LOST, STOLEN OR SKIMMED

Overcoming credit card fraud in South Africa

Trevor Budhram*

budhrt@unisa.ac.za

A credit card is a convenient method of payment, but it does carry risks. The enormous growth in the use of credit cards has resulted in high levels of credit card fraud. Technological advances have allowed the perpetrators to produce counterfeit cards that resemble the genuine card so closely that it is difficult for shopkeepers, tellers, police and bank investigators to identify a fraudulent card. Identity theft and the exponential growth of the internet have further compounded the crime of credit card fraud by allowing for on-line purchasing, resulting in huge financial losses to the card industry and consumers alike. This article discusses credit card fraud in South Africa and offers information about the measures taken to reduce it.

The use of credit cards has become a way of life in many parts of the world. Today, credit cards are used like cash. All credit cards have one thing in common, namely that the bearer can obtain something of value simply by presenting the card. However, credit card fraud results in high losses both for the banking industry and consumers, and seems to be increasing. According to the South African Banking Risk Intelligence Centre (SABRIC), financial losses resulting from credit card fraud increased by 53% between 2010 and 2011.[1] Total losses to the sector amounted to R403,15 million, an increase from 2010 of R263,8 million.[2] The high rate of card fraud perpetrated should thus be a major concern for establishments accepting credit cards, the banking industry, and especially for individual users.

* Trevor Budhram is a senior lecturer in the Department of Police Practice, University of South Africa. This article is based on a review of the national and international literature on credit card fraud and the security features found on cards, undertaken for the author's master's dissertation titled 'Examining the Unique Security Features of a Credit Card with the Aim of Identifying Possible Fraudulent Use', 2007.

AN OVERVIEW

Credit card fraud takes many forms, from 'thieves using stolen credit cards to buy goods, to the greater, more sophisticated problem of criminals altering security features'.[3] According to Snyman, fraud is defined as the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another.[4] Despite a host of hi-tech anti-fraud measures, the battle against fraud continues as criminals continue to 'poke and prod at the card industry's weak spots'.[5] In the early days of the card industry, card fraud was a crime of opportunity, originating from a sales slip found in a dustbin or a card found in a lost or stolen wallet. An example from case law can be found in *S v Salcedo* (2003)[6] where the accused committed credit card fraud by picking up a credit card that had fallen out of the account holder's pocket in a mall and going on a spending spree the same day. The accused was convicted on nine counts of fraud and sentenced to six months imprisonment on each count.[7] Since then the crime of credit card fraud has evolved into a highly organised business that reaches around the world.

When a person receives a credit card from the bank s/he enters into a legal relationship with the bank. Van der Bijl states that 'the legal relationship between the parties to the credit card agreement is regulated by the contract itself, the general principles of contract law and the National Credit Act 34 of 2005'.[8] The Act provides that the cardholder bears all the risks for unauthorised transactions until the issuer is informed, whereafter the issuer will bear the loss. With regards to the 'unauthorised use of the original credit card and alleged unfair contractual terms'[9] in a leading case of *Diners Club SA (Pty) Ltd v Singh and another*,[10] the account holder was found guilty for authorising certain transactions that occurred with his card in London. The case discussed 'numerous issues surrounding the encryption of the pin and the possibility of the card being cloned'. The court ruled that an original card and pin were used to perpetrate the fraud and not a duplicate card. The court was however critical of the risk specific to the contract, in that it was one-sided and favoured the issuer, so that the risk of wrongful use is placed on the customer.[11]

Different types of credit card fraud exist, ranging from counterfeit card fraud to lost and stolen card fraud. 'Lost and stolen card fraud is opportunistic and can be controlled by precautionary measures being adopted by cardholders, whilst counterfeit card fraud involves a number of technological fraud types such as cloned cards, altering of information on the magnetic stripe and the re-embossing of details onto cards.'[12] Credit card fraud does not exist in a vacuum. Often credit card fraud is 'linked with other crimes, such as burglary, mail theft and organised crime'.[13]

TYPES OF CREDIT CARD FRAUD

Fraud with stolen and lost credit cards

Fraud with stolen and lost credit cards is the most common type of credit card fraud and involves the 'theft of genuine card details that are used to make a purchase through a remote channel such as the phone, fax, mail order or the Internet',[14] and/or by presenting the card at a till point. Combined, these two categories constituted the highest percentage card fraud incidents in South Africa in 2007/2008 (68%). It further constituted the highest card fraud losses in South Africa on RSA issued cards year on year between 2005 and 2008 (57,1m in 2005/2006, R122,9m in 2006/2007, R150m in 2007/2008 and R33,1m in 2008/2009).[15]

However, according to SABRIC, the use of this fraud type decreased by 60% in 2010.[16] This was attributed to the roll out of the chip-and-pin card, which requires a person to enter a pin code when transacting with the card. The South African Police Service (SAPS) Annual Report[17] for the period 2010/2011 shows that a total of 339 cases were recorded in this category with an actual loss of R22 599 546 (a substantial decrease since 2007/8). As with counterfeit card fraud, the legitimate card holder may not be aware of this fraud until they check their bank statements. To counter this, banks, for example First National Bank, have started to send out sms alerts to account holders' mobile phones and e-mail addresses whenever a transaction is made.

Counterfeit card fraud

Counterfeit card fraud involves a card that has been illegally manufactured from information stolen from a magnetic strip of a genuinely issued card.[18] In other cases, lost and stolen cards and old cards are encoded with information stolen from a genuine card for the purposes of committing counterfeit card fraud. The information needed for counterfeit card fraud is usually stolen through 'skimming' a genuine card. Van der Bijl states that 'skimming entails that the magnetic strip on the back of the card is copied using a hand held card reader'.[19] Skimming can also be perpetrated by concealing a 'skimming device in the card slot of an ATM which results in the recording of data of all cards accessing the specific ATM as well as recording the secret pin code of the card'.[20] According to the SAPS training manual on credit card fraud, 'skimming normally occurs at retail outlets, particularly at

bars, restaurants and petrol stations where a corrupt employee skims a customer's card before handing it back'.[21]

The year on year percentage growth of counterfeit card fraud has remained fairly constant since 2005/2006 (at an average annual growth rate of between 15% and 21%).[22] This is an indication that counter measures, such as card awareness campaigns, merchant training and joint operations between SAPS and the card industry have not been successful. In addition the problem points to the security weakness of magnetic stripe, as the data they store can be copied. According to SABRIC, losses through this type of fraud for the year October 2009 to September 2010 amounted to R141,4 million[23] and statistics for the period September 2010 to October 2011 show losses amounting to a staggering R176 million and 'accounts for 57,2% of overall losses to the banking sector'.[24] The SAPS Annual Report 2010/2011 records a total of 4 059 cases received for this category of fraud, for which 308 suspects were arrested, resulting in an actual loss of R118 053 534.[25] The discrepancy between the SAPS and SABRIC figures in the opinion of the author may be a consequence of the fact, that only cases in which suspects are identified (308 in this case) are reported to the SAPS. In addition, cardholders who are victims report their cases to the banks and hold the bank accountable for the fraud. The banks reimburse the clients and do not pursue the case nor report it to the SAPS.

Card not present fraud

Card not present fraud 'denotes a fraudulent transaction that occurs when the card, the card holder or the merchant representative is not present at the time of the transaction which is made online or via the telephone'.[26] This means that:

- The merchants are unable to check the physical security features of the card to determine if it's genuine
- Without a signature or a pin it is not easy to confirm that the customer is the genuine card holder
- Card issuers cannot guarantee that the information provided in a card not present environment relates to the genuine card holder.

This fraud type has increased at the rate of approximately 50% year on year since 2005/6; from R6,5m in 2005/06, to R12,8m in 2006/07, to R21,3m in 2007/08, to R30,9m in 2008/09 and amounting to R80,9m in 2009/2010.[27] According to SABRIC this fraud type 'increased by 77% in 2011 and is the second most prevalent form of [credit card] fraud'.[28] Losses amounted to R142,8 million in 2011.[29] The ease and frequency with which on-line and telephonic purchases can be made contribute to the increase in the prevalence of this form of fraud. Internet and telephonic transactions provide anonymity, making it possible for the fraud to be perpetrated without fear of arrest. Online purchases may be done at internet cafes, and telephonic purchases at public phone booths, making it difficult to trace perpetrators.

The year-on-year growth in the extent of financial losses suffered by the banking industry indicates that no counter measures have been effective in reducing this kind of card fraud.

MEASURES TO SECURE CREDIT CARDS

Over the past 25 years there has been a constant race between the credit card industry developing new security features to deter counterfeiting, and criminals working hard to compromise the technology and manufacture counterfeit cards. The discussion that follows shows two types of VISA credit cards, indicating the different security features and where they are located. The security features endorsed on the cards have been in effect worldwide since May 2006.

The Visa Mini Dove Hologram and Visa Dove Hologram are among the most prominent features on the front of a credit card. Rapp explains that 'holograms are small metallic oblongs, containing a laser-etched image on their surface'.[32] The image changes shape and colour depending on the

Figure 1

Security features – Visa mini dove design hologram on back of card

The **signature panel** has an updated tamper evident design, as shown here, or has a custom design. It may vary in length dependent on card type. If someone has tried to erase the signature panel, the word 'VOID' will be displayed.

The **mini dove design hologram** may appear on the back to the right or left of the signature panel, or below it. A three-dimensional dove hologram should reflect light and seem to change as you tilt the card. Most counterfeit cards contain a one-dimensional printed image on a foil sticker.

A Four-digit number must be printed directly below the account number. This four-digit number must match exactly with the four digits of the account number. Both must begin with a '4'.

'Good thru' (or 'valid thru') date is the expiration date of the card. It is located below the embossed account number. If the current transaction date is after the 'good thru' date, the card has expired.

Ultraviolet 'V' is visible over the Visa brand mark when placed under an ultraviolet light.

The **magnetic stripe** is encoded with the card's account number, expiration date, and other identifying information. It should be smooth and straight, with no signs of tampering.

The **Card Verification Value (CVV2)** is a three-digit code that appears either on the signature panel or on a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-not-present transactions to verify that the customer is in possession of a valid Visa card at the time of the sale.

Embossed or printed account number on valid cards begins with '4'. The account number must be even and straight; on altered cards, they may have fuzzy edges, or you may be able to see 'ghost images' of the original numbers.

Visa brand mark appears in blue and gold on a white background. It must appear in either the bottom right, top left or top right corner.

Source: *Visa Logo Card Security Features 2007*

viewing angle, and is very difficult to forge. The Visa mini dove hologram appears on the back of the card (see Figure 1) whilst the Visa dove hologram appears on the front of the card (see Figure 2). The design is three dimensional. The last four digits of the embossed account number are incorporated in the hologram.[33]

Very few counterfeit holograms have actually been used.[34] In most cases of counterfeit cards, the hologram is not a hologram but a look-a-like item that is reflective rather than refractive. Holograms are refractive, that is, the item in the hologram appears to actually move, whereas a reflective item is only a photo on a reflective material. Forged holograms have included printed images, using a variety of materials and inks. Some have used plain foils and/or diffraction grating foils.[35] Fraudulent holograms comprise flat images of a dove which includes no movement or colour change. This is one way in which vendors can determine whether a card presented for payment is a genuine card or one that has been forged.

Of equal prominence is the embossed or printed account number. 'Embossing is the oldest security or identification technique for marking payment or ID cards in machine readable form.'[36] The account number must appear clear, clean, and uniform in size and spacing. The four digit number printed below the embossed account number must match the first four digits of the account number. (See Figure 1).

A feature that cannot be viewed with the naked eye is the ultra violet feature. This is found on the Visa logo and on the signature panel. (See Figures 1 and 2.) Criminals do not interfere with this security feature because they are unaware of its existence.[37] Rapp states that 'some cheques and credit cards have images or symbols printed in ultraviolet ink'.[38] These are invisible to the naked eye in normal light, but show up very clearly under ultraviolet light. The Ultra Violet V, found in the VISA brand mark, is such an example. The Ultra Violet V is 'visible over the Visa Brand Mark when placed under an ultra violet light'.[39]

Another highly visible feature is the pre-printed bin situated below the first four digits of the embossed account number, which shows the issuing bank's identification number.[40] In Figure 1 it is referred to as 'Four-Digit number' and in Figure 2 'printed first 4 digits of account number'. This is a four digit printed number that matches the first four digits of the embossed account number. If the two numbers do not match, the card has been altered or is a counterfeit.

Affixed to the back of the card is a stripe of magnetic tape, which contains essential cardholder and account information. The magnetic stripe can store about 130 characters or numbers.[42] It allows a transaction to be processed when it is read at an electronic point of sale at a merchant by 'swiping it across a reading head, either manually or automatically'.[43] The information includes the account number and expiry date, which must correspond with those embossed on the face of the card.[44] Although it is technically possible to remove a magnetic stripe from a card and replace it with another, or re-record over it, in practice it is uneconomical.

Below the magnetic stripe is the signature panel, which contains an ultra violet element that repeats the word VISA.[45]

Chemical eradicators have allowed some card criminals to remove the legitimate signature from a stolen or lost card and substitute their own. This made it necessary 'to over print a signature strip with a light coloured pattern using a special ink that would change colour when it came in contact with ink eradicator'.[46] The ink will also rub off if any attempts are made to remove the signature with a rubber eraser. If an attempt is made to erase the signature panel the word 'VOID' will be displayed. The three digit Card Verification Value 2 (CVV2) are reverse-italic, indented printed numbers which must appear in a white box to the right of the signature panel or on the signature panel. Part of this number is an 'algorithmically calculation which the issuer can verify as genuine'.[47] The value can be checked when a merchant is required to refer to the issuer of an account for authorisation of a transaction where an electronic approval is not available or permissible.[48] See Figure 1.

Figure 2

Source: *Visa Merchant Quick Guide 2006*[41]

The high rate of credit card fraud has prompted the various card associations to develop new technology in an attempt to try and curb the counterfeiting of credit cards. Magnetic stripe technology has proven to be vulnerable and now, after 'more than 30 years of providing security the magnetic stripe is to be replaced with new technology, namely the microchip'.[49] Cards now have an embedded integrated circuit or microchip, which is found on the left side of the card above the embossed or printed account number (see figure 2). The card has electronic logic to store data, and in some cases, a microprocessor that can process data. Also known as a 'smart card' or 'relationship card', it can be 'contact' (activated when terminals touch a smart card reader) or 'contactless' (activated by radio waves when passed near a transmitter). The type of chip cards currently used range from fairly simple memory devices to sophisticated microprocessors. The latest generation of chip cards contain a microprocessor, a liquid crystal display and a power source, which enable the card to be used independently of a card reader.[50]

PREVENTATIVE COUNTER-MEASURES

The vulnerability of the magnetic strip to skimming has resulted in banks replacing this technology with chip-and-pin technology. The chip-and-pin technology has so far proved successful in countries such as the United Kingdom, where total counterfeit card fraud decreased by 32% in the past two years.[51] In South Africa not all cards will have the chip-and-pin feature because not all merchants have the systems installed to support chip-and-pin cards. This means that magnetic stripe technology will remain in use for some years to come.

Banks in South Africa have, however, deployed sophisticated IT programmes that help to detect, prevent and reduce bank card fraud. Examples include SMS confirmation of transactions, the implementation of authorisation parameters and thresholds, and forensic investigations. These measures are, however, reactive and banks should consider an intelligence-led approach to combating card fraud. However, in order for this approach to be successful it requires co-operation between SAPS and the banks. This approach requires a combined use of crime analysis and criminal intelligence in order to determine crime reduction tactics.

The launch of the on-line verification system, a joint initiative between the Department of Home Affairs and SABRIC, on 8 November 2011 allows banks access to the Home Affairs National Identification System to verify the identity of prospective and current clients, using their fingerprints. This tool provides an added benefit to the bank client in that it offers the banks 'a second layer of confirmation that the persons presenting identity documents are indeed who they purport to be'.[52]

CONCLUSION

Credit card fraud has been committed since credit cards were first introduced; however, modern technology has increased the ways in which it can be committed. Criminals see the card industry as a lucrative business that can be exploited by the use of technology. To counter the problem, credit card companies constantly review security features and measures that are applied to cards and devote considerable resources to the maintenance of security systems and programming.

There are numerous challenges to dealing with credit card fraud, particularly since transactions do not require the physical presence of seller and purchaser. The establishment of a dedicated joint working group consisting of members from the Commercial Crimes branch in the SAPS, the Asset Forfeiture Unit, and banks, in addressing card fraud, may provide the tonic in addressing card fraud in that it brings about the joining of divergent skills, expertise and resources. The low conviction rates for counterfeit card fraud for the period 2010/2011 indicate the difficulties the police face in investigating crimes of this nature. In 2010/11, 11 276 cases of credit card fraud (counterfeit, stolen and fraud with other cards) were reported to the police for investigation. A total of 229 cases went through the court process

and a total of 223 accused persons were convicted.[53] It is therefore important that a new approach, for example an intelligence led approach, be considered in combating card fraud.

To comment on this article visit
http://www.issafrica.org/sacq.php

NOTES

1. Credit card fraudsters hit it big, IT Web, available at http://www.itweb.co.za/index.php?option=com_content (accessed 23 March 2012).
2. Ibid.
3. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2002, 8.
4. Carel Rainier Snyman, Criminal Law, (Third Edition), Durban: Butterworths, 1995, 487.
5. Snyman, Criminal Law, 8.
6. S v SALCEDO 2003 (1) SACR 324 (SCA).
7. S v SALCEDO 2003, 31.
8. Charnelle van der Bijl, The cloning of credit cards: The dolly of the electronic era, *Stellenbosch Law Review*, 18, 2 (2007), 338.
9. Van der Bijl, The Cloning of Credit Cards, 334.
10. Diners Club SA (Pty) Ltd v Singh and another 2004 (3) SA 630 (D).
11. Van der Bijl, The cloning of credit cards, 338
12. Van der Bijl, The cloning of credit cards, 30-31.
13. Burt Rapp, *Credit card fraud,* Port Townsend, Washington: Loompanics Unlimited, 1991, 23.
14. Rapp, Credit Card Fraud, 31.
15. SABRIC: Credit Card Fraud South Africa, 2008, 34.
16. Credit card fraud drops, *South Africa: The Good News,* http://www.sagoodnews.co.za/private_sector_business/credit_card_fraud_drops_html (accessed 24 August 2011).
17. *South African Police Service, Annual Report,* 2010/2011, 97.
18. SAPS *Annual Report*, 32.
19. Van der Bijl, The cloning of credit cards, 331.
20. Credit card fraud, www.interac.ca/consumers/security_fraud.php (accessed 24 August 2011).
21. South African Police Service Advanced Training Manual, Commercial Crime, 2002, 126.
22. SABRIC: Credit Card Fraud South Africa, 2008, 32.
23. Credit card fraudsters hit it big, IT Web, available at http://www.itweb.co.za/index.php?option=com_content (accessed 23 March 2012), 1.
24. Ibid.
25. SAPS *Annual Report*, 2010/11, 97.
26. SABRIC: Credit Card Fraud South Africa, 2008, 30.
27. SABRIC: Credit Card Fraud South Africa, 2008, 30. Credit card fraudsters hit it big, IT Web, available at http://www.itweb.co.za/index.php?option=com_content (accessed 23 March 2012).
28. SAPS Advanced Training Manual, 1.
29. Credit card fraudsters hit it big, IT Web, available at http://www.itweb.co.za/index.php?option=com_content (accessed 23 March 2012), 1.
30. Trevor Budhram, Examining the unique security features of a credit card with the aim of identifying possible fraudulent use, dissertation submitted for Masters degree, University of South Africa, 2007, 53.
31. Merchant quick reference guide. Visa card security features, May 2006. CEMEA Region.
32. Burt Rapp, Credit card fraud, 23.
33. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2000, 29.
34. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2000, 30.
35. Ibid.
36. Wilhelm Georg Schulze, Smart cards and e-money: new developments bring new problems, *Mercantile Law* (2004), 704.
37. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2000, 32.
38. Burt Rapp, Credit card fraud, 25.
39. Merchant quick reference guide. Visa card security features, May 2006. CEMEA Region.
40. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2000, 32.
41. Merchant quick reference guide. Visa card security features, May 2006. CEMEA Region.
42. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2000, 33.
43. Wilhelm George Schulze, E-money and electronic fund transfers: A short-list of some unresolved issues, *Mercantile Law* (2004), 16..
44. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2000, 33.
45. Trevor Budhram, Examining the unique features of a credit card with the aim of identifying possible fraudulent use, 59.
46. Burt Rapp, Credit card fraud, 22.
47. Visa International Law Enforcement Education Programme, Credit Cards, CEMEA Region, 2000, 36.
48. Ibid.
49. Wilhelm Georg Schulze, Smart cards and e-money, 705.
50. Wilhelm Georg Schulze, E Money and Electronic Fund Transfers, A Shortlist of Some of the Unresolved Issues, HEINONLINE: Mercantile Law. Journal, (2004), 16.
51. Wilhelm Georg Schulze, E-money and electronic fund transfers, 16.