often convicted of the contravention of s 86(3) and/or s 86(4) in respect of the possession and/or utilisation of handheld skimming devices, these convictions mostly followed guilty pleas and to date it has never been challenged whether a handheld skimmer meets the definition.

[227] This is similar to the wording used in the definition of an interception devise in s 1 of RICA.

[228] For a description of "tools of the trade" see ch 3 par 3.1 below.

unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence."

Contravention of section 87(2) of the ECT Act seems to be an appropriate charge when phishing is being prosecuted. However, due to the low maximum penalty provided for in the ECT Act, it would be prudent in such circumstances to rather prosecute for the common-law offence of fraud and to add a contravention of section 87(2) as an alternative charge.

Section 88 criminalises any attempt to commit an offence referred to in section 86, as well as aiding and abetting of a person to commit such an offence.

Jurisdictional matters are regulated by section 90 of the ECT Act and a South African court will *inter alia* be vested with jurisdiction where only part of the offence was committed in the Republic or if the result of the offence had an effect in the Republic.[229]

The maximum period of imprisonment for the crimes prohibited by sections 86(1) and 86(3) of the ECT Act is one year, whilst a conviction of a contravention of section 86(4) could result in a fine or imprisonment for a period not exceeding five years.[230] Van der Merwe correctly points out that these penalty provisions, when compared with those of similar legislation, such as RICA, seem "woefully inadequate".[231] Ironically, anybody who assists the fraudsters to launder the proceeds of a crime such as counterfeit card fraud is liable to a fine not exceeding R100 million or to imprisonment for a period not exceeding 30 years.[232]

Before enactment of the ECT Act there were no provisions in either the South African common law or statutory law that prohibited the possession of, trafficking in, or utilisation of devices used to overcome security measures for the protection of data.

According to Cassim the "ineffectiveness of the South African common law to combat cybercrime" led to the promulgation of the ECT Act.[233] Whether it sufficiently addresses the

---

[229] s 90(b).
[230] s 89. Since the sanction for a contravention of s 86(4) is heavier than that provided for a contravention of s 86(1), it is recommended that perpetrators using high-tech skimmers to access track data, rather be charged with a contravention of s 86(4).
[231] Van der Merwe *et al* (n 216) 78.
[232] s 8 of the Prevention of Organised Crime Act 121 of 1998.
[233] Cassim "Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players" 2011 *CILSA* 123 127.

problem is debatable.[234] As mentioned above it is for instance questionable whether skimming with a handheld skimming device or even possession of such a device will constitute a contravention of the ECT Act, since a handheld skimmer may not be "designed primarily to overcome security measures for the protection of data".[235] Unlawful possession and utilisation of "tools of the trade" other than high-tech skimmers are also still not criminalised.[236] It is unfortunate that the legislature did not use the opportunity to criminalise the unlawful copying and subsequent use and/or distribution of data.

3.1.2 Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)

RICA regulates certain communications, but also enacted certain criminal offences.[237] The manufacturing, assembling, possessing, selling, purchasing or advertising of any "listed equipment" constitutes a criminal offence.[238] The unlawful interception or attempted interception of communication during the course of its occurrence or transmission has also been criminalised.[239]

Unlike the ECT Act, the penalty provisions in RICA have a sufficient deterring impact. Section 51 provides for imprisonment of up to 10 years and fines not exceeding R2 000 000.

In its endeavour to ensure that the provisions of RICA will be as far reaching as possible, the legislature burdened us with a number of very broad and often rather confusing definitions, examples of which are the definitions of "listed equipment", "interception device" and "monitoring device".

"Listed equipment" is defined as "any electronic, electro-magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for

---

[234] Ebersöhn identified at least one omission, namely not criminalising the removal of a digital watermark (n 223) 17.
[235] Accessing the data with a handheld skimmer will however constitute a contravention of s 86(1).
[236] See ch 2 par 3.1 for a description of "tools of the trade".
[237] ch 9 of Act 70 of 2002.
[238] s 45 read with s 44 and 51.
[239] s 49 read with section 51.

purposes of the interception of communication"[240] declared as such by notice in the Government Gazette.

This definition has been expanded upon by a schedule of listed equipment, [241] being "any instrument, device or equipment which is capable of being used to access, record, monitor or retrieve communications from a computer, without the permission of the author of the communication",[242] eg keystroke recorders, "any instrument, device or equipment which is capable of being used to record, monitor or listen to a communication",[243] such as miniature sound recording devices, "any instrument, device or equipment which is capable of being used to visually record, monitor or observe a communication"[244] including a miniature camera, and "any instrument, device or equipment which is capable of being used to determine or monitor the geographical location of a person, vehicle or object".[245]

The conditions under which the abovementioned instruments, devices and equipment are considered to be "listed equipment" are specified as

> "[t]o manufacture, assemble, possess, sell, purchase or advertise any of these instruments, devices or equipment, with the intention to use it, whether by itself or in combination with any other instrument, device, equipment or apparatus for the purposes of unlawful interception of communications in contravention of section 49…."[246]

The breadth of the definition of "listed equipment" is indicative of the legislature's endeavour to criminalise the manufacturing, assembling, selling, purchasing, advertising and possessing of any equipment which could be used to unlawfully intercept communications. Yet the legislature deemed it necessary to also define "interception device".

An "interception device" means

> "any electronic, mechanical or other instrument, device, equipment or apparatus which is used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any

---

[240] s 44.
[241] The Minister of Justice and Constitutional Development introduced in reg 1263 as promulgated under *GG* 28371 (29 Dec 2005) a schedule of "listed equipment" as provided for in s 44 of RICA.
[242] *GG* 28371 (n 302) column 1(1).
[243] *GG* 28371 (n 302) column 1(2).
[244] *GG* 28371 (n 302) column 1(3).
[245] *GG* 28371 (n 302) column 1(4).
[246] *GG* 28371 (n 302) column 2(1).

> communication, … and a reference to an 'interception device' includes, where applicable, a reference to a 'monitoring device'".[247]

"Monitoring device" was also widely defined as "any electronic, mechanical or other instrument, device, equipment or apparatus which is used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication".[248] "Monitor" "includes to listen to or record communications by means of a monitoring device".[249]

High-tech skimming devices and pinhole cameras seem to fit the definitions of listed equipment, monitoring devices and interception devices for the purpose of prosecutions under RICA and the possession, manufacturing, assembling, selling, purchasing and advertising thereof will constitute a contravention of section 45.

"Intercept" is defined as

> "the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender, recipient or intended recipient of that communication, and includes the-
>
> (a) monitoring of any such communication by means of a monitoring device;
> (b) viewing, examination or inspection of the contents of any indirect communication; and
> (c) diversion of any indirect communication from its intended destination to any other destination."[250]

It is clear that the legislature also meant for "interception" to be interpreted widely.

In terms of section 1 of RICA "communication" includes both direct and indirect communication. "Direct communication" includes both oral communication and audible utterances.[251] "Indirect communication" means the

> "transfer of information, including a message or any part of a message, whether-
>
> (a) in the form of –
> (i) speech, music or other sounds;
> (ii) data;
> (iii) text;
> (iv) visual images, whether animated or not;

---

[247] s 1.
[248] s 1.
[249] s 1.
[250] s 1.
[251] s 1. Direct communication thus includes both oral communication between any number of people in one another's presence and indirect communication overheard by another person, such as a telephone conversation.

(v) signals; or
(vi) radio frequency spectrum; or
(b) in any form or in any combination of forms,

that is transmitted in whole or in part by means of a postal service or a telecommunication system."[252]

Telecommunication is "the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio or other electromagnetic waves, or any other agency of a like nature, whether with or without the aid of tangible conductors".[253] In terms of s 1 of RICA "Telecommunication system" means "a telecommunication system as defined in the Telecommunication Act",[254] and the definition thereof reads as follows:

> "any system or series of telecommunication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to re-arrangement, composition or other processes by any means in the course of their transmission or emission or reception."[255]

Although "telecommunication service" and "telecommunication system" are not specifically defined in the Electronic Communications Act, "telecommunication" appears to have been included in the definition of "electronic communication" which has been defined as follows:

> "the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electromagnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service."[256]

Telecommunications could be described as the conduit over which electronic transactions, including banking transactions at an ATM,[257] take place.

In terms of section 2 of RICA the interception of communication "in the course of its occurrence or transmission" is prohibited. This requirement may prove to be problematic when prosecuting for the use of an ATM-mounted skimming device to acquire the track data on the magnetic strip of a card while it is used at an ATM to transact or "communicate" with the bank. The same challenge will not be encountered in respect of a pinhole camera being used to intercept the communication of the PIN of the client when entered on the keypad of

---

[252] s 1.
[253] s 1. See also Thornton *et al* in Buys (ed) (n 166) 256.
[254] 103 of 1996. This Act was repealed by the Electronic Communications Act 36 of 2005.
[255] s 1 of the Telecommunications Act 103 of 1996.
[256] s 1 of the Electronic Communications Act.
[257] See ch 2 par 1 below.

the ATM. In both instances the data communicated to authorise access to the client's account is made available to "a person other than the sender, recipient or intended recipient of that information".

A high-tech skimming device is usually placed on the outside of the ATM card slot and the track data on the payment card is thus technically read by the skimmer before it is read by the ATM card reader which reads the track data to identify the card and account holder before instructions on the keypad to effect transactions are allowed to the bank.[258] For sections 2 and 49 of RICA to apply to the unlawful acquisition of the track data on the magnetic strip of a payment card through the use of an ATM-mounted high-tech skimming device, one will have to argue that the "communication" already commences when the card is put into the card slot and not only once the ATM card reader commences with the reading of the data in question. It is submitted that this argument should succeed, especially if it is taken into account that the payment card cannot reach the ATM card reader without first going through the skimming device coupled with the legitimate card holder's intention to communicate with his or her bank when he or she starts to put the card in the card slot of the ATM.

Since handheld skimmers are not used to intercept communication, but rather to copy and record the data on the magnetic strip of the card during a separate action,[259] it will not meet the requirements of any of the equipment or activities defined in RICA.

Although there have been a number of convictions for the contravention of sections 2 read with section 49 and/or of section 45 read with section 44 and further read with sections 1 and 51 of RICA when accused are charged for the possession and use of card readers or skimming devices and cameras to intercept the PIN of the legitimate payment card holder,[260] these convictions followed plea and sentence agreements with the accused.[261] The appropriateness of the charges has therefore not been challenged or tested yet. Should any of these charges be challenged, the definitions in the legislation may be an obstacle and it is recommended that

[258] For a discussion of ATM-mounted skimming devices see ch 3 par 2.1.2 below.
[259] For a discussion of handheld skimming devices see ch 3 par 2.1.1 below.
[260] Examples include *Foo Hui Ooi* case no CCC1/32/11 East London Commercial Crime Court (unreported) and *Xotongo* case no 29/08 Matatiele Magistrates Court (unreported).
[261] provided for in s 105A of the Criminal Procedure Act.

they be reviewed and simplified to facilitate the prosecutions of the activities they criminalised.

None of the provisions of RICA has been tested in the constitutional court and Van der Merwe questions whether especially the presumptions accompanying the criminal provisions will withstand constitutional scrutiny.[262]

3.2 Other relevant statutory provisions

3.2.1 Prevention of Organised Crime Act 121 of 1998 (POCA)

This legislation was *inter alia* enacted to introduce measures to combat organised crime, money laundering and criminal gang activities and created the offence of racketeering. In the preamble of POCA a number of factors contributing to the decision to enact the legislation, are listed, among which:

- the rapid growth of organised crime, money laundering and criminal gang activity nationally and internationally;
- the identification of organised crime as an international security threat;
- the infringement of organised crime, money laundering and criminal gang activity on the rights of the people of South Africa as enshrined in the Bill of Rights;
- the potential to inflict social damage and the danger presented to public order, safety and economic stability by organised crime, money laundering and criminal gang activity;
- the difficulty to prove direct involvement of organised crime leaders in particular cases due to them not performing the actual criminal activities and
- the fact that the South African common law and statutory law fail to deal effectively with organised crime, money laundering and criminal gang activities and also fail to keep pace with international measures aimed to deal effectively therewith.

"Criminal gang" is defined as to include

> "any formal or informal ongoing organisation, association, or group of three or more persons, which has as one of its activities the commission of one or more criminal offences, which has an identifiable name

[262] Van der Merwe *et al* (n 216) 30.

> or identifying sign or symbol, and whose members individually or collectively engage in or have engaged in a pattern of criminal gang activity".[263]

The inclusion of the requirement of an "identifiable name, sign or symbol" excludes the known organised criminal groupings currently involved in counterfeit card fraud. The offences criminal gang activities provided for also relate mainly to violent crime.[264]

An "enterprise" is defined to include "any individual…, association, or other juristic person…, and any…group of individuals associated in fact…".[265] Any crime syndicate, whether formally or informally organised, would thus constitute an enterprise as envisaged in POCA.

Section 2(1) of POCA creates various offences related to racketeering activities. The one most often appropriate to counterfeit card fraud activities reads as follows: "whilst managing or employed by or associated with any enterprise, conducts or participates in the conduct, directly or indirectly, of such enterprise's affairs through a pattern of racketeering activity" [266]

A "pattern of racketeering activity" has been defined as

> "the planned, ongoing, continuous or repeated participation or involvement in any offence referred to in Schedule 1 and includes at least two offences referred to in Schedule 1, of which one of the offences occurred after the commencement of this Act and the last offence occurred within 10 years (excluding any period of imprisonment) after the commission of such prior offence referred to in Schedule 1."[267]

Schedule 1 offences include fraud, theft, forgery, uttering and any conspiracy, incitement or attempt to commit any offence referred to in Schedule 1.

A typical counterfeit card fraud syndicate would:

- have members responsible to obtain the "tools of the trade";
- recruit waiters, cashiers and others to assist with the skimming of payment cards using handheld skimming devices and the noting of PIN numbers; and/or
- recruit persons to install high-tech skimming devices and cameras at ATMs and subsequently remove the devices;

---

[263] s 1.
[264] s 9.
[265] s 1.
[266] s 2(1)(e).
[267] s 1.

- use skilled people to download data retrieved with skimming devices;
- possibly use hackers to obtain confidential card data or bribe people to disclose such data;
- use skilled people to manufacture counterfeit payment cards; and
- use people to present counterfeit cards for payment and/or people to withdraw cash at ATMs using counterfeit cards.[268]

In the typical syndicate scenario various people perform various activities at different times and places and they need not know one another. It is also not a requirement for any member of the syndicate or enterprise to participate in all the related activities or to even know the detail thereof.

The legislature makes provision for the admission of evidence in a prosecution on racketeering charges that would otherwise have been inadmissible, such as hearsay evidence and evidence of similar facts and relating to previous convictions.[269]

The penalties provided for in POCA are significantly harsher than the penalties contained in any of the other statutory offences relevant to counterfeit card fraud. A person convicted of racketeering offences faces a fine not exceeding R1 000 million or imprisonment for a period up to imprisonment for life.[270]

POCA also provides for various offences related to money laundering or the proceeds of unlawful activities and any of the runners or mules involved in making payments by using counterfeit payment cards or in withdrawing cash from ATMs with such cards, as well as "friendly merchants" could be prosecuted for these.[271] A person so convicted is liable to a fine up to R100 million or imprisonment for a period not exceeding 30 years.[272]

The criminal and civil recovery and/or forfeiture actions provided for in POCA should also be considered to disrupt the activities of syndicates involved in counterfeit card fraud.[273]

---

[268] See ch 3 below.
[269] s 2(2).
[270] s 3(1).
[271] s 4 – 6.
[272] s 8.
[273] See ch 5.

3.2.2 General Law Amendment Acts

In more than one instance the legislature criminalised actions that do not meet all the elements of the common-law offence of theft, but are theft related.

3.2.2.1 General Law Amendment Act 62 of 1955

In terms of section 36 of the General Law Amendment Act 62 of 1955 a person is guilty of an offence if he or she is found in possession of goods in regard of which there is a reasonable suspicion that they have been stolen and is unable to give a satisfactory account of such possession.[274]

Since counterfeit payment cards are not stolen property, the possession thereof will not constitute a contravention of section 36 of the General Law Amendment Act 62 of 1955 and neither will the possession of stolen card data since card data does not qualify as "goods capable of being stolen".[275] Since the first requirement has not been satisfied, the other elements of the crime are not discussed.

This offence was created to address the difficulty that the prosecution in certain circumstances has to prove all the requirements of the common-law offence of theft or receiving stolen property knowing it to be stolen.[276]

The constitutional court held that the provisions of section 36 are not incompatible with the constitution.[277]

It is recommended that the creation of a similar offence be considered to facilitate the prosecution of possession of counterfeit payment cards.

3.2.2.2 General Law Amendment Act 50 of 1956

Following the decision in the case of *Sibiya*[278] the legislature passed the General Law Amendment Act which made unauthorised borrowing an offence in certain circumstances.

---

[274] Stock or produce as defined in the Stock Theft Act 26 of 1923 has been excluded.
[275] *Monyane* 1960 3 SA 20 (T) 23 A. See discussion in par 2.1.1.2 above.
[276] Snyman (n 6) 524.
[277] *Osman v Attorney-General, Transvaal* 1998 2 SACR 493 (CC).
[278] (n 40).

This was to compensate for the fact that the common law crime of theft would only apply to instances where it was proved that the perpetrator's intention was to deprive the owner permanently of his full benefits of ownership.[279]

Section 1 of the General Law Amendment Act only provides for unauthorised borrowing of property. However, the unauthorised copying of data and the possession of copied data are still not criminalised and statutory provisions to address this *lacuna* are recommended.

3.2.3 Customs and Excise Act 91 of 1964

Various provisions of the Customs and Excise Act are intended to govern and control the importation of goods into South Africa and provides for the forfeiture of goods in certain circumstances.[280] A number of criminal offences provided for in the Customs and Excise Act furthermore ought to be considered when perpetrators involved in criminal activities related to counterfeit card fraud are prosecuted.

In terms of section 81 read with section 15 of the Customs and Excise Act non-declaration of all goods acquired abroad,[281] or of prohibited or restricted goods or goods controlled under any law,[282] and which goods were brought into South Africa, is a criminal offence. A sentence of the greater of a fine not exceeding R8 000 or treble the value of the goods in question or to imprisonment not exceeding a maximum of two years are provided for, as well as seizure of the goods in question.[283] Skimming devices, including high-tech skimming devices, will fall within the ambit of the devices mentioned. Since the importation of these devices or components thereof is rarely declared when earmarked for unlawful use, it would often be appropriate to add a charge of contravention of the Customs and Excise Act when perpetrators are prosecuted.

---

[279] Skeen "Crimes committed by computer" 1984 *BML* 9.
[280] s 83, 87 and 88. For a discussion of the sections and relevant case law see Legwaila "Seizure and forfeiture in terms of the Customs and Excise Act 91 of 1964: rigid application continues, but what about the legislative rationale? A note relating to *Capri Oro v Commissioner of Customs and Excise* 2001(4) SA 1212 (SCA) as a basis" 2002 *StellLR* 444.
[281] s 15(1)(a)(i).
[282] s 15(1)(a)(iii).
[283] s 81.

Possession of goods liable to forfeiture under the Customs and Excise Act is criminalised by section 83(b) of the same Act. A person who makes false statements or declarations or submits false documents to the custom official and/or South African Revenue Services regarding the nature or origin of devices or other goods declared when entering South Africa will also be guilty of an offence.[284] A person selling skimming devices or offering such devices for sale, will furthermore be guilty of an offence if he or she cannot prove the origin of such goods when requested by an officer.[285]

3.2.4 Immigration Act 13 of 2002

During the last couple of years a number of foreigners have been arrested for their involvement in counterfeit card fraud.

Section 49(15) of the Immigration Act creates various offences in respect of the use and/or possession of *inter alia* fabricated or falsified passports, travel documents, identity documents or other documents used for the facilitation of movement across borders.

Fraudsters, who enter the country without valid travel documents or who remain in the country after their travel visas or permits lapsed and commit any of the activities involved in the business value chain related to counterfeit card fraud,[286] could also be prosecuted for being illegal foreigners and sentenced to a fine or imprisonment not exceeding three months.[287] Anybody who knowingly assists such a foreigner to remain in the country without valid documents will also be guilty of an offence and on conviction liable to a fine or to imprisonment not exceeding one year.[288]

[284] False statements and/or declarations are criminalised in terms of s 84. An example of this is when skimming devices were declared as USB ports as was the case in *Mokoena* case no D3001/2010 in the Witbank Magistrates Court (unreported).
[285] s 102(1). In terms of s 1 an "officer" means a person duly employed on any duty relating to customs and excise.
[286] See ch 3 below for a discussion of the activities involved in the business value chain related to counterfeit card fraud.
[287] S 49(1)(a) criminalises presence of a foreigner in South Africa in contravention of the Immigration Act.
[288] s 49(2).

3.2.5 Identification Act 68 of 1997

Section 18(1) of the Identification Act creates various offences related to the possession of forged identity documents, the forgery or alteration of identity documents and the presentation of incorrect particulars or somebody else's identity document as his or her own. These offences are punishable with a fine or imprisonment for a period not exceeding five years.[289]

Prosecution for these offences should be considered when a fraudster using a counterfeit payment card submitted forged identity documents when asked to submit proof of his or her identity or when false identity documents are seized during the arrest of any of the members of a syndicate involved in counterfeit card fraud.

3.2.6 Trade Marks Act 194 of 1993

Various trademarks, such as the distinguishable marks of Visa or MasterCard and the bank who issued the card, appear on a payment card. However, the Trade Marks Act does not provide for the criminalisation of forged trademarks used on counterfeit payment cards.[290]

3.2.7 Counterfeit Goods Act 37 of 1997

"Counterfeit goods" are described as "goods that are the result of counterfeiting…".[291] The definition of "counterfeiting" includes

> "without the authority of the owner of any intellectual property right subsisting in the Republic in respect of protected goods, the manufacturing, producing or making, whether in the Republic or elsewhere, of any goods whereby those protected goods are imitated in such manner and to such a degree that those other goods are substantially identical copies of the protected goods; … . However, the relevant act of counterfeiting must also have infringed the intellectual property right in question."[292]

The intellectual property rights referred to include a trademark conferred by the Trade Marks Act 194 of 1993.[293]

---

[289] s 18(2).
[290] The criminal offences in the Trade Marks Act 194 of 1993 are limited to fraud in relation to the registers in terms of s 60, making false statements for purpose of deceiving or influencing the registrar or other officers in terms of s 61 and falsely representing a trade mark as a registered trade mark in terms of s 62.
[291] s 1.
[292] s 1.
[293] s 1.

From the preamble of the Counterfeit Goods Act it is clear that its objective was to prohibit trade in counterfeit goods and to protect the owners of intellectual property rights against the release of counterfeit goods into commerce. Various criminal offences have been created in the Act.[294] Mere possession of counterfeit goods without possession thereof in the course of business for the purpose of dealing in those goods is, however, not criminalised. The manufacturing or production of counterfeit goods is an offence, except if it is manufactured or produced for "private use". The offences created in section 2 of the Counterfeit Goods Act are not applicable to the manufacturing, possession or use of counterfeit payment cards as an instrument to commit fraud or steal money or credit.

3.2.8 Prevention of Counterfeiting of Currency Act 18 of 1965

The Prevention of Counterfeiting of Currency Act criminalises the counterfeiting of coins and the forging or altering of bank notes, the uttering, tender or acceptance of such coins and/or notes, as well as the possession, import and/or export thereof.[295] Similar offences have also been created by the South African Reserve Bank Act 90 of 1989.[296] The forgery and/or uttering of such notes and/or coins are seen in a serious light and sanctioned with imprisonment of a period not exceeding fifteen years.[297] No provision has however been made for offences related to the counterfeiting, possession, dealing or use of bank payment cards.

The state has the sole right to produce coins and bank notes in the Republic of South Africa,[298] and anybody who usurps this prerogative of the state to issue money commits a crime.[299] Although this Act's only objective is to protect the state's right to issue money, the criminalisation of the counterfeiting of payment instruments such as bank payment cards, would be an appropriate "fit" in an amendment of the Act.

---

[294] See s 2.
[295] s 2.
[296] s 34(1)(a) and (b).
[297] s 34(1)(i).
[298] s 14(1) of the South African Reserve Bank Act 90 of 1989.
[299] Milton *South African Criminal Law and Procedure vol III: Statutory Offences (formerly known as Gardiner and Lansdown)* 1971 56.

3.2.9 National Payment System Act 78 of 1998

The National Payment System Act does not contain any provisions relevant to counterfeit payment card fraud.

3.2.10 Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA)

Chapter 2 of the PRECCA created various offences in respect of corrupt activities. If the acquisition of the data or any of the equipment required to facilitate counterfeit card fraud is obtained through corruption, the related criminal activity could be prosecuted in terms of PRECCA. A "friendly merchant" would not only be an accomplice on fraud, theft or money laundering charges, he or she would in most instances also have contravened sections 3 and/or 10 of PRECCA.

3.2.11 Riotous Assemblies Act 17 of 1956

3.2.11.1 Attempt

In terms of section 18(1) of the Riotous Assemblies Act,[300] any person who attempts to commit any statutory offence is guilty of an offence.[301]

If, for example, either a handheld or a high-tech skimming device is used to copy the data on the magnetic strip of a payment card, but no data is being captured due to the device being faulty, the perpetrator would be guilty of attempt. Since both the ECT Act and RICA provide for criminalisation of an attempt to commit a contravention of provisions of the legislation in question, it is unlikely that section 18(1) would be used during a related prosecution.[302]

[300] See also s 257 of the Criminal Procedure Act which provides for a conviction of an offence should the evidence proof that an accused was an accessory after such offence was committed. An accessory after the fact is somebody who, after the commission of the crime, unlawfully and intentionally helps the perpetrator or accomplice to escape liability.
[301] See Burchell (n 6) 624 – 641 and Snyman (n 6) 284 – 294 for a discussion on attempts to commit crime. See also s 88(1) of the ECT Act.
[302] See s 88 and s 2 of the ECT Act and RICA respectively.

3.2.11.2 Conspiracy

Unlike the situation in English law, the crime of conspiracy does not exist in the South African common law.[303] Conspiracy to commit a crime was introduced into the South African law by section 18(2)(a) of the Riotous Assemblies Act, which reads as follows:

> "Any person who conspires with any other person to aid or procure the commission of or to commit…any offence, whether at common law or against a statute or statutory regulation, shall be guilty of an offence and liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable."

A conspiracy is thus an agreement between two or more persons to commit an offence. Although the crime of conspiracy originated from an old statute dealing with riotous assemblies, the definition is wide enough to cover conspiracy to commit any crime.[304]

While the legislature is silent on the issue, most courts' interpretation of the provision contained in section 18(2)(a) is that it should only be used if the envisaged crime has not been committed.[305] If the envisaged crime has been commissioned, it would be more appropriate to prosecute the conspirators as co-perpetrators or accomplices.[306] Hartzenberg J however expressed the view that there is no reason in principle why the state cannot charge the perpetrator with the antecedent conspiracy rather than the completed offence.[307] Whether an accused could be prosecuted in South Africa for conspiracy in circumstances where the conspiracy was committed in South Africa and the primary offence was committed in another country, will depend on the facts of each matter.[308] An accused could not be convicted of both the crime conspired to and conspiracy.[309]

---

[303] *Cooper* 1976 2 SA 875 (T) 878. See Snyman "Die misdaad sameswering" 1984 *SACC* 3 for a general discussion of the offence of conspiracy.
[304] *Libazi* 2011 1 All SA 246 (SCA) 256 par 18. In *Sibuyi* (n 109) the alleged conspiracy related to theft of bearings from axles of train trucks.
[305] *Milne and Erleigh(7)* (n 14) 823 G and *Fraser* 2005 1 SACR 456 (SCA) par 7.
[306] See Snyman (n 6) 295 for an example where s 18(2)(a) of the Riotous Assemblies Act 17 of 1956 would be used if the main charge has been committed.
[307] *Basson* 2000 1 SACR 1 (T).
[308] See *Fraser* (n 305) where the conspiracy to kidnap took place in South Africa and the child was to be brought to South Africa after being kidnapped in Malawi. See further *Del Ré* (n 206) where the conspiracy to commit fraud or theft took place in South Africa by three perpetrators, whilst the fraud or theft were committed by two of the perpetrators in Botswana. See also *Basson* (n 307).
[309] *Agliotti* 2010 JOL 26556 (GSJ) 7.

There must be at least two people involved for the crime to be committed and the prosecution has to prove that there was an actual agreement entered into and that there was a meeting of the minds among the conspirators.[310] The conspirators must furthermore have the intention to conspire with each other and to commit the crime in question or to assist in its commission.[311] It is not a requirement that the conspirators reach an agreement on the exact manner in which the crime is to be committed or as put by Boshoff J "it is not necessary that any particular means or devices for attaining the object be agreed upon".[312] The agreement to commit an offence constitutes conspiracy and the precise methods to be used, the specific acts or who are to carry these out to commit the crime are unimportant.

The conspiracy need not be expressed and neither is the evidence of a conspirator essential to prove it.[313] It is however not necessary for the agreement to commit a crime to be made in explicit terms.

> "although the common design is the root of a conspiracy, it is not necessary to prove that the conspirators came together and actually agreed in terms to have the common design and to pursue it by common means and so to carry it to execution."[314]

The court may infer the existence of a conspiracy from the conduct of the accused, but only if that inference is the only reasonable one to be drawn from the evidence as a whole.[315] Direct evidence of a conspiracy is often not available to the prosecution, but as stated by Malan J:

> "By reason of the very nature of the offence charged it is clear that the case cannot be set out in crisp and well-defined issues. This is, in a sense, a misfortune under which a person charged with conspiracy may be labouring in certain instances because once a *prima facie* case of having agreed to act in concert is made out, the acts and conduct of each of them are attributable to the others and constitute evidence against them."[316]

In *Twala* the legal principle was explained as follows:

> "When the liability of respective conspirators is considered it is trite law that when two or more persons are engaged in a common enterprise the acts and declarations of any one of them done in pursuance of that common purpose may be admissible against the other. If various people pursued by their acts the same unlawful object, often by the same means, some performing one part of an act and others another part of the same act so as to complete it with a view to the attainment of the object which they were

---

[310] *Sibuyi* (n 109) 249E.
[311] *S* 1959 1 SA 680 (C) 683B – 684H and *Agliotti* (n 309) 8- 9.
[312] *Cooper* (n 303) 879H.
[313] *Sibuyi* (n 109) 249F.
[314] *Moumbaris* 1974 1 SA 681 (T) 686H.
[315] *Cooper* (n 303) 879G; *S* (n 311) 683E, *Heyne* 1958 1 SA 607 (W) 609B and *Singo* 1993 2 SA 765 (A).
[316] *Heyne* (n 315) 609C-D.

pursuing, the conclusion may be justified that they have been engaged in a conspiracy to effect that object."[317]

Even if an accused plays a complementary role meant to ensure the successful completion of the planned crime, he will be guilty of conspiracy. A case in point is found in *Stanley,*[318] where the driver of the vehicle responsible for the transport of the poachers of rhinoceros into and again out of the trust area where the illegal hunting were supposed to take place, was convicted on a charge of conspiracy. Although the hunting never took place due to the poachers being shot by detectives and game scouts who kept them under surveillance, the driver of the vehicle, who was arrested when he came to pick up his accomplices, was a willing participant in the illegal hunting of the rhinoceros and knew that the intended operation was illegal.

When all the parties involved in the commission of an offence are not prosecuted in the same trial, evidence related to the acts by the persons not being prosecuted will be admissible during the prosecution of the accused in order to prove the complicity.[319] An agreement to commit a number of offences constitutes a single conspiracy, regardless of whether the perpetrators conspire to commit the same offence a number of times or whether the agreed scheme comprises different crimes.[320]

The fact that the offence of conspiracy is complete when the agreement is concluded does not mean that the agreement ceases to exist. It continues in existence until it is discharged, for example by the commission of the completed crime. While the conspiratorial agreement is in existence it may thus be joined by other persons, who will then also be guilty of conspiracy.[321]

It is not necessary for all the conspirators to know one another or even to know the identity of all the other conspirators and therefore it is also not necessary for the state to allege the identity of the person making the representation when prosecuting a syndicate, as long as the particulars of the fraudulent scheme is alleged.[322] In an "umbrella spoke conspiracy" the person in the centre at different occasions independently discusses and agrees the crime to be

---

[317] 1979 3 SA 864 (T) 865B-D.
[318] 2010 JOL 26252 (ZH).
[319] *Miller* 1939 AD 106.
[320] Snyman (n 303) 12.
[321] *Moumbaris* (n 314) 687D.
[322] *Mall* 1959 4 SA 607 (N) 617 and *Heyne* (n 315) 609.

commissioned with the different conspirators,[323] whilst in a "chain conspiracy" the conspirators form links of a chain and every conspirator enters into an agreement with another conspirator who will again enter into an agreement with a third conspirator etc.[324]

A syndicate responsible for counterfeit card fraud would typically follow a chain conspiracy with the group responsible for placing and removing the high-tech skimming devices for instance reaching an agreement with the people responsible for downloading the data who will again reach an agreement with the people recruited to manufacture the counterfeit cards etc.

The offence of conspiracy offers a useful tool in the prosecution to include members of a syndicate who have not yet presented the counterfeit payment cards at an ATM or merchant.

[323] *Snyman* 1984 SACC 3 13. An umbrella spoke conspiracy would typically be encountered when a secret organisation of political activists plan their criminal activities aimed at overthrowing the government.
[324] *Snyman* (n 323) 13.

CHAPTER 2

INTRODUCTION TO BANK PAYMENT CARD FRAUD

1 *Introduction*

The revolution in banking in general and payment methods specifically has predominantly been caused by changes in information technology, changes in communication technology and globalisation.[325] Payment can nowadays be effected in various ways of which payment by means of a payment instrument such as a credit or debit card is one. Despite a payment card not being a form of money and not qualifying as legal tender,[326] the use thereof as an instrument or method of payment is not only generally acceptable in the modern economy, it has surpassed the use of cash (coins and notes) and negotiable instruments such as cheques by far.[327]

The increased number of customers and transactions involving the withdrawal of cash forced banks to introduce cash dispensers enabling depositors and borrowers to withdraw cash 24 hours per day.[328] Cash dispensers were subsequently replaced by an ATM allowing for a bigger range of banking business to be conducted 24 hours per day, seven days a week.[329] An ATM could be described as "a computerized telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier, human clerk or bank teller".[330] Typically an ATM connects directly to

---

[325] Schulze "Countermanding an electronic funds transfer: the supreme court of appeal takes a second bite at the cherry" 2004 *SA Merc LJ* 667. See also Oelofse "Enkele regsaspekte van ontwikkelings in die bankwese" 1985 *MBL* 6.

[326] Gering *Handbook on the Law of Negotiable Instruments* (2007) 86 ff; Stassen "Betaling deur middel van 'n driepartykredietkaart" 1978 *De Jure* 134 135; Stassen and Meiring "Ongemagtigde kredietkaartgebruik: wie dra die skade?" 1979 *MBL* 28; Schulze "E money and electronic fund transfers. A shortlist of some of the unresolved issues." 2004 *SA Merc LJ* 50 and s 17 of the South African Reserve Bank Act. See also Stassen "Some legal aspects of credit cards – III Paying by credit card" 1978 *BML* 12 13, where the author argues that a merchant who advertises that he will accept certain credit cards, makes an offer and will be obliged to accept payment through the credit card system once a contract has been concluded with the consumer.

[327] Malan "The liberation of the cheque" 1978 *TSAR* 107. See Malan *et al Malan on Bills of Exchange, Cheques and Promissory Notes* (2009) 5 ff for a discussion of negotiable instruments. For a discussion of the history of payment cards and the development of the security markings thereof, see Schulze "Smart cards and e-money: new developments bring new problems" 2004 *SA Merc LJ* 703 – 708.

[328] Visser "The evolution of electronic payment systems" 1989 *SA Merc LJ* 189 198.

[329] Visser (n 328) 198. For the history of AMTs see "Automatic teller machine the history of computing project" accessed through http://www.thocp.net/hardware/atm/htm (5-5-2012).

[330] See Wikipedia encyclopaedia "automated teller machine" http://en.wikipedia.org/wiki/Automated_teller_machine (30-4-2012).

its host via either ADSL or dial-up modem over a telephone line or directly via a leased line.[331] ATM devices in remote areas will usually rely on a dial-up modem connected to a telephone line.[332] An ATM-activated payment card also serves as a means to access cash.

To accommodate the use of technology in banking, an electronic funds transfer system (EFT) was introduced. It is a generic term and includes various devices employed to transfer funds without the use of paper, including ATMs and the transfer of funds at point of sale.[333] For both these types of transactions bank payment cards are used to identify the account holder and to grant access to the client's account.

Bank payment cards predominantly consist of debit,[334] credit and charge cards.[335] Fraud types experienced in respect of these payment instruments comprise counterfeit card fraud, card-not-present card fraud, fraud committed using stolen or lost cards and fraudulent use of cards obtained through application fraud. Currently the biggest contributors to payment card fraud are counterfeit card fraud and card-not-present fraud.

2 *Card-not-present fraud*

Card payment transactions that are not made face-to-face are known as card-not-present transactions.[336] Fraudulent purchases are often made telephonically, per fax or over the Internet.[337] In such cases account information, including pseudo-account information is used

[331] Consultation with Olivier, head of point of sale, HA and S1 switch, Nedbank Ltd Group Technology (19-4-2012).
[332] Consultation with Olivier (n 331).
[333] Visser "Banking in the computer age: the allocation of some of the risks arising from the introduction of automated teller machines" 1985 *SALJ* 646 647.
[334] A garage-card is a debit card. See Dijkman "Garage-card fraud, a solution" 1986 *BML* 35.
[335] Disputed transactions in respect of all forms of payment cards are normally resolved through chargeback mechanisms. For a discussion of the chargebacks and the chargeback process see Buys in Buys (ed) (n 166) 370 ff.
[336] For a discussion of the development of and law relating to internet credit card programmes in the United Kingdom, see Casanova "Establishing internet credit card programmes in the United Kingdom" 2001 *Journal of International Banking Law* 70.
[337] For an analyses of the legal nature of a card payment over the Internet, see Lawack "Electronic innovations in the payment card industry" 1998 *SA Merc LJ* 233. What is of concern is that consumers in South Africa do not enjoy the same legal protection as consumers in the European Union in the case of fraudulent card payment in distance selling contracts such as when a fraudulent purchase is made over the internet. In this regard see Lawack-Davids and Marx "Consumer protection measures for erroneous or unauthorized internet payments: some lessons from the European Union?" 2010 *Obiter* 446 457.

without the involvement of a physical card.[338] Unlike the case with face-to-face transactions, online transactions are not protected by some of the security features such as signatures and chip technology. During online transactions no verification is performed to establish whether the purchaser is authorised to use the account.[339] To commit card-not-present fraud, the fraudster requires the personal details of the victim, in particular the name in which the legitimate card has been issued, the card number, the expiry date of the card and the CVV[340] or CVC[341] number of the card.[342] The CVV and CVC numbers are the three- or four-digit card security numbers on cards, which are designed to validate that a genuine card is being used during the transaction.[343]

Any stolen card or lost card that fell in the wrong hands could be used to commit card-not-present fraud.[344] Only once the legitimate cardholder reports the loss or theft to his bank and the card is being blocked, further transactions are prevented.

In order to make this type of fraud profitable, it has to be perpetrated at a large scale, requiring the card data of a large number of people. Although the data could be obtained by bribing an employee with access to such data, the easiest way to obtain the required volume is through hacking of card data or phishing. Based on media reports, this unfortunately happens frequently.[345] In respect of phishing the financial services is the most targeted industry

---

[338] See "Payment fraud statistics – summary of results fraud perpetrated on Australian issued payment instruments 1 July 2010 – 30 June 2011" accessed through http://www.apca.com.au/docs/fraud_statistics_2011a_printfriendly.pdf (2-5-2012).
[339] Clough (n 75) 186.
[340] Visa's card verification value.
[341] MasterCard's card validation code.
[342] All the required data is available on a bank payment card.
[343] Wells *Encyclopedia of Fraud* (2007) 271. Since the CVV or CVC is not available when counterfeit payment cards are manufactured, such cards cannot successfully be used for card-not-present fraud.
[344] Although lost and stolen cards could also be used as counterfeit cards once re-encoded with details of another card, it is more often used to commit card-not-present fraud.
[345] Poremba "What identity thieves want from a data breach" 25-4-2012 http://www.msnbc.mns.com/id/47179180#.T51F7fFhiSM/html (26-04-2012); McGlasson "Network Solutions data breach: 573 000 cardholders at risk" 28-7-2009 http://www.bankinfosecurity.com/articles.php?art_id=1660 (7-9-2011); MacDonald "Citi says number of credit cards hacked was actually 360,000" 16-6-2011 http://news.consumerreports.org/money/2011/06/citi-says-number-of-credit-cards-hacked-was-actually-360000.html; Criminal division of the United States Department of Justice "Hacker pleads guilty to identity theft and credit card fraud resulting in losses of more than $36 million" 21-4-2011 http://www.justice.gov/opa/pr/2011/April/11-crm-501.html (30-4-2012) and Mangis "Global payments breach puts 1.5 million credit card numbers at risk" 2-4-2012 http://news.consumerreports.org/money/2012/04/global-payments-breach-puts-15-million-credit-card-numbers-at-risk.html (30-4-2012).

sector.[346] One such malicious computer program available to hackers to obtain credit card information by recording keystrokes of card owners and transmitting them to a third party via the Internet, is a Trojan.[347]

The card data thus obtained could be used to manufacture counterfeit payment cards, but due to the absence of track data such cards would have limited use and can only successfully be used for purchases under the floor limit. The data as such is however a commodity and is often either sold for use overseas, where the floor limits are usually higher, or traded for another instrument acquired by another syndicate, for example identity books, for subsequent use to facilitate or perpetrate various criminal activities.[348]

Card-not-present fraud is rife. In South Africa this type of fraud in respect of credit cards increased by 77% during the period 1 October 2010 to 30 September 2011 compared to the same twelve months during the 2009/2010 years and the R142.8m related loss formed 35.4% of the total credit card fraud losses suffered during the 2010/2011 period.[349] Based on the experienced of the United Kingdom,[350] one can predict that as payment cards become less vulnerable to counterfeiting, the losses related to card-not-present fraud will become correspondingly higher.

3 *Counterfeit card fraud*

The fastest growing type of bank card fraud in South Africa is counterfeit card fraud.[351] Counterfeit card fraud can be described as fraud arising from a card that has been illegally manufactured with information stolen from the magnetic strip of a genuinely issued card.[352]

---

[346] "Phishing activity trends report, 1st half 2011" accessed through www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf (5-5-2012).

[347] Henning and Ebersöhn "Insider trading, money laundering and computer crime" 2001 *Transactions of the Centre of Business Law: Combatting Economic Crime* 105 112 – 113. As explained in Verma *Cyber Crimes & Law* (2009) 58, a Trojan is "an unauthorised program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing".

[348] According to a crime profile on card fraud issued by the Australian Crime Commission in 2011 credit card information was in 2009 the most commonly sold item in the underground economy (n 67).

[349] South African Banking Risk Information Centre (SABRIC) *Card fraud South Africa 2010 -2011* 3.

[350] "The UK Cards Association annual report 2012" accessed through www.theukcardsassociation.org.uk/press_release/index.asp (5-5-2012).

[351] SABRIC Commercial Crime Office *2011 annual report*.

[352] Anonymous "Counterfeit cards drive up card fraud losses" *The Professional Accountant* (May/June 2009) 24 25. See also Financial Fraud Action UK "Counterfeit card fraud facts and figures" 2011 accessed through http://www.financialfraudaction.org.uk/Financial-Counterfeit-Fraud.asp (30-4-2012).

The magnetic strip affixed to the back of a payment card contains essential cardholder and account information, including the account number and expiry date.[353] The information required to manufacture counterfeit cards is usually obtained through card skimming.[354]

Since the early 1970s the standard security backbone of all payment cards has been the magnetic strip with which they are issued that comprises two or three tracks of confidential data in machine readable format.[355] However, the increased access to and use of technology by organised criminal groupings nowadays cause this security feature to pose a security risk. Access to the data on the magnetic strip enables criminals to manufacture counterfeit payment cards that are used to steal the legitimate card holder's available credit. Magnetic strip cards are vulnerable to compromise since the information is magnetically encoded and stored on the exterior of the card, thereby allowing the data to be read, copied, deleted, forged, altered or rewritten at will by anyone with access to the appropriate read/write device.[356]

Due to the vulnerability of the magnetic strips on payment cards, South African banks decided to replace these cards with cards with a microprocessor chip embedded in it.[357] The data is burnt into the microprocessor chip on the card and can be read by a scanning device or smart card reader when the specific security access codes (usually a personal identification number) associated with the data contained in the card is entered.[358] The microprocessor chip thus stores the data in a more secure manner and together with a personal identification number, a secret numeric password that is shared between the user and the system used to authenticate the user to the system,[359] better security is offered to clients. Although all South

---

[353] This data is collectively known as the "track data".
[354] Card skimming is the copying of encoded information from the magnetic strip of a legitimate card using a card reader in order to use the data to encode blank cards (also known as "white plastic"), lost or stolen cards for fraudulent use.
[355] Schulze (n 327) 705.
[356] Watney (n 68) 517.
[357] Mhlanga "Credit card fraud on the rise…but the banks are fighting back with new technology" *Personal Finance Newsletter* (13-03-2008) 1. The microcomputer chip embedded on a chip-and-PIN card does not only have a significantly bigger memory enabling it to store vast amounts of confidential data, but it also has robust security features involving the utilisation of a secret key embedded on the chip to recognise a randomly coded challenge sent to it by the payment terminal. In this regard see Schulze (n 326) 54 – 55.
[358] Henning and Ebersöhn (n 347) 137. For a discussion of the features of a "chip" card see Faul "Die 'smart' kaart – hoe werk dit?" 1989 *SA Merc LJ* 381.
[359] As explained by Schulze in "Duty of a bank to act with necessary skill and care when issuing an automated teller machine card" 2007 *De Jure* 370 375, the PIN serves as "signature" and authentication when a bank payment card is used to withdraw cash at an ATM and the money will only be paid out by the ATM if the correct PIN is keyed in.

African banks have rolled out "chip-and-PIN" cards to replace credit cards, most debit cards are still issued with magnetic strips. "Chip-and-PIN" furthermore do not completely prevent counterfeit card fraud.[360]

The gross loss suffered by the South African banking industry due to South African-issued credit card fraud during the period 1 October 2009 to 30 September 2010 was R263.3m of which R141.4m resulted from counterfeit card fraud.[361] During the same period in 2010/2011 the gross loss was R403.1m of which R230.7m was due to counterfeit card fraud.[362] Counterfeit credit card fraud increased by 63% in 2010/2011 and contributed to 57.2% of the total gross credit card fraud loss suffered.[363] Industry losses pertaining to South African issued debit card fraud has only been collated since January 2010 and totalled R277,3m for the period 1 October 2010 to 30 September 2011, of which 95% were due to counterfeit debit cards.[364]

Despite the roll out of "chip-and-PIN" on credit cards and various industry awareness campaigns to equip banking clients to minimize the risk of their cards being skimmed,[365] the use of counterfeit credit and debit cards remains a matter of grave concern to all stakeholders. This echoes the international experience.[366]

During 2010, 190 handheld and 36 ATM-mounted skimming devices were retrieved through the combined efforts of the South African Police Service and the banking industry.[367] Further

---

[360] For a discussion of the continued vulnerability of payment cards in respect of counterfeit card fraud, see Van der Bijl "The cloning of credit cards: the dolly of the electronic era" 2007 *StellLR* 331.
[361] SABRIC (n 349) 4 and 6.
[362] SABRIC (n 349) 4 and 6.
[363] SABRIC (n 349) 3.
[364] SABRIC (n 349) 3.
[365] See for example Pillay "Tips to prevent being a victim of fraud at an ATM" *Personal Finance Newsletter* (July 2010) 8. Providing the consumer with the necessary knowledge and tips to protect themselves from becoming the victim of card fraud is also part of the international response to this threat. Examples of such awareness material is readily available on the Internet, for instance Anonymous "Facts about credit card fraud" *Shopping Guides Online for Consumers* http://www.infofaq.com/fraud/credit-card/index.html (7-8-2011).
[366] In 2009 in the United States $1.36 billion was lost due to debit card fraud as reported in Biba "Burning question: why are ATM cards still so vulnerable to fraud?" 28-2-2011 http://www.wired.com/magazine/2011/02/pr_burning_atm_fraud/html (7-8-2011). See also Wells (n 343) 263 ff; Sullivan "Debit card thieves get around PIN obstacle. Wave of ATM fraud indicates criminals have upped the ante." 3-9-2006 http://www.msnbc.msn.com/id/11731365/ns/technology_and_science-security/html (26-4-2012) and Kitten "ATM skimming spree investigated" 2-9-2011 http://www.bankinfosecurity.com/articles/html (26-4-2012).
[367] The electronic device used to read and store the data contained on the magnetic strip at the back of a payment card is colloquially known as a "skimmer" or "skimming device".

investigation resulted in the seizure of ten embossers, 24 card readers, 53 computers and one key logger. Related arrests totalled 249 and 165 criminal cases were opened. According to the available statistics subsequent prosecutions resulted in 60 convictions to date with the majority of sentences being either suspended or fines of less than R20 000 per offender.[368]

During 2011, 194 handheld and 53 ATM-mounted skimming devices were retrieved.[369] In Gauteng alone 66 handheld and 38 ATM-mounted skimming devices, 31 card encoders, 3 embossers, 886 counterfeit cards, 35 computers and 164 pages of card track data were seized and 200 perpetrators were arrested.[370] Although the available statistics are not complete, the majority of the convictions followed guilty pleas on watered down statutory charges with light sentences, most of which were suspended.

From the above statistics it is clear that counterfeit card fraud is a growing crime that pays well, whilst prosecutions and sentences hardly have any deterring effect. Detection of the crime is also more challenging due to the fact that physical proximity between a victim and the perpetrator is not required.[371]

Counterfeit card fraud has increasingly become a faceless crime. Identifying and arresting the perpetrators has become more challenging due to the movement towards greater anonymity in the choice of *modus operandi*. Through the increased use of sophisticated high-tech skimming devices that are attached to ATMs, more perpetrators do not interact physically with any person, thus reducing the threat of identification and arrest of both the person responsible for the skimming of a card and of the person using a counterfeit card. One can safely concur that "computer crime by means of the ATM is alive and well and living dangerously in South Africa".[372] To combat this type of offence effectively, the identification, arrest and prosecution of all role players in the business value chain of counterfeit card fraud are thus of increased importance.

---

[368] There is no complete and accurate database available in respect of prosecutions and reliance was placed on the cases reported to SABRIC.
[369] SABRIC (n 351) 18.
[370] SABRIC (n 351) 21.
[371] Cassim (n 233) 125.
[372] Carstens and Trichardt (n 121) 129.

When fraudsters present counterfeit payment cards in a commercial transaction, the criminal activity is seemingly covered by the common-law offences of theft and fraud. The possession and use of devices such as high-tech skimmers, which were primarily designed to overcome security measures for the protection of data, are being prosecuted as contraventions of the ECT Act. There are no known prosecutions to date for other criminal activities related to counterfeit card fraud, such as the use of a card encoder or embosser to produce the counterfeit cards or mere possession of the data required to produce counterfeit cards.

CHAPTER 3

THE CRIMINAL BUSINESS VALUE CHAIN[373]

1 *Introduction*

Counterfeit bank payment cards can either be newly manufactured or re-encoded cards. Newly manufactured cards are cards that are manufactured from scratch starting with a so-called "white plastic",[374] while a re-encoded card is usually a lost or stolen card of which the magnetic strip has been re-encoded with unlawfully obtained track data. In the majority of cases "white plastic" is used.

The life cycle of counterfeit card fraud where the aim is to produce newly manufactured cards for use, consists of various stages, including obtaining all relevant data, downloading the data, manufacturing the counterfeit cards, distributing and using the cards.[375]

In the typical counterfeit card fraud syndicate different people will be responsible for executing the different activities and some of the perpetrators may also be working for more than one syndicate or organised crime grouping. As technology becomes more sophisticated and user-friendly, so does its role increase in each of the different stages of the life cycle of counterfeit card fraud. With reference to the growing concern regarding the role of cybercrime in organised crime, Walden made the following observation:

> "Concerns about the spotty teenager hacking into military systems motivated by mere curiosity have been largely transferred to concerns about the criminal organization, mafia-style, involved in every sector of profitable criminality, from counterfeiting to child pornography, malware to spam, and operating on a transnational basis."[376]

The criminal business value chain can be broadly divided into the following categories:

- Obtaining the required equipment and information.
- Manufacturing the counterfeit payment cards.

---

[373] The facts in this chapter is based on interviews held with Van Wyk of the South African Police Service (11-8-2011), Nel of Nedbank Credit Card Fraud (11-9-2011), Greetham of the MasterCard Card Association (29-8-2011), Potgieter of SABRIC (20-12-2011) and Fryer (n 225).
[374] This would be the case when purchased white plastic already has a magnetic strip at the back.
[375] In instances where the objective is to use the card without physically presenting it, so-called card-not-present fraud, obtaining and using the relevant card information are the only requirements. See ch 2 par 2 above.
[376] Walden *Computer Crimes and Digital Investigations* 2007 66.

- Utilising these cards to obtain cash.

We will now briefly examine each of these stages.

2 *Obtaining the required information*

Criminals require both the track data encoded on the magnetic strip at the back of a payment card and the PIN belonging to the legitimate card holder to produce and use a counterfeit payment card.

2.1 Obtaining the personal information encoded on the magnetic strip of a bank payment card

Obtaining the personal information encoded on the magnetic strip of a legitimately issued bank payment card is essential to manufacture a counterfeit card, irrespective of whether the method requires re-encoding an existing bank payment card or manufacturing a counterfeit card using "white plastic". To achieve this perpetrators usually make use of skimming using an electronic or magnetic card reader better known as a skimming device.[377] Skimming could be described as the illegal copying of the encoded information from the magnetic strip of a card with the aid of a magnetic card reader.

A skimming device is a physical device that can be used to read, copy and store electronic data from the magnetic strip of a bank payment card. By swiping the payment card of a client through the electronic card reader, the data contained on the magnetic strip is captured and stored. Such data can subsequently be downloaded from the skimming device with the aid of a computer terminal.

Electronic card readers are freely available and in the majority of instances bought on the Internet and/or imported. These devices are not currently manufactured in South Africa. Due to the wide legitimate use of these devices for access and security purposes, their importation is not regulated in South Africa.

In South Africa both handheld and ATM-mounted skimming devices are encountered; the use of the latter, also known as high-tech skimming devices, is on the increase.

---

[377] Other methods of obtaining the sought information include corruption of an employee of the legitimate manufacturers of bank payment cards and hacking.

2.1.1 Handheld magnetic card readers

Handheld magnetic card readers or skimming devices can be used at any point of sale or payment where payment by bank cards is allowed, such as a restaurant or a tollgate. When a customer hands over the card for payment, the criminal also surreptitiously swipe the card through a handheld magnetic card reader, which copies and stores the track data copied on the magnetic strip.

As explained by Fisher-French

> "[r]estaurants especially are rife with waiters skimming information off cards. It just takes a couple of seconds to them to skim the card through a devise the size of a matchbox, and then all they have to do is watch you key in your PIN – hey presto, unfettered access to your account…".[378]

Handheld skimming devices are also frequently used at ATMs where unsuspecting victims are coerced in swiping their cards through the handheld card reader. Various permutations of this *modus operandi* have been experienced in South Africa.

In most of the incidents reported the ATM card reader entry slot was damaged. The victim is then approached by the perpetrator who seemingly tries to help him. In the process the perpetrator takes the victim's card and escorts him to another ATM. By the time the victim receives his card back it was already skimmed with a handheld skimming device. In other known cases a person purportedly working for the bank approached the client with a request to "re-activate" his card by swiping it through the skimming device. Handheld card readers have even temporarily been attached to an ATM together with a leaflet requesting the naive customer to swipe their cards prior or after making use of the ATM facility.

2.1.2 ATM-mounted skimming devices

When online, the ATM is directly connected to the central computer of the financial institution and the transactions processed immediately.[379] When offline, the transaction will be reflected in a tape at the machine and the consumer's account will only be credited once

[378] "Chip-and-PIN cards: they're not as safe as you think…" *Personal Finance Newsletter* (January 2010) 8.
[379] Carstens and Trichardt (n 121) 125.

the information on the tape is registered in the bank's central computer.[380] When a typical ATM transaction is conducted, it involves the following steps:[381]

> "(a) the customer inserts a plastic card into the terminal;
>
> (b) he enters his PIN on a keyboard;
>
> (c) the ATM instructs the customer by displaying messages on a screen;
>
> (d) the customer presses the appropriate function key to indicate the transaction he wishes to perform;
>
> (e) the customer enters the amount;
>
> (f) the ATM displays the information the customer entered, and the customer presses an appropriate key to verify the transaction or to correct any mistakes; and
>
> (g) the ATM completes the transaction."

The so-called high-tech skimmers used to retrieve the track data of cards legitimately used during ATM transactions vary in sophistication and appearance. Although some ATM-mounted skimming devices interfere with the ATM during its operation, the majority of the devices recovered from ATMs in South Africa fall in the category of devices that do not interfere with the operation of the ATM.

When the skimming device is inserted in the place of the actual card reader, the functioning of the ATM is interfered with. The magnetic strip data is captured by the skimming device when the client enters his card, but since the actual card reader has been removed, the ATM does not read or respond to the card. The customer will assume the machine is broken and leave the ATM unaware of the fact that his card has been skimmed.

The devices more frequently used in South Africa look like the card reader entry point on the ATM and are fitted over the factory installed card reader slot. The magnetic card reader in the skimming device acquires and stores the track data on the magnetic strip when the card is inserted to conduct an ATM transaction. As in the case of a handheld skimming device, the data can be retrieved by disconnecting the device and downloading the information using a computer. In the case of more advanced technology being employed, the data can also be transmitted to the perpetrator within reasonable proximity using wireless technology.

---

[380] The opportunity for fraud when an ATM is offline is significantly bigger than when online.
[381] Visser (n 333) 649.

Due to the fact that the high-tech skimmers are customised to fit precisely over the card slot of the targeted ATM, they only take seconds to install and remove. Since these devices are furthermore very small, fraudsters are not often caught "in the act" during the installation or removal. Having the appearance of a standard part of the terminal, high-tech skimmers are also very difficult to detect while attached to an ATM. Their retrieval is furthermore obstructed by the fact that the devices have usually already been removed when customers detect and report related fraudulent transactions on their bank accounts.

The risk of being identified and arrested using a high-tech skimming device is significantly lower than when a criminal uses a handheld skimmer. This explains the increase in use of ATM-mounted skimming devices in comparison to the more traditionally used handheld skimming devices.

2.2 Obtaining the PIN

Another piece of information that is essential for the successful use of a counterfeit card at an ATM, is the PIN of the owner of the legitimately issued card.

When a handheld skimming device is used to copy the encoded track data on the magnetic strip of a card, "shoulder surfing" is usually relied upon to obtain the PIN.[382]

In the case of an ATM mounted skimming device, the PIN was at first obtained either through shoulder surfing or by using a pin-hole camera which was concealed within trunking and placed directly above the PIN pad to observe the PIN entry. More recently these miniature cameras are being installed in the same customised piece of equipment containing the false card reader which is installed on top of the legitimate card reader. In the latter case the information is then either transmitted using a wireless device, or stored for subsequent downloading and use. Another method of obtaining the PIN occasionally encountered is the placing of a transparent plastic overlay on the keypad which appears to serve as a cover to

[382] "Shoulder surfing" takes place when the fraudster acquires the PIN by covertly observing the legitimate cardholder entering his or her PIN, usually by looking over the victim's shoulder.

keep the keypad clean, but in reality contains microchips recording the keystrokes when the PIN is entered.[383]

The skimmed card details and compromised PIN are subsequently matched for fraudulent use.[384]

2.3 Downloading the track data

Using the necessary software and USB cables, the data copied from the magnetic strips of cards is downloaded onto a computer. The software program required will depend on the skimming device used.[385]

3 *Manufacturing counterfeit cards*

The next phase in the life cycle and business value chain of counterfeit card fraud is the manufacturing of counterfeit cards. Criminals use technology to produce exact replicas of existing cards and to create fictitious payment cards from scratch. Previously counterfeit cards were usually manufactured using a silk screening process to duplicate the card logo and background onto a plain white plastic card. Advanced technology facilitates the manufacturing of counterfeit cards, complete with a hologram and fully encoded magnetic strip that is difficult to distinguish from the genuine bank payment card, through a multi-step process using computer equipment, embossers, laminators and tipping foil.

White plastic used for the manufacturing of bank payment cards is freely available and purchased for various legitimate purposes, such as access control at residential and business premises.

A card encoder and appropriate software are used to encode the magnetic strip of the counterfeit card with the stolen data of the legitimately issued card and to re-encode the magnetic strip of stolen and lost cards.

---

[383] Vrona "Automatic thieving machines: ATM frauds exposed" *The Kessler Report* 2006 vol 9 4.
[384] Hyland and Thornhill (ed) *Fraud Manager's Reference Guide* (2005) 169.
[385] Recently a number of skimming devices retrieved by the South African Police Service contained data in the format of sound files, which is indicative of more advanced technology being introduced by the fraudsters.

Various different embossing machines or embossers are available and used to convert the white plastic into a counterfeit card. The more recent models seized by the South African Police Services are modern and capable of producing an entire card, including trademark specific information.

Most embossing machines are imported. As with skimming devices the import of embossers is not regulated by South African legislation due to their widespread legitimate use in the banking, retail and education industries.

A tipper or automatic gilding press machine is used to tip and foil the embossed characters with gold or silver foil.

The authentic appearance of the counterfeit card is further enhanced by the adding of the hologram and logo of the card association on the front of the card and a signature panel on the back. Holograms can be stolen, obtained from used cards, ordered online or bought from a corrupt employee at one of the legitimate card manufacturing service providers,[386] while the logo can be scanned and printed if not stolen. Signature panels are purchased, scanned and printed or stolen.

Blank white plastic embossed and encoded with stolen account particulars can be used for fraudulent cash withdrawals at ATMs or purchases at merchants.

The data of a single compromised card can be used to manufacture a number of counterfeit cards used by different runners or mules.[387] This maximises the syndicate's ability to spend and/or draw cash before the compromise is detected and the card blocked in order to prevent further use.

3.1 The tools of the trade

As is evident from the above description a variety of equipment is required to manufacture counterfeit payment cards. Adding to the complexity of the combating of this crime type is the fact that all of these tools are freely available.

---

[386] Wells (n 343) 271 states that Visa and MasterCard suffered losses in excess of $700 m in 1994 caused by one Chinese hologram-producing syndicate alone.
[387] See par 5 below.

Due to the fact that cards are legitimately used for access control and monitoring of time and attendance and thus very common in South Africa,[388] equipment such as white plastic issued with magnetic strips, magnetic card readers and encoders is freely available, affordable and not regulated. Toolkits containing the said equipment are most of the time purchased online and imported, while the white plastic and encoders are also locally available. When imported, the equipment is often dismantled, brought into the country purportedly as components of other equipment and reassembled once collected by the fraudsters. The software required for downloading the data from the card readers or skimming devices is usually included in the toolkit, but can also be downloaded from the Internet free of charge.

Although corruption is still occasionally being used as a method to obtain the required data or other necessities such as the logos, holograms and signature panels, the use of technology to achieve the same objectives is winning ground. This is no surprise since it is not only simpler, but the risk of being identified, arrested and prosecuted is significantly less with the use of technology.

The availability and low cost of the tools of the trade has made this a relatively simple form of fraud of low risk to the fraudsters.

4 *Utilising counterfeit payment cards to obtain cash or merchandise*

The objective of counterfeit card fraud is to obtain cash, alternatively merchandise.

4.1 Obtaining cash

One can safely assume that the ultimate objective of using counterfeit cards is for the criminals to obtain cash, which is not only used to pay the members of the syndicate for their contributions, but also for a variety of other purposes, including the facilitation of a number of other criminal activities such as drug and human trafficking.

When merchandise is purchased using counterfeit cards, the merchandise is usually sold to generate cash. "Friendly merchants" will accept a counterfeit card as method of payment,

[388] Examples include secured residential areas, universities and most business premises.

issue a receipt reflecting the purchase of some goods, usually electronic equipment, while handing the fraudster cash instead.

The easiest way of mitigating the risk of being identified and arrested when obtaining cash using a counterfeit bank card is, however, to draw cash from an ATM. When high-tech skimmers are used, the victim's PIN is copied at the same time as the track data on the magnetic strip.[389] Subsequently manufactured counterfeit payment cards can thus immediately be used at a number of ATMs simultaneously to draw the money available in the customer's bank account. Using a counterfeit debit card, the fraudsters will have access to the overdraft facilities available to the account, whilst a counterfeit credit card will enable them to withdraw money against the credit limit extended to the card. The daily ATM withdrawal limit set by the bank in question will determine the maximum amount of cash that can be stolen in this manner from any targeted account in one day.

Although it has not yet been encountered locally, development of technology now seemingly also enables criminals to "convert skimmed cards into cash" without making a real purchase or drawing money from an ATM; all that is seemingly required is a credit card magnetic strip, the appropriate software and a laptop.[390]

4.2 Purchasing merchandise

When used to purchase merchandise, an altered, re-embossed or re-encoded stolen card is easier to detect than a complete reproduction of a counterfeit card.[391] With collusion of the retailer, referred to as a "friendly merchant", white plastic with only the details of a valid card being copied onto the magnetic strip is sometimes used to purchase merchandise.[392]

---

[389] Anonymous "ATM and debit card fraud" 2011 *Fraudguides* http://www.fraudguides.com/consumer-atm-debit-card-fraud.asp (7-8-2011).

[390] Kayle "iPad credit card reader hacked" 2011 *iTWeb Security* http://www.itweb.co.za/index.php?option=com_content&view=article&id=46057 : ipad-credit-card-reader-hacked&catid=234 (29-8-2011).

[391] To mitigate related losses bank investigators regularly provide retailers with training to detect counterfeit payment cards.

[392] Hyland and Thornhill (n 384) 161.

5 The perpetrators

The execution of the activities related to counterfeit card fraud involves various parties with different skills, roles and responsibilities and is perpetrated in an organised fashion.[393]

Foreigners are mostly used to obtain the tools of the trade. The required equipment is currently mostly imported from Bulgaria.

So-called runners or mules are usually employed for both the initial and the final phases of the lifecycle, albeit different runners generally operate in each phase. Service staff such as waiters and cashiers are often recruited and issued with skimming devices. They are then paid to use the skimming devices to obtain the track data on the magnetic strip of legitimate payment cards received by them during the normal course of business. Runners are also recruited to install and remove high-tech skimming devices mounted at ATM's. Finally, runners are employed to use the manufactured counterfeit payment cards to generate cash for the syndicate as described above.[394]

The back office responsibilities are executed by so-called intermediaries who are technologically skilled. They would typically be responsible for all the activities from downloading the data off the skimming devices up to manufacturing the final product, a counterfeit payment card ready for use.

The risk of being identified and arrested is significantly bigger for runners than for other members of the syndicate. Since the runners are easy to recruit, train and replace, their prosecution unfortunately does not disrupt the criminal activities of the syndicates behind this crime type.

---

[393] Wells (n 343) 580 adopts the Secret Service description of organised crime being "a loosely similar number of criminal groups, who sometimes cooperate with each other, and sometimes antagonize one another, but who generally conduct independent operations". For a discussion of the involvement of different organised crime groups in payment card fraud see the "Europol EU organised crime threat assessment 2011" 30 ff accessed through www.europol.europa.eu/content/publication/octa-2011-eu-organised-crime-threat-assessment-1465 (5-5-2012).

[394] See par 4 above. These runners will usually do similar work for a number of syndicates, regardless of whether the instrument is a counterfeit payment card or for instance a cloned or altered cheque.

CHAPTER 4

CONCLUSION AND RECOMMENDATIONS

As stated by Skeen, "Every advance made by the inventive and idealistic mind is rivalled by parallel developments of the deceitful and criminal mentality. The computer is no exception…."[395] The development of technology has provided previously unknown scope for the facilitation of fraud.[396] It has engendered new and more sophisticated forms of commercial crime and made the redistribution of the proceeds of crime quicker and more difficult to prevent and/or recover. Moreover, the almost endless new possibilities for misappropriating funds have been accompanied by a significant reduction in risk for the criminals stealing money and credit to be identified and apprehended.

"Card fraud and online identity theft are now arguably two of the fastest-growing computer crimes, facilitated by a combination of phishing and malware."[397]

A total of R680.4m was lost in South Africa during the period 1 October 2010 and 30 September 2011 due to South African-issued debit and credit card fraud, of which R449.9m resulted from counterfeit card fraud.[398] The prevalence of card skimming incidents and specifically incidents involving high-tech skimming devices, is concerning. Such arrests as have been made around these offences resulted in few prosecutions and mostly with insignificant sentences; this has had little if any deterring impact on a flourishing and very lucrative crime type. One therefore need to ask the question whether the South African criminal law has kept up with the development of crime or whether it is rather the application of our criminal law which is in dire need of attention.

In his inaugural lecture as professor in criminal law on 24 April 2002, Burchell pointed out that activities where a computer is used as an instrument to commit crime might already be adequately covered by existing common-law crimes.[399] A typical example pertinent to the crimes under discussion is the use of a counterfeit card to steal money from a legitimate

---

[395] Skeen "Computers and crime" 1984 *SACC* 262.
[396] Wilson "Cybercrime in the private sector: partnerships between the private sector and law enforcement" 2006 *Australian Law Journal* 694.
[397] Rowland *et al Information Technology Law* (2012) 103.
[398] SABRIC (n 349) 3 and 4.
[399] "Criminal justice at the crossroads" 2002 *SALJ* 579.

account holder or to defraud a bank or merchant through the drawing of cash at an ATM or the purchasing of merchandise. The common-law crimes of theft and fraud respectively sufficiently cater for these criminal activities.

During the same lecture Burchell warned against the so-called "blunderbuss" approach of simply resorting to the enactment of new offences rather than improving the detection and investigation of existing crimes:

> "Before succumbing to the crime-control model of criminal justice and developing new crimes to counter the ingenuity of the criminal mind, we need to answer two questions: (a) has a thorough and creative examination been done to determine whether the existing common or statutory law is inadequate to deal with the new or revived nefarious manifestation; and (b) does the cost in human and financial terms warrant the intervention of legislation, diverting already limited resources from the detection and prosecution of common-law crimes of violence to special and costly forms of law enforcement and to defending potentially time-consuming constitutional challenges to the legislation?"[400]

It is apparent from the discussion above that the South African law does to a large extend deal with counterfeit card fraud and that the focus should be on the effective application thereof by law enforcement agencies to ensure successful investigations and prosecutions. To ensure that fraudsters lose their appetite for this type of crime, it is, however, necessary for all the unlawful activities in the business value chain of counterfeit card fraud to be criminalised. Intervention by the legislature is thus necessary to facilitate prosecution of unlawful activities outside the ambit of the South African criminal law.

The criminalisation of the unlawful acquisition, possession, distribution and utilisation of all equipment required for the manufacturing of counterfeit payment cards (other than high-tech skimming devices and pinhole cameras which are already covered by both the ECT Act and RICA) will thus be a welcome addition to our law.

One can foresee difficulties in trying to prove the required intent if especially the acquisition, possession, and distribution of devices such as encoders, embossers and tippers are criminalised. The inclusion of presumptions in the related legislation should thus be considered to facilitate such prosecutions. However, it is unlikely that a clause placing the

[400] Burchell (n 399) 585.

burden of proof on the accused will pass constitutional muster.[401] It is thus recommended that the presumptions be formalised with a clear consideration for the criteria that have crystallised throughout the various relevant constitutional decisions.[402] In essence the broad objective of the reverse onus, namely the effective prosecution of crime, will only be considered sufficiently important if it can be shown that there is a pressing social need for the effective prosecution of the category of offences to which the presumption applies.[403]

There are furthermore a number of areas in respect of which offences created in legislation could be formulated with greater clarity and precision to either specifically deal with counterfeit card fraud or to provide for clearer and more understandable descriptions of devices used to access, copy and store data required for the manufacturing of counterfeit cards. It should not be necessary for prosecutors to force the facts of a case into the language of legislation that was clearly not designed to accommodate them.[404] Notwithstanding the fact that it would be appropriate to expand and develop the interpretation of the existing South African criminal law in such a way as to take account of advances in technology and its use, such modification has to remain consonant with the elements of the alleged offence; the law should not be stretched beyond its breaking point.[405]

It is a pity that South Africa does not have any statutory provisions dealing with the manufacturing, possession and use of counterfeit payment cards similar to the simple and straightforward provisions in respect of counterfeit coin and bank notes provided for in the Prevention of Counterfeiting of Currency Act and the South African Reserve Bank Act. It is recommended that the introduction of such provisions be considered by the legislature either for inclusion in one of the existing Acts dealing with related matters or as new legislation specifically aimed at criminalising the various activities related to card payment or non-cash

---

[401] See *Zuma* (n 201) where the constitutional court found s 217(1)(b)(ii) of the Criminal Procedure Act to be unconstitutional in that by placing the burden of proving the absence of voluntariness on the accused, it violated the presumption of innocence.
[402] *Zuma* (n 201); *Coetzee* (n 131); *Mbatha; Prinsloo* 1996 1 SACR 371 (CC); *Scagell v Attorney-General of the Western Cape* 1996 2 SACR 579 (CC); *Meaker* 1998 3 SACR 73 (W) and *Manamela* 2000 1 SACR 414 (CC). For a discussion on the infringement of the presumption of innocence see Schwikkard and Van der Merwe *Principles of Evidence* (2010) 514 ff.
[403] Schwikkard and Van der Merwe (n 402) 518 and *Scagell v Attorney-General of the Western Cape* (n 402) par 74.
[404] An example of this is the use of RICA to prosecute the possession and use of skimming devices.
[405] Rowland *et al* (n 397) 115.

payment fraud. The prevalence of this type of fraud, its impact on the community and the threat it poses to the economy, coupled with the challenges encountered during the investigation and prosecution thereof, clearly beg the introduction of specific legislation to combat counterfeit card fraud and to criminalise all the activities related thereto.

There is also a dire need for the revision of the penalty provision in the ECT Act. At present criminals do not feel the pain, they are merely inconvenienced. Harsher penalties are required to deter counterfeit card fraudsters and other cyber criminals. As per Langa J "Deterrence is, obviously, a legitimate objective which the state may pursue. We live in a crime-ridden society; the courts and other relevant organs of the state have a duty to make crime unattractive to those who are inclined to embark on that course."[406] As mentioned earlier, there is also a glaring disconnect between the sentences provided for in the ECT Act and those contained in legislation such as RICA and especially POCA.

One of the questions that Burchell advocates one should consider before deciding to develop new crimes to counter the ingenuity of the criminal mind, is whether the cost in human and financial terms warrants it.[407] The significant increase in the losses suffered as a result of counterfeit card fraud seems rather persuasive. Collier argues that the evolution of technology leaves no option but for the law to evolve itself in this regard.[408]

The emphasis of the Roman-Dutch law on tangibles lies at the roots of the struggle to apply our criminal law to intangibles such as data and information.[409] In my view the theft of data and information should be recognised in our law with its own *sui generis* principles and requirements similar to the theft of credit. The legislature's silence on the issue of theft and/or the unlawful copying of data and information seemingly leaves this aspect to the judiciary. An analysis of the law relating to the theft of credit leaves no doubt that our law has developed to the extent that the theft of incorporeal things is recognised.[410] The constitutional principle of legality will in all likelihood render our courts hesitant to develop the law much further in this

---

[406] *Williams* 1995 3 SA 632 (CC) par 80.
[407] (n 399) 585.
[408] Collier in Buys (ed) (n 166) 322.
[409] Van der Merwe "Computer crime- recent national and international developments" 2003 *THRHR* 30 43.
[410] Snyman "Die gemeenregtelike vermoënsmisdade en die eise van ons moderne samelewing" 1977 *SACC* 11 14 refers to this development of the common law as "'n broodnodige aanpassing van ons gemenereg by die besondere behoeftes van ons tyd".

regard. The endemic nature of criminal activity in this field, together with the social impact of this type of crime, make the time ripe for the legislator to intervene by means of a statutory provision in order to criminalise unauthorised copying and use of data and other information, as was previously done with the introduction of new offences related to, but not covered by, the common-law offence of theft.[411]

As the development of technology inspires more creative methods of accessing personal data and committing related crimes more speedily under a digital veil of anonymity, the timely detection and successful investigation of identity theft will become even harder. This will inevitably cause this already rampant phenomenon to proliferate even further. It is consequently recommended that the South African legislature follows international example by creating a statutory offence of identity theft.

Regardless of whether such proposed legislation is enacted, there still remain underutilised avenues to harness existing legislation against the offences I have discussed. For the fight against counterfeit card fraud to succeed it is vital for investigators and prosecutors to refrain from accepting pleas on statutory offences and unsatisfactory sentences. Instead, where supported by the evidence, reliance should be placed on common-law offences of fraud and theft, the doctrine of common purpose and conspiracy and proving the organised nature of the crime, or where appropriate on racketeering charges provided for in POCA. Charges under the ECT Act and RICA should, where possible, only be used in the alternative. Where appropriate, perpetrators should also be charged with other relevant statutory offences such as contraventions of the Immigration Act, the Identification Act and the Customs and Excise Act. Effective investigations and prosecutions will ensure suitable sentences. This will go a long way in combating this global phenomenon and threat to our economy.

[411] Examples of this include s 1 of the General Law Amendment Act 50 of 1956 and s 36 of the General Law Amendment Act 62 of 1955.

BIBLIOGRAPHY

Books

Burchell J *Principles of Criminal Law* 3rd ed Juta & Co Claremont (2005)

Buys R (ed) *Cyberlaw@SA II* 2nd ed Van Schaik Publishers Pretoria (2004)

Clough J *Principles of Cybercrime* 1st ed Cambridge University Press Cambridge (2010)

Currie I and De Waal J *The Bill of Rights Handbook* 5th ed Juta & Co Claremont (2005)

De Wet JC and Swanepoel HL *Die Suid-Afrikaanse Strafreg* 4th ed Butterworths Durban (1985)

Gering L *Handbook on the Law of Negotiable Instruments* 3rd ed Juta & Co Claremont (2007)

Hyland M and Thornhill S (ed) *Fraud Manager's Reference Guide* BBA Enterprises Ltd London (2005)

Malan FR, Pretorius JT and Du Toit SF *Malan on Bills of Exchange, Cheques and Promissory Notes* 5th ed LexisNexis Durban (2009)

Milton JRL *South African Criminal Law and Procedure vol III: Statutory Offences (formerly known as Gardiner and Lansdown)* 1st ed Juta & Co Cape Town (1971)

Milton JRL *South African Criminal Law and Procedure vol II: Common Law Crimes (formerly Gardiner and Lansdown)* 3rd ed Juta Cape Town (1996)

Rowland, Kohl and Charlesworth *Information Technology Law* 4th ed Routledge London (2012)

Schwikkard and Van der Merwe *Principles of Evidence* revised 3rd ed JUTA & Co Claremont (2010)

Snyman CR *Criminal Law* 5th ed LexisNexis Durban (2008)

Soanes C and Stevenson A *Concise Oxford English dictionary* revised 11th ed Oxford University Press Oxford (2009)

Van der Merwe D, Roos A, Pistorius P and Eiselen S *Information and Communications Technology Law* 1st ed LexisNexis Durban (2008)

Verma A *Cyber Crimes & Law* 1st ed Central Law Publications Allahabad (2009)

Walden I *Computer Crimes and Digital Investigations* 1st ed Oxford University Press Inc. New York (2007)

Wells JT *Encyclopedia of Fraud* 3rd ed Association of Certified Fraud Examiners Inc. Texas (2007)

Articles

Atta-Asamoah A "Understanding the West African cyber crime process" 2009 *Institute for Security Studies African Security Review* 107

Augustyn D "Identity theft escalation – you may need to change your life" 2005 *South African Journal of Information Management* 1

Barker GD "Trespassers will be prosecuted: computer crime in the 1990s" 1993 *Computer Law Journal* 61

Botha CR "*S v Myeza* 1985(4) SA 30 (T): Oor blikringetjies en boetebessies – aspekte van bedrog" 1986 *South African Journal of Criminal Justice* 72

Botha CR "Bedrog ten opsigte van die gebruik van tjek- en/of kredietkaarte" 1988 *South African Journal of Criminal Justice* 377

Botha CR "Sogenaamde 'rekenaarbedrog'" 1990 *South African Journal of Criminal Justice* 231

Burchell EM "Does potential prejudice suffice for fraud?" 1963 *South African Law Journal* 168

Burchell J "Criminal justice at the crossroads" 2002 *South African Law Journal* 579

Cameron E "Inferential reasoning and extenuation in the case of the Sharpeville Six" 1988 *South African Journal of Criminal Justice* 243

Carstens P and Trichardt A "Computer crime by means of the automated teller machine – just another face of fraud?" 1987 *South African Journal of Criminal Law and Criminology* 122

Casanova J "Establishing internet credit card programmes in the United Kingdom" 2001 *Journal of International Banking Law* 70

Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study" 2009 *Potchefstroom Electronic Law Journal* 36

Cassim F "Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players" 2011 *Comparative and International Law Journal of Southern Africa* 124

Coetzee J "Incoterms, electronic data interchange, and the Electronic Communications and Transactions Act" 2003 *South African Mercantile Law Journal* 1

Coetzee J "The Electronic Communications and Transactions Act 25 of 2002: Facilitating electronic commerce" 2004 *Stellenbosch Law Review* 501

Coetzee JA "Diefstal van onliggaamlike sake" 1970 *THRHR* 369

Cornelius S "The legal nature of payment by credit card" 2003 *South African Mercantile Law Journal* 153

Dijkman JH de V "Garage-card fraud, a solution?" 1986 *Businessman's Law* 35

Dreyer JW "Computer law in South Africa" 1983 *De Rebus* 534

Ebersöhn G "Catching hackers" 2004 *Juta's Business Law* 14

Ebersöhn GJ "A common law perspective on computer-related crimes (1)" 2004 *THRHR* 22

Ebersöhn GJ "A common law perspective on computer-related crimes (2)" 2004 *THRHR* 193

Ebersöhn GJ "A common law perspective on computer-related crimes (3)" 2004 *THRHR* 375

Eksteen JPG "Die bydrae van akademici tot die regspleging" 1984 *Obiter* 1

Faul W "Die 'smart' kaart – hoe werk dit?" 1989 *South African Mercantile Law Journal* 381

Henning JJ and Ebersöhn GJ "Insider trading, money laundering and computer crime" 2001 *Transactions of the Centre of Business Law: Combatting Economic Crime* 105

Horwitz G "Computer abuse – the legal implications" 1986 *De Rebus* 503

Kleyn D "Dogmatiese probleme rakende die rol van onstoflike sake in die sakereg" 1993 *De Jure* 3

Labuschagne JMT "*De minimis non curat lex* as strafregtelike verweer in 'n regstaat: opmerkinge oor strafsinvolheid en die groeiende rasionele dimensie van geregtigheid" 2003 *THRHR* 455

Lawack VA "Electronic innovations in the payment card industry" 1998 *South African Mercantile Law Journal* 233

Lawack-Davids V and Marx FE "Consumer protection measures for erroneous or unauthorised internet payments: some lessons from the European Union" 2010 *Obiter* 446

Legwaila T "Seizure and forfeiture in terms of the Customs and Excise Act 91 of 1964: rigid application continues, but what about the legislative rationale? A note relating to *Capir Oro (Pty) Ltd v Commissioner of Customs and Excise* 2001(4) SA 1212 (SCA) as a basis" 2002 *Stellenbosch Law Review* 444

Le Roux DJ "Diefstal deur middel van die rekenaar" 1985 *De Rebus* 401

Le Roux J "Die aard van diefstal as voortdurende misdaad in die Suid-Afrikaanse strafreg" 2005 *THRHR* 472

Loubser MM "Sekere probleme in verband met diefstal van geld" 1978 *De Jure* 86

Makakaba P "Rubber cheques" 2007 *Juta's Business Law* 17

Makakaba P "Credit card holder's conduct and credit limit" 2007 *Juta's Business Law* 71

Malan FR "The liberation of the cheque" 1978 *Tydskrif vir die Suid-Afrikaanse Reg* 107

Matzukis NA "The nature and scope of common purpose" 1988 *South African Journal of Criminal Justice* 226

Naude CMB "Rekenaarmisdaad: 'n skewe beeld?" 1983 *South African Journal of Criminal Law and Criminology* 165

Neethling J "S v A 1971 2 SA 213 (T)" 1971 *THRHR* 324

Neethling J "The concept of privacy in South African law" 2005 *South African Law Journal* 18

Oelofse AN "Enkele regsaspekte van ontwikkelings in die bankwese" 1986 *Modern Business Law* 6

Otto JM "Credit card transactions and a spouse's consent in terms of the Matrimonial Properties Act" 1997 *Tydskrif vir Suid-Afrikaanse Reg* 216

Paizes A "Common purpose by active association: some questions and some difficult choices" 1995 *South African Law Journal* 561

Rabie A "Kousaliteit en 'common purpose' by moord" 1988 *South African Journal of Criminal Justice* 234

Reddi M "The doctrine of common purpose receives the stamp of approval" 2005 *South African Law Journal* 59

Schulze WG "E money and electronic fund transfers. A shortlist of some of the unresolved issues." 2004 *South African Mercantile Law Journal* 50

Schulze WG "Countermanding an electronic funds transfer: the supreme court of appeal takes a second bite at the cherry" 2004 *South African Mercantile Law Journal* 667

Schulze WG "Smart cards and e-Money: new developments bring new problems" 2004 *South African Mercantile Law Journal* 703

Schulze WG "Of credit cards, unauthorised withdrawals and fraudulent credit-card users" 2005 *South African Mercantile Law Journal* 202

Schulze WG "Duty of a bank to act with necessary skill and care when issuing an automated teller machine card" 2007 *De Jure* 370

Skeen A St Q "Crimes committed by computer" 1984 *Businessman's Law* 9

Skeen A St Q "Computers and crime" 1984 *South African Journal of Criminal Law and Criminology* 262

Snail S "Cyber crime in the context of the ECT Act" 2008 *Juta's Business Law* 63

Snyman CR "Die begrip "toe-eiening" in die omskrywing van diefstal" 1975 *THRHR* 29

Snyman CR "Die gemeenregtelike vermoënsmisdade en die eise van ons moderne samelewing" 1977 *South African Journal of Criminal Law and Criminology* 11

Snyman CR "Die misdaad sameswering" 1984 *South African Journal of Criminal Law and Criminology* 3

Stassen JC "Some legal aspects of credit cards – III Paying by credit card" 1978 *Businessman's Law* 12

Stassen JC "Betaling deur middel van 'n driepartykredietkaart" 1978 *De Jure* 134

Stassen JC and Meiring I "Ongemagtigde kredietkaartgebruik: wie dra die skade?" 1979 *Modern Business Law* 28

Thomas PH "The South African common law into the twenty-first century" 2005 *Tydskrif vir Suid-Afrikaanse Reg* 292

Van der Berg J "The criminal act of violation of dignitas" 1988 *South African Journal of Criminal Justice* 351

Van der Bijl C "The cloning of credit cards: the dolly of the electronic era" 2007 *Stellenbosch Law Review* 331

Van der Bijl C "SIM-card swapping, mobile phone banking fraud and RICA 70 of 2002" 2009 *South African Mercantile Law Journal* 159

Van der Merwe D "Computer crime- recent national and international developments" 2003 *THRHR* 30

Van der Merwe D "Information technology crime – a new paradigm is needed" 2007 *THRHR* 309

Van der Merwe DP "Computer Crime" 1983 *Obiter* 124

Van der Merwe DP "Diefstal van onliggaamlike sake met spesifieke verwysing na rekenaars" 1985 *South African Journal of Criminal Law and Criminology* 129

Van Rensburg J "Intercepting communications and providing communication related information" 2003 *Juta's Business Law* 90

Visser C "Banking in the computer age: the allocation of some of the risks arising from the introduction of automated teller machines" 1985 *South African Law Journal* 646

Visser C "The evolution of electronic payment systems" 1989 *South African Mercantile Law Journal* 189

Vrona N "Automatic thieving machines: ATM frauds exposed" 2006 *The Kessler Report* 4

Watney M "Die strafregtelike en proseduele middele ter bekamping van kubermisdaad (deel 1)" 2003 *Tydskrif vir Suid-Afrikaanse Reg* 56

Watney M "Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)" 2003 *Tydskrif vir Suid-Afrikaanse Reg* 241

Watney M "Identity theft – the dangerous imposter" 2004 *De Rebus* 20

Watney M ""Identity theft": the mirror reflects another face" 2004 *Tydskrif vir Suid-Afrikaanse Reg* 511

Whiting R "Joining in" 1986 *South African Law Journal* 38

Wilson J "Cybercrime in the private sector: partnerships between the private sector and law enforcement" 2006 *Australian Law Journal* 694

South African law commission papers

South African Law Commission *Computer-related crime: preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects* Paper 99 Project108 (2001)

South African reports

SABRIC *Card fraud South Africa 2010 -2011*

SABRIC Commercial Crime Office *2011 Annual Report*

International reports, working papers and convention

African Union Commission *Draft African Union convention on the establishment of a credible legal framework for cyber security in Africa* 2011

Western Australia Standing Committee on Uniform Legislation and Statutes Review *Report on Criminal Code Amendment (Identity Crime) Bill* 2010

Legislation

Constitution of the Republic of South Africa, Act 108 of 1996

Counterfeit Goods Act 37 of 1997

Criminal Procedure Act 51 of 1977

Customs and Excise Act 91 of 1964

Documentary Evidence from Countries in Africa Act 62 of 1993

Electronic Communications Act 36 of 2005

Electronic Communications and Transactions Act 25 of 2002

General Law Amendment Act 62 of 1955

General Law Amendment Act 50 of 1956

Identification Act 68 of 1997

Immigration Act 13 of 2002

National Payment System Act 78 of 1998

Prevention and Combating of Corrupt Activities Act 12 of 2004

Prevention of Counterfeiting of Currency Act 16 of 1965

Prevention of Organised Crime Act 121 of 1998

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Riotous Assemblies Act 17 of 1956

South African Reserve Bank Act 90 of 1989

Telecommunications Act 103 of 1996

Trade Marks Act 194 of 1993

International legislation

Criminal Law Consolidation (Identity Theft) Amendment Act 2004 (South Australia)

Electronic Fund Transfer Act of 1978 (United States)

Identity Theft and Assumption Deterrence Act of 1998 (United States)

Identity Theft Enforcement and Restitution Act of 2007 (United States)

Case law

Afrox Healthcare Bpk v Strydom 2002 6 SA 21 (SCA)

Amod v Multilateral Motor Vehicle Accidents Fund 1998 4 SA 753 (CC)

Brinsley v Drotsky 2002 4 SA 1 (SCA)

Carmichele v Minister of Safety and Security 2001 4 SA 938 (CC)

Delange v Costa 1989 2 SA 857 (A)

Ex parte Lebowa Development Corporation Ltd 1989 3 SA 71 (T)

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 2 SA 451 (A)

Libazi v S 2011 1 All SA 246 (SCA)

Masiya v Director of Public Prosecutions, Pretoria 2007 2 SACR 435 (CC)

Narlis v South African Bank of Athens 1976 2 SA 573 (A)

Osman v Attorney-General, Transvaal 1998 2 SACR (CC)

Pharmaceutical Manufacturers Association of SA; In re Ex parte President of Republic of South Africa 2000 2 SA 674 (CC)

Premier Western Cape v Parker & Mohammed 1999 1 All SA 176 (C)

R v B 1958 1 SA 199 (A)

R v Brand 1960 3 SA 637 (A)

R v Cilliers 1937 AD 278

R v Dyonta 1935 AD 52

R v Geere 1952 2 SA 319 (A)

R v Heyne 1956 3 SA 604 (A)

R v Heyne 1958 1 SA 607 (W)

R v Hymans 1927 AD 35

R v Joffe 1934 SWA 108

R v Kruger 1961 4 SA 816 (A)

R v Larkins 1934 AD 91

R v Mall 1959 4 SA 607 (N)

R v Manuel 1953 4 SA 523 (A)

R v Miller 1939 AD 106

R v Milne and Erleigh (7) 1951 1 SA 791 (A)

R v Mlooi 1925 AD 131

R v Monyane 1960 3 SA 20 (T)

R v Muller 1953 2 SA 146 (T)

R v Reynolds 1924 TPD 607

R v S 1959 1 SA 680 (C)

R v Schoombie 1945 AD 541

R v Scoulides 1956 2 SA 388 AD

R v Seabe 1927 AD 28

R v Sedat 1916 TPD 431

R v Shezi 1948 2 SA 119 (A)

R v Sibiya 1955 4 SA 247 AD

R v Von Elling 1945 AD 234

Reid-Daly v Hickman 1981 2 SA 315 (ZA)

S v A 1971 2 SA 293(T)

S v African Bank of SA Ltd 1990 2 SACR 585 (W)

S v Agliotti 2010 JOL 26556 (GSJ)

S v Augustine 1986 3 SA 294 (C)

S v Avion Motor Enterprises (Pty) Ltd 1978 4 SA 692 (T)

S v Banur Investments (Pty) Ltd 1970 3 SA 767 (A)

S v Basson 2000 1 SACR 1 (T)

S v Boesak 2000 1 SACR 633 (SCA)

S v Cassiem 2001 1 SACR 489 (SCA)

S v Coetzee 1997 3 SA 527 (CC)

S v Cooper 1976 2 SA 875 (T)

S v Dayizana 1989 1 SA919 (E)

S v Del Ré 1990 1 SACR 392 (W)

S v Dlamini; S v Dladla; S v Joubert; S v Schietekat 1999 4 SA 623 (CC)

S v Foo Hui Ooi case no CCC1/32/11 East London Commercial Crime Court (unreported)

S v Francis 1981 1 SA 230 (ZA)

S v Fraser 2005 1 SACR 456 (SCA)

S v Friedman (1) 1996 1 SACR 181 (W)

S v Gardener 2011 4 SA 79 (SCA)

S v Gathercole 1964 1 SA 21 (A)

S v Goosen 1989 4 SA 1013 (A)

S v Graham 1975 3 SA 569 AD

S v Hammer 1994 2 SACR 496 (C)

S v Harper 1981 2 SA 638 (D)

S v Heller 19712 SA 29 (A)

S v I 1976 1 SA 781 (RA)

S v Isaacs 1968 2 SA 187 (D)

S v Jana 1981 1 SA 671 (T)

S v Judin 1969 4 SA 425 (A)

S v Kearney 1964 2 SA 495 (A)

S v Kgogong 1980 3 SA 600 (A)

S v Khambule 2001 1 SACR 501 (SCA)

S v Khumalo 1991 4 SA 310 (A)

S v Kimmich 1996 2 SACR 200 (C)

S v Kotze 1965 1 SA 118 (A)

S v Kruger 1989 1 SA 785 (A)

S v Lungile 1999 2 SACR 597 (SCA)

S v Luther 1962 3 SA 506 (A)

S v Makwanyane 1995 3 SA 391 (CC)

S v Malinga 1963 1 SA 692 (A)

S v Mambo 2006 2 SACR 563 (SCA)

S v Manamela 2000 1 SACR 414 (CC)

S v Mbatha; S v Prinsloo 1996 1 SACR 371 (CC)

S v Mbokazi 1998 1 SACR 438 (N)

S v Meaker 1998 2 SACR 73 (W)

S v Mgedezi 1989 1 SA 687 (A)

S v Mintoor 1996 1 SACR 514 (C)

S v Mokoena D3001/2010 Witbank Magistrates Court (unreported)

S v Momberg 1970 2 SA 68 (C)

*S v Mongalo*1978 1 SA 414 (O)

S v Moodie 1983 1 SA 1161 (C)

S v Mostert 2006 1 SACR560 (N)

S v Motaung 1990 4 SA 485 (A)

S v Moumbaris 1974 1 SA 681 (T)

S v Murbane 1992 1 SACR 298 (NC)

S v Myeza 1985 4 SA 30 (T)

S v Naryan 1998 2 SACR 345 (W)

S v Nedzamba 1993 1 SACR 673 (V)

S v Ngobozi 1972 3 SA 476 (A)

S v Nkwenja 1985 2 SA 560 (A)

S v Ntsele 1997 2 SACR 740 (CC)

S v Nzo 1990 3 SA 1 (A)

S v Ressel 1968 4 SA 224 (A)

S v Safatsa 1988 1 SA 868 (A)

S v Salceda 2003 1 SACR 324 (SCA)

S v Shaik 1983 4 SA 57 (A)

S v Shaik 2007 1 SA 240 (SCA)

S v Sharp 2002 1 SACR 360 (Ck)

S v Sibuyi 1993 1 SACR 235 (A)

S v Singo 1993 2 SA 765 (A)

S v Snyman 1984 SACC 3

S v Stanley 2010 JOL 26252 (ZH)

S v Thebus 2003 6 SA 505 (CC), 2003 2 SACR 319

S v Twala 1979 3 SA 864 (T)

S v Van Coller 1970 1 SA 417 (A)

S v Van den Berg 1991 1 SACR 104 (T)

S v Van Niekerk 1981 3 SA 787 (T)

S v Visagie 1991 1 SA 177 (A)

S v Williams 1995 3 SA 632 (CC)

S v Windvogel 1998 1 SACR 125 (C)

S v Xotongo case no 29/08 Matatiele Magistrates Court (unreported)

S v Zuma 1995 2 SA 642 (CC)

Scagell v Attorney-General of the Western Cape 1996 2 SACR 579 (CC)

Thesis

Botha, CR "Bedrog in die Suid-Afrikaanse Strafreg" LLD thesis, University of South Africa (1988)

Loubser, MM "The theft of money in South African law" D Phil thesis, University of Oxford (1977)
Maat, S "Cyber crime: A comparative analysis" LLM thesis, University of South Africa (2004)

Newspapers, magazines and gazettes

Government Gazette 23809 (30 August 2002)

Government Gazette 28371 (29 December 2005)

Personal Finance Newsletter (13 March 2008) Mhlanga D "Credit card fraud on the rise…but the banks are fighting back with new technology."

Personal Finance Newsletter (January 2010) 8 Fisher-French M "Chip-and-PIN cards: They're not as safe as you think…"

Personal Finance Newsletter (July 2010) 8 Pillay K "Tips to prevent being a victim of fraud at an ATM"

The Professional Accountant (May/June 2009) 24 Anonymous "Counterfeit cards drive up card fraud losses"

Internet sources

Anonynous "ATM and debit card fraud" 2011 *Consumer Fraud* http://www.fraudguides.com/consumer-atm-debit-card-fraud.asp (7-8-2011)

Anonymous "Facts about credit card fraud" 2011 *Shopping Guides Online for consumers* http://www.infofaq.com/fraud/credit-card/index.html (7-8-2011)

"Australian Crime Commission report on card fraud 2011" http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/card-fraud (30-4-2012)

"Automatic teller machine the history of computing project" http://www.thocp.net/hardware/atm.htm (5-5-2012)

Biba E "Burning question: why are ATM cards still so vulnerable to fraud?" 2011 http://www.wired.com/magazine/2011/02/pr_burning_atm_fraud/ (7-8-2011)

Criminal division of the United States Department of Justice "Hacker pleads guilty to identity theft and credit card fraud resulting in losses of more than $36 million" 21-4-2011 http://www.justice.gov/opa/pr/2011/April/11-crm-501.html (30-4-2012)

"EUROPOL EU organised crime threat assessment" (28-4-2011) www.europol.europa.eu/content/publication/octa-2011-eu-organised-crime-threat-assesment-1465 (5-5-2012)

Financial Fraud Action UK "Counterfeit card fraud facts" 2011 http://www.financialfraudaction.org.uk/Financial-Counterfeit-Fraud.asp (30-4-2012)

http://en.wikipedia.org/wiki/Automated_teller_machine (30-4-2012)

Kayle A "iPad credit card reader hacked" 2011 *iTWeb Security* http://www.itweb.co.za/index.php?option=com_content&view=article&id=46057:ipad-credit-card-reader-hacked&catid=234 (29-8-2011)

Kitten T "ATM skimming spree investigated" 2-9-2011 http://www.bankinfosecurity.com/articles/html (26-4-2012)

MacDonald E "Citi says number of credit cards hacked was actually 360,000" 16-6-2011 http://news.consumerreports.org/money/2011/06/citi-says-number-of-credit-cards-hacked-was-actually-360000.html (30-4-2012)

Mangis C "Global Payments breach puts 1.5 million credit card numbers at risk" 2-4-2012 http://news.consumerreports.org/money/2012/04/global-payments-breach-puts-15-million-credit-card-numbers-at-risk.html (30-4-2012)

McGlasson L "Network Solutions data breach: 573 000 cardholders at risk" 28-7-2009 http://www.bankinfosecurity.com/articles.php?art_id=1660 (7-9-2011)

"Payment fraud statistics – summary of results fraud perpetrated on Australian issued payment instruments 1 July 2010 - 30 June 2011" http://www.apca.com.au/docs/fraud_statistics_2011a_printfriendly.pdf (2-5-2012)

"Phishing activity trends report 1st half 2011" www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf (5-5-2012)

Poremba SM "What identity thieves want from a data breach" 25-4-2012 http://www.msnbc.mns.com/id/47179180#.T51F7fFhiSM/html (26-4-2012)

Sullivan B "Debit card thieves get around PIN obstacle. Wave of ATM fraud indicates criminals have upped the ante." 3-9-2006 http://www.msnbc.msn.com/id/11731365/ns/technology_and_science-security/html (26-4-2012)

"The UK Cards Association annual report 2012 released 27-1-2012" www.theukcardsassociation.org.uk/press_release/index.asp (5-5-2012)

Consultations

Fryer P: Director Operations, Risk Diversion (Pty) Ltd (10-8-2011)

Greetham R: Customer Risk and Security Services, MasterCard Worldwide APMEA (29-8-2011)

Nel K: Head Credit Card Fraud, Nedbank Ltd (11-9-2011)

Olivier S: Head of Point of Sale, HA and S1Switch, Nedbank Ltd (19-4-2012)

Potgieter S: General Manager, Commercial Crime Office, SABRIC (20-12-2011)

Van Wyk J: National Coordinator, Commercial Crime Banking Group, Directorate for Priority Crime Investigations, South African Police Service (11-8-2011)