THE CLONING OF CREDIT CARDS: THE DOLLY OF THE ELECTRONIC ERA

Charnelle van der Bijl
BLC LLB LLD
Senior Lecturer, Department of Mercantile law, University of Stellenbosch

1 Introduction

The long-awaited and much-anticipated EMV (Europay, Mastercard and Visa) system aimed at combating credit and debit card fraud has recently been launched by ABSA. VISA branded debit cards will contain a special chip and transactions will be verified, using a four-digit personal identification number, which will be keyed in instead of the signing of receipts.[1] The introduction of the EMV bank chip smart card system, which is to replace magnetic stripe cards with microchip cards, is aimed at eliminating the risks of unauthorised use.[2] A smart card is a plastic card based on cryptography with a microcomputer chip in it, which is swiped at a payment terminal, or smart card reader that verifies the smart card as being genuine by sending a random code. This code in turn is responded to by the microchip, which together with a security access code such as a PIN (Personal Identification Number), acts as a type of secret key.[3] Smart card technology therefore refers to the microcomputer-embedded technology linked to the card rather than to the purpose of the card.[4]

The cloning of payment instruments poses a formidable challenge to banks and consumers. The cloning of credit and debit cards is often referred to as skimming, which entails that the magnetic strip on the back of a credit card is copied using a hand held card reader.[5] Magnetic-stripe card technology is therefore flawed in the sense that the data stored on the stripe can be altered by a person who has access to the device which records the information and the magnetic-stripe credit card can be replicated (cloned) on a personal computer.[6]

---

1 "ABSA, VISA Launch Product to Curb Card 'Skimming'" *Business Day* Friday May 4 2007 19 See also Schulze "E Money and Electronic Fund Transfers" 2004 16 *SA Merc LJ* 50 54-56 for a discussion of the nature of smart cards

2 Schulze 2004 16 *SA Merc LJ* 53 and n 21 See further Havenga & Havenga, Kelbrick, McGregor, Schulze, Van der Linde & Van der Merwe *General Principles of Commercial Law* (2004) 390-391 EMV (Europay, Mastercard and Visa) is a global card standard that has been accepted by South Africa, but which remains to be fully implemented despite the implementation date being 1 January 2005 This card has a digital signature, and transaction slips will no longer be needed

3 Havenga *et al Kommersiële Reg* 410-411 Schulze 2004 16 *SA Merc LJ* 55 See also Schulze "Smartcards and E-money: New Developments Bring New Problems" 2004 16 *SA Merc LJ* 703 707

4 Schulze 2004 16 *SA Merc LJ* 53

5 *Business Day* Friday May 4 2007 19

6 Schulze 2004 16 *SA Merc LJ* 55

Following on from our previous article on cloned cheques,[7] the focus of this article will be on cloned credit cards. It will be investigated whether the EMV system is a miracle cure to credit card cloning in particular, or whether pitfalls exist, which need to be guarded against. During the transition period from the current credit card system to the bank chip smart card, it will no doubt be important to ensure that both types of credit card are interoperable and that terminals would be able to accept both magnetic stripes and magnetic chips.[8] This in itself will not be without its own challenges, especially as far as the prevention of cloned credit cards is concerned, as has since been discovered in France and the United Kingdom which already implement the EMV system.[9]

In France, algorithmic research (ARX) has uncovered security problems related to the exposure of PIN codes of magnetic stripe and EMV cards used at ATM's (Automated Teller Machines).[10] Anyone with access to the PIN verification facility could use hardware to reveal the PIN codes and either perpetrate fraudulent transactions or manufacture cards with different PIN codes to those of the legitimate cards.[11] The French system experienced further setbacks as some electric point terminals used for smart cards still had magnetic swipe readers. The reason for this is that certain ATM cash terminals were only able to use data stored on the cards' magnetic stripe due to incompatibility problems with cards embedded with chip technology.[12] Serge Humpich, a 36 year-old engineer, discovered flaws in the smart card microchip system used in France and actually managed to crack the French banking smart card system by fabricating a fake smartcard that was recognised by electronic point of sale terminals.[13]

A further report on fraud-related EMV payment, perpetrated at petrol stations with unattended payment terminals, has been made in the United Kingdom. Money has reportedly been stolen from customers after their payment card data was skimmed (cloned). The reason cited for this is that the cards were swiped through a magnetic stripe reader, which captured the data. In the process, the terminal also detected whether a chip was present and the transac-

---

7 Pretorius & Van der Bijl "A New Mode of Forgery: The Rise of Cloned and Washed Cheques" 2006 18:2 *SA Merc LJ* 196

8 Schulze 2004 16 *SA Merc LJ* 56

9 "Card Technology" *Newsroom Global Newswatch* vol 11 06/01/06 Card Tech 8 2006 WLNR 9391895; "French Card Hacker Convicted" available at http://www theregister co uk/2000/02/26/french_card_hacker_convicted (accessed 10 May 2007)

10 "Algorithmic Research Reveals PIN Processing Weakness that Allow Payment-Card Fraud" available at http:// www smartcardstrends com/det_atc php?idu (accessed 8 May 2007) See also *Diners Club SA (Pty) Ltd v Singh* 2004 3 SA 630 (D)

11 "Algorithmic Research Reveals PIN Processing Weakness that Allow Payment-Card Fraud" available at http:// www smartcardstrends com/det_atc php?idu (accessed 8 May 2007)

12 "French Card Hacker Convicted" available at http://www theregister co uk/2000/02/26/french_card_hacker_convicted (accessed 10 May 2007)

13 "French Card Hacker Convicted" available at http://www theregister co uk/2000/02/26/french_card_hacker_convicted (accessed 10 May 2007) See further "Security: Hackers Reveal How to Forge a Bank Card" available at http:// www tla ch/TLA/NEWS/2000sec/20000317credicard htm There it is mentioned that the information hacked included deciphered codes which validated forgeries where microchip-carrying cards were fed into ATM's, or mobile phone style terminals where amounts are immediately debited once the card has been read and the PIN number has been entered See further "Smart Card Crypto Genius Sent to Trial" available at http:// the register co uk/2000/01/23/smart-card-crypto-genius-sent (accessed 8 May 2007)

tion was completed with the detection of the chip.[14] Once magnetic-stripe and PIN data are captured, cards can be cloned, thus enabling the perpetration of ATM fraud.

The EMV system is undoubtedly a welcome advancement in technology. However, it will be shown that the cloning of credit cards will not necessarily disappear for a number of reasons. First, problems will remain where certain banks or issuers of tripartite credit cards have not implemented the system.[15] Secondly, there might be flaws in the system related to the migration or transition process, which have not yet become apparent as has been the case in the United Kingdom and France, where the smart card bank chip system has already been implemented. Thirdly, due to the expense involved, this form of technology might not be utilised in bipartite credit cards.[16] Lastly, problems could still emerge where purchases are made telephonically or over the internet. These are merely some of the practical problems that may occur. An important question that must of necessity be asked, relates to risk allocation. Should the cardholder bear the largest part of the risk or should the risk rest with the bank or issuer of the card? This question can perhaps best be answered by distinguishing between the position pertaining to unauthorised use of the original credit card and the position where there is unauthorised use involving a cloned credit card. Both these positions will be explored after delving into the nature of a credit card relationship.

2 The nature of a credit card and the legal relationships between the parties

A credit card is an instrument of payment. It is issued by the card issuer to the cardholder, who enjoys revolving credit and can use the card to draw cash or to purchase goods or services up to a prescribed limit. The amount provided in credit should then be paid back within a specific period, and interest becomes payable on certain outstanding amounts.[17] There are usually three parties to a credit card transaction, namely the cardholder (consumer), the issuer (credit provider)[18] and the supplier. The transaction is usually implemented by way of a direct payment-obligation scheme based on a standard type contract.[19] Bilateral credit cards would involve two parties, namely the issuer/supplier, who would usually be the same party, and the cardholder. Credit cards have a number of purposes, and are mainly used for ATM withdrawals, internet and telecon shopping, and sale or service agreements.

---

[14] "Card Technology" *Newsroom Global Newswatch* vol 11 06/01/06 Card Tech 8 2006 WLNR 9391895

[15] The terms issuer/credit provider will be used interchangeably as well as cardholder/consumer in keeping in line with the terminology used in the National Credit Act 34 of 2005

[16] There may, however, also be only two parties involved in credit card transactions, for example, if the supplier is also the issuer of the card, which is often the case with certain chain stores

[17] Schulze "Of Credit Cards, Unauthorized Withdrawals and Fraudulent Credit-Card Users" 2005 17 *SA Merc LJ* 202; Cornelius "The Legal Nature of Payment by Credit Card" 2003 15 *SA Merc LJ* 153 156-157; *R v Lambie* 1981 2 All ER 776 (HL)

[18] A credit provider is the party who extends credit under a credit facility (s 1 of Act 34 of 2005)

[19] Nagel & Roestoff *Commercial Law* (2000) 410 *et seq* Note that the 2006 version of this textbook does not contain references to the relationships on a credit card, which is why the earlier version is used

Nagel & Roestoff[20] state that:

> "The issuer enters into a standard-form contract with the various suppliers, in terms of which the latter undertake to accept payment for goods or services by means of the credit cards issued by the former, while the issuer undertakes to refund the suppliers, subject to certain conditions and usually minus a certain percentage, for purchases made by the card holder. The issuer, therefore, takes upon himself the obligation to pay directly to the supplier. The issuer also enters into a standard-form contract with every card holder which contains the conditions of use of the card and in terms of which the card holder may make payments up to a certain credit limit, the issuer debits the card holder with the amounts spent and the latter undertakes to repay these amounts, or a portion thereof, within a specific time directly to the issuer."

The different types of relationship between the parties to a credit card transaction can be summarised as follows:[21]

- The cardholder is normally authorised by the bank to obtain services or purchase goods from various suppliers. The cardholder will be liable to reimburse the issuer once the latter has carried out the instructions of the cardholder and paid the relevant supplier.
- The relationship between the supplier and cardholder would be determined by the underlying contract, such as a contract of sale, between them. Upon completion and signing of a transaction slip, the supplier obtains a personal right against the issuer and the cardholder's obligation will merely be suspended until the supplier is paid by the issuer. Should payment not take place, the cardholder will be liable.
- The relationship between supplier and issuer will usually entail that the issuer will reimburse the supplier in terms of their standard contract, which will also usually make provision for the presentation of the transaction slips to the issuer by the supplier.

The legal relationship between the parties to the credit card agreement could therefore be said to be regulated by the contract itself, the general principles of contract law and the National Credit Act 34 of 2005.[22] The National Credit Act 34 of 2005 replaces both the Credit Agreements Act 75 of 1980 and the Usury Act 68 of 1973 and covers a wide spectrum of credit agreements. A credit agreement is a credit transaction, credit facility, or a credit guarantee, or a combination of these three transactions.[23] An agreement is defined in section 1 as including an arrangement or understanding between or among two or more parties, which purports to establish a relationship in law between those parties.

---

[20] *Commercial Law* 411

[21] See Nagel *et al Commercial Law* 411-414, esp 413 where it is mentioned that the liability of a cardholder towards the issuer is based on mandate and loan for consumption; Oosthuizen (ed) *Suid-Afrikaanse Handelsreg* (1993) 149; Cornelius 2003 15 *SA Merc LJ* 153 163-171 for an alternate discussion of payment by credit card as being made in terms of an antecedent multilateral contract based primarily on delegation and novation; Schulze 2005 17 *SA Merc LJ* 202 204; Havenga *et al General Principles of Commercial Law* (2004) 370; Sharrock *Business Transactions Law* (2002) 194-195

[22] Note that The Electronic Communications and Transactions Act (ECTA) 25 of 2002 does not provide exclusively for credit card schemes or electronic banking services for that matter and will therefore not be discussed further

[23] S 8(1) of Act 34 of 2005

The provisions pertaining to credit facilities are applicable to credit card transactions. A credit facility is defined as such in section 8(3) of the National Credit Act 34 of 2005 if in terms of that agreement:

"(a) A credit provider undertakes–
  (i) to supply goods or services or to pay an amount or amounts, as determined by the consumer from time to time, to the consumer or on behalf of, or at the direction of, the consumer; and
  (ii) either to–
    (aa) defer the consumer's obligation to pay any part of the cost of goods or services, or to repay to the credit provider any part of an amount contemplated in (i) or
    (bb) bill the consumer periodically for any part of the cost of goods or services, or any part of an amount, contemplated in (i) and
(b) any charge, fee or interest is payable to the credit provider in respect of –
  (i) any amount deferred as contemplated in paragraph (a)(ii) (aa) or
  (ii) any amount billed as contemplated in paragraph (a) (ii) (bb) and not paid within the time provided in the agreement."

The Act therefore applies to both bipartite and tripartite credit cards. It would appear that the Act would apply to credit cards issued to the cardholder on the latter's insistence. It is therefore doubtful whether the Act could apply to a cloned credit card as the latter is not issued to the credit cardholder (consumer) on such person's insistence and consensus or an understanding between the parties would be lacking. It becomes increasingly important to establish exactly as to what has been agreed upon in order to bind the cardholder to the contract and also for the determination of risk allocation. It is not unheard of for issuers to post credit cards (especially bipartite credit cards) to prospective and identified consumers in order to invite them to make use of a card with a pre-approved limit. The National Credit Act 34 of 2005 provides that a credit provider may not make an offer to enter into a credit agreement where the agreement will automatically come into existence unless the consumer declines the offer.[24] It could perhaps be argued that the posting of a credit card increases the risk of credit card fraud or cloning and that the risk should therefore lie with the issuer as the card has not been issued at the insistence of the cardholder, nor has such cardholder had the opportunity of declining the offer expressly envisaged by the Act.

If a consumer has not been properly informed of a unilateral increase in the credit limit, the question arises whether there can be any mutual understanding between the parties. This might well be the case where written notification is sent via the postal system, and the notice then goes missing, thereby enabling credit card fraud to be perpetrated in the interim up to the new limit. Is it then reasonable to hold a consumer liable? Again the National Credit Act 34 of 2005 expressly provides that a credit provider may not make an offer to increase the credit limit under a credit facility on the basis that the limit will be automatically increased unless the consumer declines the offer.[25] Section 119 further provides that a credit limit may only be increased with the agreement of

[24] S 74(1) In s 74(4) the Act provides that where a credit agreement is entered into as a result of an offer contemplated in s 74(1), the agreement is unlawful and void

[25] S 74(2) In s 74(5) the Act provides that where a provision is entered into as envisaged by s 74(2), such provision is unlawful and void

the consumer or unilaterally, subject to certain conditions, where the consumer has previously requested in writing that the credit limit be increased automatically from time to time.[26] It is important to note that such a specific request may neither be made orally nor be part of the standard provisions that have been assented to by the consumer.[27]

The implications of the Act and contractual provisions concluded by the various parties will now be considered in more detail in a comparison of the position relating to unauthorised transactions based on the original credit card, and the position applicable to unauthorised use involving cloned credit cards.

3 Unauthorised use of the original credit card

The unauthorised use of the original issued credit card could stem from the use thereof at a supplier's pay point, at an automated teller machine (ATM) where cash is withdrawn or perhaps over the internet or telephone when used as a method of payment. Should the risk in such instances lie with the supplier, issuer or cardholder? As far as unauthorised card use pertaining to the original credit card issued is concerned, self-regulation is usually opted for and the individual contract should be consulted. It will usually provide that the cardholder bears the risk for unauthorised transactions until the issuer is informed, whereafter the issuer will bear the loss.[28] These provisions would of course be subject to the provisions of the National Credit Act 34 of 2005, which also makes provision for unauthorised card use.[29]

Schulz states that:[30]

> "The issuers of payment cards and e-money (in South Africa, limited to banks) unilaterally determine the rules and procedures in terms of which cards and e-money are to be used including who bears the risk in the case of loss arising from the use of such products. Suffice it to say that the card or purse holder bears the largest part of the risk of loss resulting from the use of the card or electronic purse."

The provisions of the National Credit Act 34 of 2005 relating to unauthorised transactions are clear. It provides that the credit provider (issuer) may not impose a liability on a consumer (card holder) for the use of credit facilities after the consumer has reported the loss or theft of the associated card, personal identification code (PIN) or number or similar device. Liability may be imposed where the consumer's signature appears on the voucher, sales slip or record or where the credit provider has sufficient evidence to establish that the consumer authorised or was responsible for that particular use of the credit facility.[31] The implementation of the EMV system could be problematic as far as this section is concerned as the use of this system eliminates the need for the use of transaction slips and could consequently have evidentiary implications with regard to proving that the consumer signed for that specific transaction.

---

[26] S 119(a)-(c) and s 119(4)

[27] S 119(5)(a)

[28] Nagel *et al Commercial Law* 414; Schulze 2005 17 *SA Merc LJ* 205; Havenga *et al General Principles of Commercial Law* 371 As far as unauthorised ATM withdrawals are concerned, see *Diner's Club SA (Pty) Ltd v Singh* 2004 3 SA 630 (D) 659A where the issuer placed the risk of wrongful use on its client

[29] See s 94 in this regard

[30] Schulze 2004 16 *SA Merc LJ* 703 715

[31] S 94 of Act 34 of 2005

It might be argued that the provisions of the Act pertaining to credit cards and the unauthorised use thereof are not as extensive as they could perhaps be. In the United States, the Consumer Credit Protection Act[32] provides that no credit card may be issued unless a response or a request has been received.[33] The liability of a holder of a credit card is somewhat more extensive in that a cardholder will not be liable *inter alia* for the unauthorised use of a credit card unless such card is accepted as a credit card; the liability is not in excess of $50; the card issuer gives adequate notice to the cardholder of the potential liability; the card issuer has provided the cardholder with a description of a means by which the card issuer may be notified of loss or theft of the card; the unauthorised use occurs before the card issuer has been notified that an unauthorised use of the credit card has occurred or may occur as the result of loss, theft, or otherwise; and the card issuer has provided a method whereby the user of such card can be identified as the person authorised to use it. The cardholder will also not be liable for the unauthorised use of a credit card in excess of his liability for such use under a specific law or under any agreement with the card issuer.[34] The aforementioned Act also provides for penalties for the fraudulent use of a credit card in the form of a fine not exceeding $10,000 or imprisonment of not more than ten years, or a combination of both.[35]

If the same provisions used in the United States were used, more effective protection to consumers might be afforded in that the risk to consumers might be reduced even further. Examples of possible additional measures that could also perhaps be introduced could entail:

- A credit card with a photo and signature against a hologram background together with smart card technology. An additional safeguard could be that the supplier could demand to see the person's identity document for comparison purposes.
- An express prohibition on the posting of credit cards to potential consumers with pre-approved limits especially where the latter has not applied for a credit card. The posting of such a credit card could facilitate fraud as the card could be intercepted and a duplicate card be fabricated. Once the consumer decides to make use of the posted credit card with its attached terms and conditions, the wheels would have already been set in motion for unauthorised transactions to be concluded with the cloned card at will. This could foreseeably happen with either bipartite cards used by chain stores where smart card technology is not used or in the case of tripartite credit cards where the EMV system has not been implemented.
- An automatically induced text message via e-mail or telecon, which is currently used on an ad-hoc basis by some issuers, could be made compulsory for all issuers, to inform a cardholder that a transaction has been completed, especially if the daily limit is reached. A disadvantage of this measure would

---

[32] Codified to 15 U S C § 1601 of the United States Code, Title 15 (Commerce and Trade), Chapter 41 (Consumer Protection), Subchapter 1, Part A

[33] § 132

[34] § 133

[35] § 134

be that it would entail notification after the fact. However, it could be argued that at least the consumer would be alerted before a number of additional transactions are concluded.

With regard to unauthorised use of the original credit card and alleged unfair contractual terms, it would appear that the position in the cases of *Diners Club SA (Pty) Ltd v Singh*[36] and *Sasfin Ltd v Beukes*[37] would apply. Even if the one party is placed within the economic power of another, which exceeds the reasonable protection of the latter party's interest, such contract can still be enforced. The Court will also take into account various factors such as the interests of individual parties, good faith, the alleged unfairness in the contract and the interests of society.[38]

With regard to the allocation of risk, the Court held in the *Diners Club* case[39] that clauses may be one-sided and favour the issuer so that the risk of wrongful use is placed on the customer.[40] The relevant clause in this case provided that the cardholder would be liable regardless of who made use of the PIN. The Court held further that it would not be contrary to public policy to hold the cardholder bound to the contractual terms and conditions.[41]

It is important to note that the fraud perpetrated in this case did not relate to a duplicate card but to the original issued card and PIN.[42] A distinction must surely be drawn with regard to the allocation of risk between parties on the original credit card as opposed to a fabricated card. The reason is that the terms and conditions linked to the credit card contract would apply to the specific card which the cardholder signed for, and not to the cloned credit card. It is submitted that a different set of principles should as a matter of necessity apply to a separate card. Drawing a distinction is therefore critical especially where there is fabrication of a duplicate card and even more so if a card is skimmed by dishonest insiders, as this could have dire consequences for oblivious or unsuspecting consumers.[43]

As far as payment itself is concerned, there is support for the view that purported payment by a credit card that does not comply with the contractual requirements is void, and does not constitute payment in an analogous way to the use of counterfeit notes.[44] Accordingly, the risk will inevitably lie with the

---

36 2004 3 SA 630 (D)

37 1989 1 SA 1 (A)

38 Schulze 2005 17 *SA Merc LJ* 208 See in general Van der Merwe & Van Huyssteen "The Force of Agreements: Valid, Void, Voidable, Unenforceable" 1995 58 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 549; Lubbe "*Bona Fides*, Billikheid en die Openbare Belang in die Suid-Afrikaanse Kontraktereg" 1990 1 *Stell LR* 7; *Bank of Lisbon & South Africa Ltd v De Ornelas* 1988 3 SA 580 (A)

39 2004 3 SA 630 (D)

40 659A See also Schulze "Unauthorized Cash Withdrawals with a Credit Card, and Unfair Contract Terms" 2005 12:3 *JBL* 143 *et seq* for a full discussion of the *Diners Club* case

41 659D-E See also *Sasfin (Pty) Ltd v Beukes* 1989 1 SA 1 (A) 9 13-14

42 630D-I

43 Note that the case draws no distinction between cloned (duplicate card) and the original issued card and at times seems to blur the distinction between the two See 637A, 638C-D and 641E-F

44 Cornelius 2003 15 *SA Merc LJ* 153 168 The author states (171) that he is of the view that payment by means of credit card constitutes novation whereby the supplier can claim from the credit card issuer Where the contractual requirements for valid payment have not been met, the cardholder will be bound in terms of the underlying contract to the supplier

supplier in such a case, with the cardholder remaining liable in terms of the underlying contract.

4 Unauthorised use involving cloned credit cards

As is the case with the unauthorised use of the credit card originally issued, fraud perpetrated with a cloned credit card could also stem from the use thereof at a supplier's pay point, at an automated teller machine (ATM) where cash is withdrawn, or perhaps over the internet or telephone as a method of payment. Based on the assumption that the cardholder is not fraudulently involved in an unauthorised transaction involving the use of the cloned card, the position relating to the allocation of risk in each of the aforementioned situations might be the following:

- In the case of use at a supplier's pay point, the original cardholder and original card are not involved. The risk necessarily has to lie with the supplier or the issuer in the case of tripartite cards, or with the supplier, who is also issuer, in the case of bipartite credit cards. In such a situation, the mandate of the cardholder has not been complied with, as payment is not in accordance with the instructions of the latter. Purchases made with cloned bipartite credit cards surely cannot be attributed to the original cardholder: there is no contractual relationship between the supplier and original cardholder linked to the use of the cloned card, nor is there an underlying contract of sale which can be relied upon to hold the latter liable.
- In the second instance, where a withdrawal is made at an ATM, the original cardholder would not typically be involved unless such cardholder is involved with the fraudsters. The issuer would possibly only be able to recoup the amount in terms of delictual liability as there is typically no contract on which to rely upon. Again, should any payment be made, it will neither be in accordance with the instructions of the cardholder nor with the terms and conditions of use.
- In the third scenario the cloned card details are furnished to a supplier telephonically or over the internet. The supplier would look to the issuer for payment as there is a contractual relationship between these parties. The relevant transaction slips are usually presented by the supplier to the issuer. Where transaction slips are signed on cloned cards or where perhaps no transaction slips are signed at all in telephonic or internet purchases, the situation becomes more complex in determining which of two innocent parties should bear the loss. The implementation of the EMV system complicates the matter further, especially where the use of transaction slips is eliminated, as this makes it difficult to prove negligence (or the absence thereof), and the National Credit Act 34 of 2005 only provides for the imposition of liability on a consumer where the latter's signature appears on a voucher, sales slip or similar record.[45] In determining whether the supplier or issuer should bear the risk in such cases, the contract could possibly be relied upon, or an

[45] S 94(2)(a)

answer could possibly be sought in the law of delict.[46] In establishing who would bear the risk of loss in these situations, the position with regard to the cloning of cheques will briefly be referred to as a useful comparison in attempting to identify a possible solution to the allocation of the risk.

Cheque fraud, which can also be perpetrated by cloning, has often been the focus of attention.[47] When information is removed from the entire cheque, it is known as cheque washing. Alterations are effected by using chemicals or solvents, which include acetone (nail polish remover), bleach, brake fluid, carbon tetrachloride (carpet cleaner) and special high performance erasers.[48] Cloned cheques are normally produced using advanced colour photocopiers or sophisticated software whilst the original cheque is still available and information may also be fraudulently encoded (cloned) in magnetic ink in the form of a magnetic ink character recognition (MICR) line onto another document purporting to be a cheque. Indicators that a cheque may have been tampered with could be that the MICR is glossy or shiny whereas magnetic ink is normally dull and/or MICR numbers might be missing.[49]

The cloning of a cheque therefore in essence entails that a cheque is intercepted and the original cheque is used to manufacture a duplicate fraudulent cheque. Each cheque is processed through the Automated Clearing Bureau (ACB), which uses electronic data equipment to ensure Magnetic Ink Character Recognition.[50] As far as the allocation of risk on a cloned cheque is concerned, it has been suggested in a prior article that should there be no fault on

---

[46] The principles applicable to an action based on contract and an action founded upon delict should be carefully distinguished A concurrence of contractual and delictual actions has been recognised (see *Media 24 Ltd v Grobler* 2005 6 SA 328 (SCA); *Holtzhausen v ABSA Bank* 2005 2 All SA 560 (SCA)) One should bear in mind, however, that the onus of proof differs in respect of delictual and contractual claims In the case of a breach of contract, the onus would fall on the defendant to show that he was not negligent In a delictual action, the onus rests on the plaintiff to prove that the defendant is negligent See Neethling, Potgieter & Visser *Law of Delict* (2006) 242

[47] Other types of cheque fraud include forged signatures and endorsements, cheque kiting and the washing or altering of cheques Cheque kiting requires multiple bank accounts where the kiter takes advantage of the clearance period required by a bank and money is moved in between accounts See Pretorius & Van der Bijl 2006 18:2 *SA Merc LJ* 196; "Cheque Fraud: Fraud Investigator (SA)" available at http://www fraudinvestigator co za/cheque_fraud htm; "APACS (UK organization)" available at http://www apacs org uk/payments_industry/payment_fraud_2 html ; "Fraud the Facts: APACS article, UK" available at http://www apacs org uk/resources_publications/documents/FraudtheFacts2006; "National Check Fraud Centre" available at http://www ckfraud org/; "Federal Reserve System: Check Fraud Report" available at http://www frbservices org/Retail/pdf/CheckFraud pdf; "Wikipedia: Check Washing" available at http://en wikipedia org/wiki/Check_washing; "Black Market Press: Chemicals Used" available at http://www blackmarketpress net/info/bank/Check_Washing htm (all accessed 10 May 2007)

[48] Pretorius & Van der Bijl 2006 18:2 *SA Merc LJ* 197; *Trans-Atlantic Equipment (Pty) Ltd v Minister of Transport* 2002 2 SA 167 (T) 171C-D; "Cheque Fraud: Fraud Investigator (SA)" available at http://www fraudinvestigator co za/cheque_fraud htm ; "Federal Reserve System: Check Fraud Report" available at http://www frbservices org/Retail/pdf/CheckFraud pdf; "APACS (UK organization)" available at http://www apacs org uk/payments_industry/payment_fraud_2 html; "Fraud the Facts: APACS article" available at http://www apacs org uk/resources_publications/documents/FraudtheFacts2006; "National Check Fraud Centre" available at http://www ckfraud org/ ; "Wikipedia: Check Washing" available at http://en wikipedia org/wiki/Check_washing ; "Black Market Press: Chemicals Used" available at http://www blackmarketpress net/info/bank/Check_Washing htm.

[49] *Ibid*. See further Pretorius & Van der Bijl 2006 18:2 *SA Merc LJ* 196; *R v Abankwah (Jerry)* 2003 EWCA Crim 1875

[50] MICR cheques have a code line, which have precoded characters in magnetic ink such as the serial number of the cheque, the drawer's account number, the drawee bank's branch code and a transaction code See Pretorius & Van der Bijl 2006 18:2 *SA Merc LJ* 200

the part of the drawer, the drawee bank would not be entitled to debit the customer's account with the amount on the forged cheque unless the alteration was apparent. It was argued that in such a case the collecting bank could also possibly incur delictual liability where it failed to notice the alteration or if there was negligence in the collection of the cheque.[51] Furthermore, it was also submitted that where payment is made on a cloned cheque, such payment is made in accordance with the electronic information received through the ACB system and is thus not payment on the original cheque. Furthermore, such payment does not accord with the client's instructions or mandate and the risk of the loss should lie with the bank for not complying with its mandate in terms of the bank-customer relationship.[52]

The bank-customer relationship is usually contractual in nature and classified as a contract of mandate whereby the bank renders services to the customer upon the latter's instructions.[53] The exact terms and conditions of the bank-customer contract are mostly contained in standard contracts.[54] As is the case with cheques, the terms and conditions pertaining to credit cards are also based upon a contractual issuer-cardholder relationship. However, a different set of principles will obviously apply to credit cards, since the provisions of the Bills of Exchange Act 34 of 1964 are not applicable to credit cards, and credit cards are not negotiable instruments. One should also bear in mind that in the case of bipartite credit card agreements, the issuer is usually not a bank and so the bank-client relationship would not be applicable if such party does not qualify as a bank.[55]

An examination of legislation such as the National Credit Act 34 of 2005 appears to confirm that where payment is made on a cloned credit card, it is not done with the authorisation of the card holder/consumer and is not conducted on behalf of, nor at the direction of, the consumer.[56] The question now arises whether the bank could possibly be held liable where it pays on such an unauthorised transaction, as it is not in accordance with the terms and conditions of use and instructions of the client. It can further be asked whether the Apportionment of Damages Act applies to transactions where both the cardholder and the issuer, or supplier and cardholder, are negligent.

Regarding the first question, the issuer is required to make payments on behalf of the correct person, namely the consumer or cardholder in the case of

---

51 Pretorius & Van der Bijl 2006 18:2 *SA Merc LJ* 202

52 See *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* 1986 Ac 80 PC 106B-D The Court states in this case that the "business of banking is the business not of the customer but of the bank They offer a service, which is to honour their customer's cheques when drawn on an account in credit or within an agreed overdraft limit If they pay out on cheques which are not his, they are acting outside their mandate and cannot plead his authority in justification of their debit to his account This is a risk of the service which it is their business to offer " See further Pretorius & Van der Bijl 2006 18:2 *SA Merc LJ* 201-202; Malan & Pretorius *Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law* 4 ed (2002) 356

53 Stassen "Die Regsaard van die Verhouding tussen Bank en Klient" 1980 2 *Modern Business Law* 77 79; *Standard Bank of SA Ltd v Oneanate Investments (Pty) Ltd* 1995 4 SA 510 (C) 530; Malan & Pretorius *Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law* par 203

54 Cranston *Principles of Banking Law* (2002) 144

55 Schulze 2004 16 *SA Merc LJ* 703 713

56 A consumer includes the party to whom credit is granted under a credit facility See s 1 of Act 34 of 2005 in this regard

the contractual relationships pertaining to a credit card. The orders of the client would be carried out in the form of transaction slips, which would need to be signed by the consumer on the completion of a transaction.[57] Where the issuer has performed its obligations in accordance with the terms and conditions of use, the latter will be entitled to reimbursements for payments rendered on the cardholder's behalf.[58]

Where a credit card is cloned, it would entail that payment is made on a separate substitute credit card, which purports to be the original credit card. In such a case, it is clear that the terms and conditions of use are not complied with, as it is not payment in accordance with the client's instructions. The signature on the transaction slips relating to the cloned card would also probably contain an unauthorised signature which again is not at the instruction of the client. It is therefore apparent that payment made on the cloned credit card is not payment made on the original credit card in accordance with the terms and conditions of use. It is submitted that in such a case the issuer has not performed in terms of its mandate and should bear the risk, as the performance rendered is not made in terms of the original card issued to the client. The case of *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd*[59] serves as authority for the fact that where payment is made on cloned cheques, the risk will lie with the party acting outside its mandate, which findings could also perhaps find similar application where payment is made on cloned credit cards.

In attempting to answer the second question, bearing on the possibility of instituting delictual action based on the unauthorised use of the cloned card, it is conceivable that there would not necessarily be a contract (unless the consumer had entered into a contract based on the original card and was somehow involved in the fabrication of a duplicate card) or terms and conditions relating to the cloned card. One would accordingly need to establish whether the cardholder or the issuer was negligent. If both are possibly negligent, it may be necessary to consider whether the Apportionment of Damages Act 34 of 1956 applies. Before exploring the provisions of this Act, one should bear in mind that it is important to carefully distinguish between the principles applicable to an action based on contract and an action founded upon delict, as different considerations apply. A delict consists of a number of elements including wrongfulness, fault and causation, which should be clearly distinguished.[60]

The Apportionment of Damages Act 34 of 1956 regulates the issue of contributory fault and can be applied where not only the defendant was at fault but

---

[57] Nagel *et al Commercial Law* 414

[58] Malan & Pretorius *Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law* pars 203 206 With regard to cheques specifically, it was said in *Volkskas Bpk v Johnson* 1979 4 SA 775 (C) 777-778 that the bank is obliged to pay according to its tenor and only once this is done will the bank be entitled to debit its client's account with the amount See also *Eskom v First National Bank of Southern Africa Ltd* 1995 2 SA 386 (A) See further *Selangor United Rubber Estates Ltd v Cradock* 1968 2 All ER 1037 1118 where it is stated that a bank has a duty to exercise reasonable care and skill in terms of the bank-client contract which standard is an objective one

[59] 1986 AC 80 PC 106B-D See further Pretorius & Van der Bijl 2006 18:2 *SA Merc LJ* 202

[60] *SM Goldstein & Co (Pty) Ltd v Cathkin Park Hotel (Pty) Ltd* 2000 4 SA 1019 (SCA) 1024E-G; Neethling, Potgieter & Visser *Law of Delict* (2006) 186-187

where the plaintiff was also contributory negligent.[61] The Apportionment of Damages Act provides that:

> "(1)(1) (a) Where any person suffers damage which is caused partly by his own fault and partly by the fault of any other person, a claim in respect of that damage shall not be defeated by reason of the fault of the claimant but the damages recoverable in respect thereof shall be reduced by the court to such extent as the court may deem just and equitable having regard to the degree in which the claimant was at fault in relation to the damage.
>
> (b) Damage shall for the purpose of paragraph (a) be regarded as having been caused by a person's fault notwithstanding the fact that another person had an opportunity of avoiding the consequences thereof and negligently failed to do so.
>
> (1)(3) For the purposes of this section 'fault' includes any act or omission which would, but for the provisions of this section, have given rise to the defence of contributory negligence."

The Act will apply in instances of delictual liability where a person has been negligent in not exercising the reasonable standard of care applied in such a case. Negligence is present where a *diligens paterfamilias* would foresee the reasonable possibility of his conduct injuring another in his person or property, thus causing patrimonial loss, and would take reasonable steps to guard against such occurrence, but failed to take such steps.[62]

The test for negligence is therefore based on reasonable foreseeability and reasonable preventability of damage.[63] It could be argued that where a credit card is used, loss due to credit card fraud is reasonably foreseeable, and that reasonable steps need to be taken to prevent such loss.[64] As to what constitutes reasonable steps, one would necessarily need to take into account the cost of preventative measures. It could perhaps be seen as not reasonable where EMV smart card technology is not implemented in both the case of tripartite and bipartite credit cards. It has been shown that utilising a card reader machine that reads cards with both smart chips and magnetic stripes is not necessarily a preventative measure against fraud. Would it be more reasonable to have different card reader machines for the different types of cards despite economic implications? What happens when purchases are made over the internet or telephone? If reasonable steps are not taken it could be argued that the ordinary principles of delictual liability could apply. Where both parties such as the supplier and issuer, or issuer and cardholder are negligent in some form, then the Apportionment of Damages Act 34 of 1956 could also possibly find application.

It is problematic, however, that section 1 of the Apportionment of Damages Act 34 of 1956 is applicable to delictual claims but not to contractual claims. It would therefore appear not to be applicable to actions based on the unauthor-

---

[61] S 1

[62] *Kruger v Coetzee* 1966 2 SA 428 (A) 430E-F; Neethling *et al Law of Delict* 126-133; *Mkhatswa v Minister of Defence* 2000 1 SA 1004 (SCA) 1111-1114; *Sea Harvest Corporation (Pty) Ltd v Duncan Dock Cold Storage (Pty) Ltd* 2000 1 SA 827 (SCA); *Mukheiber v Raath* 1999 3 SA 1065 (SCA); Voet 9 4 2; Kelly "The Apportionment of Damages between a Negligent Collecting Bank and a Thief of Cheques: Does the Apportionment of Damages Act Apply?" 2001 13 *SA Merc LJ* 509 510

[63] Neethling *et al Law of Delict* 126-133; *Kruger v Coetzee* 1966 2 SA 428 (A) 430E-F; *Mkhatswa v Minister of Defence* 2000 1 SA 1004 (SCA) 1111-1114; *Sea Harvest Corporation (Pty) Ltd v Duncan Dock Cold Storage (Pty) Ltd* 2000 1 SA 827 (SCA); *Mukheiber v Raath* 1999 3 SA 1065 (SCA); Voet 9 4 2

[64] *Diners Club SA (Pty) Ltd v Singh* 2004 3 SA 630 (D) 637A

ised use of a credit card founded on credit card contracts.[65] In *Thoroughbred Breeders' Association v Price Waterhouse,* Nienaber JA, Marais JA, Farlam JA and Brand AJA confirmed that the principle of contributory negligence is designed to address specific needs identified in the law of delict and not in the law of contract.[66] In order to hold the issuer delictually liable on the basis of fault, one would therefore need to prove all the requirements of delictual liability. It could perhaps be argued that a standard of reasonableness is to be expected from an issuer. Kelly[67] says in this regard that

> "the standard of care should be measured by the general level of skill and diligence possessed and exercised at the relevant time of the conduct. A court may acknowledge the standard of care generally adopted by other members of the profession, but conformity with general practice is merely prima facie evidence of the absence of negligence."

Although Kelly is as a matter of course referring to the negligence of a collecting bank, it could surely be argued that a standard of care could perhaps also be introduced to issuers, especially as some issuers adopt additional security measures to attempt to combat fraud, whereas others do not attempt to introduce the same measures as a safeguard against fraud. It could arguably be said that these latter issuers do not comply with general practice and could perhaps be held liable in terms of the law of delict if all the requirements are met.

Fault could be proved if it could be shown that the issuer paid out negligently on the cloned credit card. Some examples of instances where negligence could perhaps be inferred and proved are where the signature on the transaction slip used for the purchases made on the cloned credit card does not match the signature of the client; where it is proved that the personal details of the client were not safeguarded sufficiently so that a fraudster could have gained access to the personal details of the client, thus enabling him to fabricate a substitute card; where credit cards are mailed with an invitation to a prospective cardholder to make use of the opportunity and such cards are intercepted; or where the use of EMV was possible and the issuer was not EMV compliant. The issuer would have to prove that it took reasonable steps to ensure that payment was made on behalf of the correct person, namely the cardholder.

Some examples of where the cardholder could be negligent might be where he leaves his card lying around so that a fraudster gains easy access to the card to manufacture a cloned card; where transactions are made under circumstances in which payment is not secured, as might be the case with internet purchases where access to all the personal details of the client is possible; or where the details are provided telephonically. This might especially be seen to be the case where the issuer provides security measures which the cardholder does not utilise. An example of this could be where digital codes are sent electronically in addition to the furnishing of passwords. Negligence may also be specifically inferred where the use of an EMV card, with a special chip as a

---

[65] See *OK Bazaars (1929) Ltd v Stern and Ekermans* 1976 2 SA 521 (C) 530

[66] 2001 4 SA 551 (SCA) 591A-D 597E-F 604G-H

[67] 2001 13 *SA Merc LJ* 509 510

special security feature, is not utilised despite the opportunity being presented to the client to make use of such system.

A few instances involving the supplier where negligence could possibly be inferred are where the supplier is also issuer and randomly mails credit cards to prospective customers, as is often the case with bipartite credit cards; where goods are supplied without properly verifying the identity of the customer in instances where the system is offline; where goods for large amounts are provided; and where accounts are opened or transactions are concluded. In instances where bipartite credit card transactions are concluded it would be even more difficult to avoid being found negligent as the issuer/supplier would also inevitably have a sample signature of its cardholder. Such signature could easily be scanned into the computer system together with a photo and signature of the client and verified against the card signature used to complete the transaction. A card with a photo of the client together with a signature and hologram could rule out possible identity fraud and could also act as a safeguard measure where a smart card system is not used and the risk of fraud is perhaps greater.

5 Conclusion

It has been shown that despite innovations in technology, the risk of unauthorised use of credit cards and the cloning of cards will persist in some form or another for a number of reasons:

- It is foreseeable that it will take time to implement smart cards during the migration process from the mag-stripe process to smart card technology. It has been shown that fraud can still be perpetrated where a card reader accepts both types of technology. Furthermore, some institutions and suppliers may still prefer more traditional methods of payment for economic reasons. It is envisaged that problems may still arise where systems are offline and transactions are nevertheless concluded with the use of a specific card.
- The use of cards telephonically or internet shopping where cards are not presented, also present problems where traditional cards need to be used or details provided electronically and verification of the chip is not possible. Precautionary measures that could be undertaken to avoid cloning of credit cards or reduce the risks inherent in credit card use could include the use of holograms together with a photo and signature of the client, especially in the case of bipartite credit cards where holograms are not often encountered as this provide a practical solution in which a supplier can more readily ascertain whether a specific card is valid or not.[68]
- Instead of having a single swipe design one could have terminals with separate mag-stripe and chip readers, which would admittedly be more expensive and would have an impact on whether it is a reasonable measure to safeguard against fraud.[69]

---

[68] "French Card Hacker Convicted" available at http:// www theregister co uk/2000/02/26/french_card_ hacker_convicted accessed 10 May 2007 See also Schulze 2004 16 *SA Merc LJ* 703 705 which discusses the embossing of cards

[69] "Card Technology" *Newsroom Global Newswatch* vol 11 06/01/06 Card Tech 8 2006 WLNR 9391895

- It is perhaps foreseeable that PINS will become more vulnerable with increased use as envisaged with the smart card system. Increased usage of PINS could foreseeably increase the possibility of fraud.[70] In such cases it would perhaps be better to have only a chip and PIN or improved software.[71]
- As a reasonable measure to safeguard all parties concerned, insurance could be made a compulsory clause in the credit card contract to safeguard to limit the risks inherent with credit card use.
- More stringent legislative measures could be adopted. Measures analogous to those adopted in the United States could perhaps be added to the National Credit Act 34 of 2005 to provide for penalties such as fines or imprisonment or provisions, which limit the cardholder's liability in instances where there is unauthorised use of the original credit card. In doing so, it is foreseeable that issuers might take additional safeguards to limit their portion of the risk. The Act would not appear to apply to cloned credit cards but merely to contracts concluded on the original card issued.

It would be useful if specific provisions regulating the use of cloned credit cards are also developed to facilitate legal certainty. It is at least certain that, despite welcome technological advances, it is unrealistic to expect a foolproof solution to fraud. In the meantime, issuers had best be prepared for continued parenting problems with their cloned offspring.

OPSOMMING

Die EMV (Europay, Mastercard en Visa) stelsel is onlangs deur ABSA geïmplementeer. Die stelsel maak gebruik van 'n sogenaamde *smart card* skyfiekaart wat daarop gemik is om die ongemagtigde gebruik van kredietkaarte uit te skakel. Kaarte bevat spesiale skyfies met PIN-nommers wat die kaarthouer identifiseer. Alhoewel hierdie stelsel 'n besondere vordering in tegnologie is, kom bedrog ongelukkig nog steeds voor. Verslae van bedrog in Brittanje en Frankryk is al gerapporteer. Onderskeie probleme kan moontlik ondervind word waar die stelsel nog nie volledig geïmplementeer word nie, soos in die geval waar kaartleesmasjiene beide magnetiese kaarte en *smart*-kaarte aanvaar; waar *smart*-kaarte nie gebruik word nie, soos byvoorbeeld in die geval van tweeledige kredietkaarte; en waar internet- en telefoniese aankope gemaak word. 'n Belangrike vraag wat beantwoord moet word is op wie die risiko rus – op die kaarthouer of op die uitreiker? Om hierdie vraag te beantwoord, word 'n onderskeid getref tussen die posisie waar daar ongemagtigde gebruik van die oorspronklike kredietkaart is, en die posisie waar 'n afsonderlike gekloonde kaart gebruik word. Daar word dan na die beginsels van kontraktereg en deliktereg gekyk om 'n moontlike oplossing te vind.

---

[70] See in this regard *Diners Club SA (Pty) Ltd v Singh* 2004 3 SA 630 (D) 637A-D; "Algorithmic Research Reveals PIN Processing Weakness that Allow Payment-Card Fraud" available at http:// www smartcard-strends com/det_atc php?idu (accessed 8 May 2007)

[71] Card Technology" *Newsroom Global Newswatch* vol 11 06/01/06 Card Tech 8 2006 WLNR 9391895