Recommendations for Mitigating Information Disclosure from Point Of Sale Devices in South Africa

S von Solms
University of Johannesburg
Faculty of Engineering and the Built Environment
svonsolms@uj.ac.za
+2711 559 2462

The advantages of flexibility and convenience offered by Point of Sale terminals or online banking sites have urged more and more South African consumers to opt for cashless payments. Although financial services corporations have very strict regulations relating to cashless purchases and take great lengths to reduce credit card fraud, legitimate Point of Sale transaction receipts may offer an easy method for fraudulent online transactions.

Introduction

First National Bank, one of South Africa's largest retail banks reported in November 2013 that non-cash payments surpassed cash withdrawals by approximately R800 million. The bank further stated that card-based spending is increasing at 38% per annum whilst they predict that cash usage will further decline in the future.[1] Many South African banks offer free card swipes, free notification alerts and reward programmes to encourage cashless purchases. Two of the most used methods of cashless purchases are through Transfer Point of Sale (POS) terminals and online shopping sites.

POS terminals are no longer limited to large retailers, as a wide range of cost-effective POS options are now available to small and medium sized businesses. This has not only enabled small business owners to process cashless payments, but to enable cashless payments outside of the permanent business premises, like a flea market or exhibition.

South Africa has also seen a surge in online shopping over recent years with an approximated e-retail growth at 30% per annum.[2] The growth in online shopping in South Africa is mostly accredited to the availability of credit or debit cards as well as the increase in availability of Internet access. With the surge in cashless purchases on business premises and online, credit card security remains a concern for customers and businesses as sensitive information related to credit cards are used in such transactions. In the last 10 years, major advances have occurred in POS and online credit card security along with banks offering secure online transaction assistance via one time pins (OTPs), services such as Verified by Visa [3] or MasterCard SecureCode [4] as well as free notification alerts.

Reputable online merchants and financial institutions go to great lengths to reduce credit card fraud and to ensure a safe and secure cashless shopping experience for clients against the backdrop of credit card fraud that remains a big problem in South Africa.[5] This investigation, however, does not consider highly technical and sophisticated credit card fraud methods, like card skimming, POS hacking, site cloning or the creation of false merchant sites.[6] This investigation is based on the exploitation of the sensitive information disclosed on legitimate POS transaction receipts to make unauthorised but legitimate online shopping transactions. After the investigation by Von Solms[7], it was found that sensitive credit card information is disclosed

on certain POS transaction receipts that can be used to successfully complete online shopping transactions.
This study was undertaken to assess the extent of these disclosures and how it can be exploited. It further suggests recommendations to halt unnecessary information disclosure on POS transaction receipts so that it cannot be misused. This paper approaches the research problem by determining the state of information disclosure, examining the impact of these disclosures and, finally, proposing recommendations to protect against possible information disclosure in POS devices.

Credit Cards and information collection
In South Africa, most issued credit cards are issued by banks are either Visa or MasterCard linked credit cards. In general, the global operating regulations are followed in South Africa with changes to selected rules to better fit the local needs and risk considerations.[8] The information printed on a typical credit card contains four main elements, [9] shown in Figure 1.

< INSERT FIGURE 1 >
Figure 1: Main Elements of a Credit Card

The name of the cardholder identifies the owner of the credit card. The expiration date (exp) shows when the card was issued and when it must be replaced. The Card Verification Value (CVV) is the three digit number on the back of the card which is an authentication procedure to reduce credit card fraud transactions for card-absent transactions as it aims to verify that the user of the card is in possession thereof.[9] The PAN is the 16 digit number on the front of the card and is governed by the International Standards Organisation (ISO/IEC 7815-1:1993). Each digit in the 16 number sequence has a meaning, shown in the Figure below [10]:

<INSERT FIGURE 2>
Figure 2: Credit Card number explained

The Major Industry Identifier (MII) identifies the category of the entity that issued the credit card where the Issuer Identification Number (IIN) identifies the organisation that issued the credit card plus additional information regarding the type of card. The account number represents the unique account number where the final digit is the modula 10 checksum used to validate the PAN.
All merchants must ensure that the sensitive cardholder account information, as detailed above, is stored according to regulations. Regulation states that all material containing complete account numbers (paper or electronic) must be kept in a secure area only accessible to personnel and must be rendered unreadable in storage and before discarding. Storage of any data additional to the cardholder's name, PAN and expiration date is prohibited. No merchant is allowed to retain the full contents of the card magnetic strip or chip, CVV, PIN and passwords for the additional authentication services, even in encrypted format. [9]
It is stated in the MasterCard Security Rules and Procedures that a POS terminal or any other point of interaction may not display, replicate or store any data read from the card, except the PAN, Expiration date and Cardholder’s name. In addition it states that all card, cardholder, or transaction data must be properly protected through passwords, access controls and other access limitations.[11]

From the regulations put forward, it can be seen that only the PAN, expiration date and cardholder's name may be retained by the merchant in a safe and secure manner. The storage of any other additional information is strictly prohibited.

POS Terminals and transaction receipts

A POS terminal, being a standalone device or integrated system, is the terminal where a credit or debit card is swiped by the customer to pay a merchant for goods or services. The POS payment process consists of a series of steps, illustrated in Figure 3.

<INSERT FIGURE 3>

Figure 3: POS Payment Process

Financial services corporations have very strict rules and regulations for businesses that accept their cards for cashless transactions. These rules and regulations enable merchants to process transactions, protect cardholder data and minimise the risk of loss from fraud. As the two most common issued bank cards in South Africa are Visa and MasterCard-based credit cards, regulatory documents from these two institutions were researched in this study.

In these regulatory documents, it is recommended that all but the last four digits of the PAN are truncated on transactions receipts. All preceding digits of the PAN should be replaced with fill characters. The expiration date of the card should not appear on the transaction receipt at all and the cardholder's signature is not required when the transaction is verified by PIN. In addition it is stated that the merchant must ensure that the terminal is correctly set up for PAN suppression and exclusion of expiration date.

No specific guidelines are put forth by the credit card brands relating to information printed on the merchant copy of a transaction receipt. The only information provided by the MasterCard documents stating that the merchant documents may never reflect the PIN, any part of the PIN, or any fill characters representing the PIN as well as the CVV. MasterCard also strongly recommended that if an electronic POS terminal generates a merchant copy of a transaction receipt, the merchant copy must only reflect the last four digits of the PAN, replacing all preceding digits with fill characters. For unsuccessful transactions, the guidelines state that when a transaction is not approved, no sales receipt has to be printed [9,11].

From the above information, it is seemingly allowed that the cardholder's name is printed on the transaction receipt, as it is not disallowed. Even though it is strongly recommended not to do so, the full credit card number might be printed on the merchant's copy. In the case of a Visa card, the regulations state that the merchant's copy, possibly containing the full PAN and cardholder's name, must be stored in a secure area only accessible by personnel.

Online Shopping

Online shopping is a form of e-commerce referring to the trading in products and services using computer networks [12]. This process is graphically depicted in Figure 4.

<INSERT FIGURE 4>

Figure 4: Online Shopping Payment Process

One of the steps to curb credit card fraud is the use of the CVV number. The merchant can request the customer to enter the CVV number to verify that the customer is in the possession of

the card, thus attempting to eliminate the usefulness of stolen credit card numbers. However, not all online merchants require the CVV number to approve an online transaction. Another attempt to limit credit card fraud by reputable online merchants and financial institutions is the use of additional authentication services, such as Verified by Visa [3] and SecureCode by MasterCard. [4] These authentication services require customer information additional from credit card information, such as an OTP or a password known only by the cardholder. These services help to protect the user from fraud if somebody obtained and used their credit card details illegally. These services are also not implemented by all online merchants.
It is clear that when an online shopping site do not employ additional authentication services or the use of CVV numbers, the only information that may be required by the customer to successfully shop at the website is the PAN, expiry date and cardholder's name. This information is the same as what can legally be handled, saved and printed on POS transaction receipts by merchants, explicating the problem at hand.

Methodology
This study sought to answer the following research question: How can information disclosure on POS transaction receipts be limited to not provide sufficient information for unauthorised online shopping transactions?
To address this research question, three main steps were followed to determine the extent of disclosure to develop recommendations to curb these information disclosures. Firstly, the information gathering step took place in the form of desktop research, active collection of evidence and consultative meetings between the researcher and merchant consultants. This step resulted in the identification of the various elements of data that may be disclosed in receipts as well as the data required to successfully make an online purchase. The second step was to determine the shortcomings in the situation, which included the information printed on POS transaction receipts and the information requested by online shopping sites. These activities resulted in finding the security shortcomings of the current situation. The third and final step was to form recommendations ensure that information disclosed on POS transaction receipts is not sufficient to make successful online shopping purchases.

Information disclosure on POS transaction Receipts
Visa and MasterCard regulatory documents state that a customer should be provided with a transaction receipt upon the completion of a transaction which must comply with the applicable standards, legislation and regulations. The requirements for an electronic POS client terminal receipt from financial services corporations differ slightly, but all investigated guideline documents state that a transaction receipt must include the following information detailed in Figure 5.[9]

<INSERT FIGURE 5>
Figure 5: Example of a Transaction Receipt

After the formal specifications and recommendations of POS transaction receipts were studied, an investigation was launched into the real situation to determine what information was indeed printed on POS customer and merchant transaction receipts.[7] Over a 16-month period, two Visa credit cards were used for POS transactions where successful and unsuccessful (Cancelled/Failed) transactions were recorded. Credit card transactions from integrated or standalone POS terminals were recorded. International transactions were excluded and multiple

transactions at the same vendor were counted only once. Only POS devices belonging to four major groups were recorded. Three belonging to three main SA banks, called Bank A, Bank B and Bank C, as well as a fourth group consisting of independent external companies that provide the POS infrastructure.
In total 374 successful transactions involving approximately 60 different vendors were recorded, as well as one failed/unsuccessful transaction for each group (standalone and integrated). In all considered transactions the customer transaction receipts were retained and a photo was taken of the merchant receipts in the cases where it was allowed.
The collected transaction receipts for successful transactions differed due to the different POS terminals, but certain combinations were discovered on the merchant and customer copies of the transaction receipts. Note that the information contained in this table is not exhaustive and that it provides the cases where the most information on transaction receipts was disclosed [7]. The results for information disclosure on customer receipts are included in the graphs in Figure 6 and 7.

<INSERT FIGURE 6>
Figure 6: Information Combinations on Customer Receipts for Successful Transactions

From Figure 6, it can also be seen that the customer copies of POS transaction receipts for successful transactions include various credit card information combinations, always including a truncated PAN.

<INSERT FIGURE 7>
Figure 7: Information Combinations on Merchant Receipts for Successful Transactions

From Figure 7, it can be seen that the merchant copy of a POS transaction receipt included various credit card information combinations, with the most being PAN, Expiry date and the customer’s signature.

Two examples of the obtained receipts are provided in Figures 8 and 9:

<INSERT FIGURE 8>
Figure 8: First Example of Credit Card POS Transaction Receipts

<INSERT FIGURE 9>
Figure 9: Second Example of Credit Card POS Transaction Receipts

The transaction receipts collected for unsuccessful transactions differed due to the different POS terminals, where the discovered combinations on the transaction receipts are shown in the graph in Figure 10. Note that the information contained in this table is not exhaustive and provides the cases where the most information on transaction receipt was disclosed.

<INSERT FIGURE 10>
Figure 10: Information Combinations on Receipts for Unsuccessful Transaction

According to the regulations for unsuccessful transactions, no sales receipt need to be printed. This proved true in cases where an integrated POS devices were used. The standalone POS terminals as well as the independent external provider's terminals did indeed produce receipts.

It can be seen from Figure 10 that the "Independent service provider" group, disclosed the most sensitive information. What was discovered in one instance was that the PAN, expiration date and cardholder's name was disclosed on a single transaction receipt. An example of this transaction receipt is shown in Figure 11.

<INSERT FIGURE 11>
Figure 11: Example of Failed Credit Card POS Transaction Receipt

Thus, in certain circumstances the full PAN, expiration date and name of cardholder could be acquired from a legitimate customer transaction receipt following an unsuccessful transaction. In other cases the full PAN, expiration date and signature, possibly revealing the customer name, was printed on a merchant transaction receipt. Also, it was noticed that all merchant receipts were not necessarily stored in a secure place and in certain instances the researcher was presented with the merchant receipt.

Information requirements at online shopping sites
Having determined which sensitive credit card information could be harvested from transaction receipts, the emphasis moved to what credit card information is actually required to conduct online shopping. To determine what information is required to complete a successful online shopping transaction, local and international online shopping sites were visited and researched. The transaction requirements differed from site to site, but the information required by the vendor can be roughly divided into four categories based on credit card information requirements, shown in Figure 12.

<INSERT FIGURE 12>
Figure 12: Online shopping credit card information requirements

Through a simple Google search, multiple sites and online forums listed online shopping sites where no CVV is required, meaning that only the PAN, expiration date and name of cardholder are required to complete a successful online shopping transaction. These sites are mostly limited to American companies and sites, which includes Amazon.com, Overstock.com and Victoriasecret.com. The majority of online shopping sites studied, however, either required the CVV of the credit card or the CVV as well as additional authentication methods.

Assessment of the Current Situation
This section details the second step in the process to answer the question: "How can information disclosure on POS transaction receipts be limited to not provide sufficient information for unauthorised online shopping transactions?"
To determine if successful online transactions can be performed by using only information found on POS transaction receipts, purchases at various online stores were attempted without using information additional to the POS transaction receipts.
It can be assumed that the person who would fraudulently make an online transaction without the presence or approval of the cardholder would most likely not want to divulge personal information, like his/her home or shipping address. To circumvent the situation, only digital downloadable products were considered for purchasing. Digital downloadable products include any software, videos, e-books, digital art, templates, articles, etc. that can be downloaded from the shopping site as soon as the purchase was successful.

Various attempts were made to purchase items from online shopping stores, with several unsuccessful. On the other hand, a number of successful purchases were made at shopping sites that do not require CVV numbers. Digital products were purchased successfully and payments were made using only the 1. Cardholder's name, PAN and Expiration date found on the POS payment receipt.
Note that the payment was made by the researcher with information obtained from a POS transaction receipt, but the applicable credit card is owned by the researcher. Thus, from an ethical point of view, a legitimate purchase was made. The bottom-line is that a successful online purchase was made and paid with the mere credit card information that appeared on a POS transaction receipt.
This is indeed a worrying situation, especially taking into account that in most cases the regulatory recommendations to the merchant and/or the POS device issuing company were followed.

Recommendations for Mitigating Credit Card Information Disclosure from POS devices
The proposed strategy to mitigate sensitive credit card information disclosure consists of a list of recommendations to the respective parties involved in such POS transactions. The recommendations aim to reduce the risk of unauthorised information disclosure on POS transaction receipts whilst complying with the legal and operational requirements as well as considering relevant policies, standards and procedures. Three main aspects are considered when making recommendations, these are; technology, process and people.
The aspect of technology considers the various technologies available and the utilisation thereof. The aspect of process considers the rules, regulations and procedures that exist for POS transactions and online purchases. Research into the handling of this sensitive information by a merchant in general falls outside the scope of this paper, but it includes the handling of this information when printed on a POS transaction receipt. The process to be followed by a merchant for POS transactions is clearly stipulated in the Visa and MasterCard guidelines.
In all the receipts received throughout the investigation, all the customer copies of the POS transaction receipt contained truncated PANs, in accordance with the regulations. However, multiple merchant copies obtained in the information collection phase included the full PAN and either contained the cardholder's name or full card expiration date. This negligent act may expose the client's PAN, expiration date and/or name and maybe even a signature. Further, in the case of a failed transaction, detailed in Figure 7, the client was handed a transaction receipt where the PAN, expiration date and cardholder's name was printed, enough to make an online purchase. As these three information items are enough to make successful online purchases, the following is recommended:
1. All merchants and POS technicians must ensure that the POS device is correctly configured as to not disclose the PAN, expiration date and cardholder's name on one transaction receipt, whether a successful or unsuccessful transaction receipt.
2. If the PAN and other customer information on the merchant copy of the transaction receipt are not required for future reconciliation purposes, follow the recommendations set out by the regulatory documents and only print a truncated PAN on the receipt.
When considering online shopping sites, there exist technologies that can be utilised to ensure a safer shopping experience for clients. Although these technologies are not mandatory for online shopping merchants, the technology is available in order to make online transaction safer. The following is recommended in order to ensure a safer shopping experience for customers:

3. Merchants should make use of the secure payment options available to them as to provide a safer online shopping experience. This will eliminate the ability for unauthorised purchases when the PAN, expiration date and cardholder's name were obtained from POS transaction receipts.
The people aspect considers client and merchant awareness and responsibility relating to POS transactions and online purchases. It is stated in all regulatory documentation that care should be taken by the merchant in the processing, storage and discarding of this sensitive client information. From the study, it was determined that in certain cases, the merchant or the staff working for the merchant did not practice caution when working with this sensitive information. In these cases it can be seen that the merchant did not properly inform the staff on how to handle the sensitive customer information. This ties in with the accidental switch of the client and customer receipts by the merchant attendant. The recommendations to merchants will be to:
4. Ensure all staff operating a POS terminal is aware that they are handling sensitive customer information and that the greatest care must be taken in protecting it.
5. Ensure that all staff operating a POS terminal is aware that the client and merchant copies of the transaction receipts differ and that the correct receipt must be retained.
Clients must also be aware that the information printed on the client transaction receipts are sensitive and must be handled accordingly. They must be aware that the PAN, expiration date and cardholder's name are the only elements required to make successful online transactions at certain sites. The following recommendations are made to credit card owners conducting online shopping:
6. When the customer's bank provides the additional authentication services for online transactions, the customer must activate that service. This will provide an additional safety measure against unauthorised purchases.
7. Credit card users must check monthly credit card statements for unrecognised or questionable purchases.
8. Credit card users should never disclose their credit card information to anybody requesting it through SMS, email or phone call. A bank will never request the information via phone, email or SMS.
9. Avoid visiting online banking services or any website storing or requesting your credit card information when using a public Wi-Fi or an unknown or unsecure connection.
In multiple cases, it was found that the merchant request the client to sign the transaction receipt when the transaction was verified by a PIN. According to the regulatory documents for Visa and MasterCard, the customer's signature is not required when the transaction is PIN-verified. In the example in Figure 8, a legible signature can expose the name of the cardholder and provide all the information required for unauthorised online transactions. Phone calls to the Credit Card Helpdesks of all four major South African banks confirmed that the cardholder may ‘black-out’ the CVV number as an additional safety measure if he/she so wish. In all cases the Helpline attendants indicated that the respective bank cannot be held liable if the cardholder forgets the CVV number. The following recommendations are made to credit card holders using a POS devise:
10. The customer is not required to sign a POS transaction receipt when the transaction was verified by a PIN.
11. Credit card users must securely dispose of credit card receipts and all other mail/documents containing sensitive banking information properly.
12. If a credit card user is comfortable and his/her bank allows it, the user can black-out the CVV number at the back of the credit card as an additional safety measure. The card owner will

obviously have to store this securely somewhere if he/she wants to do online shopping at a later stage.
The proposed strategy, by means of a series of recommendations espoused above, should contribute in mitigating the risk associated with sensitive credit card information disclosure during POS transactions and thereby successfully addressing the research question posed for this study.

Conclusion

The surge in cashless purchases in South Africa over the last few years can be attributed to advantages such as flexibility, convenience and safety for purchases onsite or online.
Financial services corporations have very strict rules and regulations for businesses relating to cashless purchases and take great lengths to reduce credit card fraud, improve Point of Sale security and secure online purchases.
It was established in this study, however, that information disclosed on POS transaction receipts can be used for limited unauthorised online purchases, putting the consumer at risk. Customer account details, like credit card number, expiry date and name of the card holder may be printed on these transaction receipts which can be used in fraudulent online transactions.
This paper presented recommendations relating to technology, process and people, to assist in mitigating unauthorised disclosure of information through Point of Sale transaction receipts in South Africa.

References

1. Terblanche, Irlon. ‘Card swipes comfortably overtake cash’ Irlon Terblanche – CEO, FNB Core Banking Solutions’. Moneyweb, 4 November 2013. Accessed August 2015. http://www.moneyweb.co.za/archive/card-swipes-comfortably-overtake-cash-irlon-terbla/
2. Goldstuck, Arthur. ‘Internet Matters: The Quiet Engine of the South African Economy’. World Wide Worx, May 2012. Accessed April 2015. http://hsf.org.za/resource-centre/focus/focus-66/AGoldstuck.pdf
3. Visa International Service Association. ‘Verified by Visa’. Visa International Service Association. Accessed April 2015. http://www.visaeurope.com/making-payments/verified-by-visa/
4. MasterCard. ‘MasterCard SecureCode - Enhanced Security For Online Shopping’. MasterCard. Accessed April 2015. http://www.mastercard.com/za/consumer/securecode.html
5. SAnews. ‘Sharp increase in bank card fraud’. South African Government News Agency, 25 November 2015. Accessed August 2015. http://www.sanews.gov.za/business/sharp-increase-bank-card-fraud
6. Staff Writer. ‘How criminals steal your credit card info’. Mybroadband, 2 December 2014. Accessed April 2015. http://mybroadband.co.za/news/banking/114873-how-criminals-steal-your-credit-card-info.html
7. Von Solms, Sune. ‘An Investigation into Credit Card Information Disclosure through Point of Sale Purchases’. Proceedings of the 14th International Information Security South Africa Conference, August 2015.
8. Payment Association of South Africa. ‘Card-based payment systems’. Payment Association of South Africa. Accessed September 2015.

http://www.pasa.org.za/more_cardbased.html
9. Visa International Service Association. ‘Card acceptance guidelines for Visa Merchants’. Visa International Service Association, 2015. Accessed August 2015. https://www.visa-asia.com/ap/sg/merchants/include/card_acceptance_guidelines_for_visa_merchants.pdf
10. HowStuffWorks. ‘How Credit Cards Work’. HowStuffWorks.com. Accessed September 2015. http://money.howstuffworks.com/personal-finance/debt-management/credit-card1.htm
11. MasterCard. ‘Security Rules and Procedures - Merchant Edition’. MasterCard, 2015. Accessed August 2015. https://www.mastercard.us/content/dam/mccom/en-us/documents/SPME-manual-February2015.pdf
12. Network Solutions. ‘What is Ecommerce?’. Network Solutions, 2015. Accessed September 2015. http://www.networksolutions.com/education/what-is-ecommerce/