An Investigation into Credit Card Information Disclosure through Point of Sale Purchases

S. von Solms
Council for Scientific and Industrial
Research (CSIR)
School of Electrical, Electronic and
Computer Engineering
North West University
svsolms@csir.co.za

Abstract—**The use of debit and credit cards has become indispensable to consumers worldwide. This cashless method of payment offers flexibility and convenience. It eliminates the safety risk of carrying large cash amounts in person and cards can be cancelled as soon as it is lost or stolen. One of the most popular methods of non-cash transactions is through a Point of Sale (POS) terminal. A POS is a quick and convenient method for a customer to pay a business, but may lead to the disclosure of sensitive information without the knowledge of the customer. By investigating the information printed on the customer and merchant transaction receipts at various POS devices in South Africa, it is shown that information provided on the POS transaction receipts can put the consumer at risk as the credit card number, expiry date and name of the card holder may be printed on these transaction receipts. This paper investigates various POS devices used by South African businesses and the relevant information printed on the merchant and customer transaction receipts after a transaction. It is shown that the information contained in the transaction receipts from certain POS terminals is sufficient to perform successful online purchases at multiple online shopping sites. We also show that when the CVV number on the back of the credit card can be obtained while the transaction is in progress, even more online shopping sites can be successfully used without the authorisation or knowledge of the credit card owner.**

Keywords- Point of sale, personal information, disclosure

I. INTRODUCTION

In November 2013, one of South Africa's largest retail banks reported that in its customer segment, monthly non-cash purchases by its customers surpassed cash withdrawals by approximately R800 million. They state that across the industry, card-based spending is increasing at 38% per annum, showing that more and more consumers opt for non-cash payment options [1].

The use of non-cash payment methods, where consumers use credit or debit cards, offers flexibility, convenience and eliminates the safety risk of carrying large cash amount in person. When a credit or debit card is missing or stolen the card holder can cancel the card immediately [3-6]. In addition, most South African banks provide free notification alerts, which include SMS or emails with every successful transaction or payment due date reminders [3-6].

Owing to the growth in non-cash transactions by customers, Point of Sale (POS) terminals are widely used by businesses to carry out the non-cash transactions quickly and conveniently. A POS terminal in this paper refers to the point where the customer pays the merchant in exchange for goods or services through the use of a credit card terminal, which can be an integrated POS system or a standalone POS terminal. POS devices are also not confined to permanent business premises anymore, as more and more small business owners at flea markets and trade shows are utilising POS devices to give customers a safe alternative to cash purchases [7,8].

Non-cash purchases are not only limited to spending on business premises, as South Africa has seen a surge in online shopping over recent years. The e-retail growth in South Africa is between 30% and 40% per annum [9] and traditional retailers are allocating increasing budgets towards e-commerce expansion [10]. The availability of a credit or debit card makes purchases at reputable online retailers convenient and safe as banks are offering secure online transaction assistance via one time pins (OTPs) and services such as Verified by Visa [11] or MasterCard SecureCode [12].

With the everyday use of non-cash payment solutions, credit card security remains a major concern for individuals and businesses. All businesses and individuals want to be ensured that the payment processes between card issuer, card holder, card processor and funds collector are secure [13]. Over the past decade, major advances have occurred in POS and online credit card security and more remains to be done as credit card fraud remains a big problem in South Africa [14].

This paper, however, does not consider high tech credit card fraud methods, such as producing fake or counterfeit cards, skimming, site cloning or the creation of false merchant sites [15]. It investigates the potential misuse of information disclosed on the transaction receipts, also called a transaction information document (TID) printed by certain POS devices. Some of the merchant transaction receipts printed by the POS devices include credit card information that is to be regarded as sensitive information which can be used for certain online shopping applications.

In this paper we discuss the information disclosed on collected POS transaction receipts and how the disclosed information can be used in fraudulent activities. Section 2 of this paper includes work related to the topic. Section 3 describes the methodology followed in this investigation, while Section 4 presents the findings. The threats and consequences,

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

as well as recommendations are included in Sections 5 and 6, where Section 7 concludes the paper.

II. Related Work

This section provides relevant background information relating to the concepts significant to this paper.

A. Merchant transaction processing

Financial services corporations have very strict rules and regulations for businesses that accept their cards for card-present (on business premises) or card-absent (online) transactions. These guidelines are put in place to provide merchants with accurate, up-to-date information, rules and regulations to help merchants process transactions, protect card holder data and minimise the risk of loss from fraud [11, 12]. These regulations ensure that when a card is used at a regulated POS device or online shopping site of a reputable business, the card will be processed safely and according to regulations.

B. Credit Card operations and information

The 16 digit primary account number (PAN) on the front of the card is governed by the International Standards Organisation (ISO/IEC 7815-1:1993). Each digit in the 16 number sequence has a meaning, which is explained in the figure below [2].

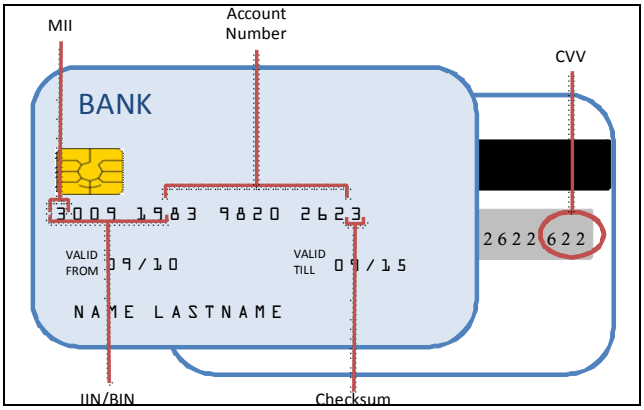

Figure 1: Credit Card information

1) Major Industry Identifier (MII): The first digit is known as the major industry identifier, which can be used to identify the category of the entity that issued the credit card [16][17]. The various categories identifiable by the MII are included in Table 1:

2) Issuer Identification Number (IIN): The IIN or the Bank Identification Number (BIN) comprises of the first 6 numbers in the PAN, including the MII. These numbers are used to identify the organisation that issued the credit card [18] and typically contains additional information regarding the type of card (debit or credit) and type of account (gold, silver, platinum) [17].

3) Account Number: Digits 7 to 15 of the PAN represents the account number. This number is unique to the credit card.

4) Checksum: The final digit of the PAN is the check digit. The Luhn algorithm, also known as the Modula 10 calculation, is used to validate the credit card number. This formula was designed to protect against accidental errors and is a simple method to distinguish between a valid number or a random range of numbers [17,19].

5) Card Verification Value (CVV): The CVV is the three digit number on the back of the credit card, which is an authentication procedure in order to reduce credit card fraud for online transactions. The CVV requested at an online purchase aims to verify that the user of the card is in the possession thereof [20].

Table 1: Major Industry Identifier categories

MII Digit	Issuer Category
0	ISO/TC 68 and other industry assignments
1	Airlines
2	Airlines and other industry assignments
3	Travel and entertainment (Diners Club)
4	Banking and financial (Visa)
5	Banking and financial (Mastercard)
6	Merchandizing and banking
7	Petroleum
8	Telecommunications and other industry assignments
9	National assignment

C. Point of Sale devices

A POS device can be seen as a computerised substitute to a cash register. A POS terminal is a mechanism for merchants to process electronic payments. It collects sales and payment information electronically, which includes the Rand amount of the purchase, the time, date and place of transaction as well as customer account information [21].

These exists many POS terminal providers, which includes South African Banks like FNB, ABSA, Nedbank, Standard Bank, as well as independent providers like Verifone and EftPOS. The standalone POS terminals provides merchants with a built-in printer, keypad and screen and can be equipped with wireless technologies for merchants seeking to receive payments remotely, for example at a restaurant or trade show. Larger companies not requiring the use of remote transactions mostly opt for a payment facility embedded within a POS system. These payment facilities are equipped with an integrated pin pad which allows for the processing of debit or credit cards and entering of a PIN at the POS [21]. The integrated PIN pad can be issued by an SA bank or independent provider.

When a credit or debit card is used at the pay point (card-present transaction), payment information is forwarded to the financial institution for authorisation and transferred back to the retailer's system to complete the transaction. The authorisation can be declined or approved, depending on the status of the client's bank account [21]. After the transaction is processed, the client and merchant are issued with transaction receipts.

Each client transaction receipt must comply with the standards and applicable law and regulations [22-25]. The requirements for an electronic POS client terminal receipt from financial services corporations differ, but all guideline documents state that a transaction receipt must include the following:

1. The merchant name.
2. The transaction date.
3. A truncated PAN showing only the last four digits.
4. A truncated card expiration date.
5. Transaction amount.
6. Space for the customer's signature, unless the transaction is completed with a PIN.

The example of a client transaction receipt shown in the Chargeback Management Guidelines for Visa Merchants [25] is shown below in Figure 2. The only guidelines put forth by the credit card brands [22-25] relating to information printed on the merchant copy of a transaction receipt was that the receipt should not reflect:

1. The PIN, any part of the PIN, or any fill characters representing the PIN.
2. The Card Verification Value (CVV).

The Mastercard Transaction Processing Rules Guidelines [22] also states that it is strongly recommended that if a POS merchant copy of the transaction receipt is produced, the copy should only reflect the last four digits of the PAN.

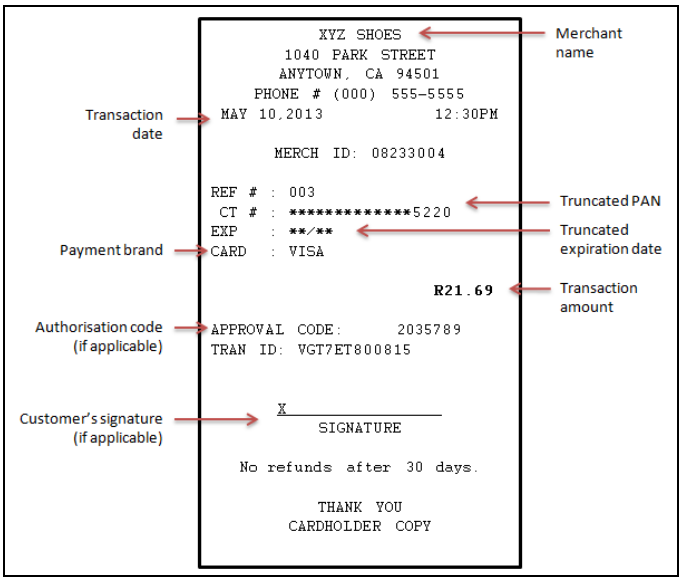

Figure 2: Proposed POS transaction receipt [25]

D. *Online transactions*

Online shopping is a form of e-commerce which refers to the trading in products and services using computer networks (card-absent transaction), such as the Internet [26]. Online shopping has been around for decades, but recently gained ground with the increase in availability of Internet access and continues to climb as mobile and Internet access continue to expand.

In general, an online store will provide a digital catalogue detailing products or services that can be purchased. Customers add the items they want to buy to a virtual shopping cart where after they provide their name, shipping address, billing address as well as their payment information. The online payment process works similarly to the POS device in a physical shop, where the credit card information is forwarded to a payment gateway which validates the information and checks for available funds, where after it transfers the funds from the client to the merchant account [27]. After a successful payment, the items are delivered to the client using various methods dependant on the acquired items or services.

Great lengths are taken by reputable online merchants and financial institutions to reduce credit card fraud and to ensure a safe and secure online shopping experience for clients. These include the implementation of additional authentication services, such as Verified by Visa [11] and SecureCode by Mastercard [12]. These services require information additional to the credit card information, which can be an OTP sent to the card holder's cell phone or a password known only by the card holder. These services protects the user from fraud if somebody used their credit card details illegally. However, not all online merchants implement these additional security measures and only request valid credit card information for transactions processing.

III. METHODOLOGY

This section discusses the method followed to determine if information provided on POS transaction receipts can be used for successful online shopping transactions. Throughout a timeframe of approximately 16 months, dating from January 2014 to April 2015, two Visa credit cards belonging to the researcher were used and two different scenarios were recorded:

1. Successful transactions.
2. Unsuccessful (Cancelled/Failed) transactions.

A. *Successfull transactions*

The successful credit card transactions from the vendors where an integrated POS device or standalone POS terminal were used, were recorded. In total, 374 successful transactions involving approximately 60 different vendors were recorded. Not all successful transactions were considered in this study. The following were considered:

1. Transactions where the author could not determine if the POS system is integrated or standalone were excluded.
2. International transactions at any POS device were excluded.
3. Only POS devices belonging to four groups were recorded. Three belonging to three main SA banks, called Bank A, Bank B and Bank C) as well as independent providers.
4. Only transactions made at a unique vendor was included.

Table 2 provides the information relating to all the successful transactions recorded. The table includes the following information:

1. Number of credit card transactions per month.

2. Number of vendors visited per month.
3. Number of transactions at facilities were an integrated POS system was used.
4. Number of transactions where a standalone POS device was used.

TABLE 2: NUMBER OF RECORDED TRANSACTIONS

Month	Total	Integrated POS		Standalone POS	
		# Transactions	# Vendors	# Transactions	# Vendors
Jan-14	15	10	10	5	5
Feb-14	15	12	8	3	2
Mar-14	16	16	7	0	0
Apr-14	21	17	6	4	4
May-14	10	7	3	3	3
Jun-14	20	16	7	4	4
Jul-14	20	16	6	4	4
Aug-14	23	19	7	4	4
Sep-14	25	19	6	6	4
Oct-14	22	21	8	1	1
Nov-14	24	18	9	6	6
Dec-14	21	18	13	3	3
Jan-15	31	28	7	3	3
Feb-15	30	29	7	1	1
Mar-15	35	27	6	8	8
Apr-15	30	26	8	4	4

In the cases when a transaction was made at a new vendor with a POS belonging to one of the four categories, the customer transaction receipts were retained and a photo was taken of the merchant receipts in the cases where it was allowed. The information on the customer and merchant transaction receipts were studied. When a transaction was made at a different branch of the same business, the customer and merchant receipts were not recorded and the vendor not considered unique.

B. *Unsuccessfull transactions*

In order to initiate failed/cancelled transactions, two main methods were used. The first method was to remove the credit card from the POS terminal before the transaction was completed and the other was to use a cancelled credit card that reached the expiration date.

Due to the difficulty of creating a failed/cancelled transactions, limited transactions were recorded in this regard. At least one unsuccessful transaction was recorded for each of the 4 groups at a standalone and integrated POS device.

C. *Online shopping*

Approximately 30 national and international online shopping sites were visited. The methods of online purchasing were studied to determine what credit card information is required for successful online transactions.

Thereafter, the information provided by POS transaction receipts were compared to information required by online shopping sites to determine if sufficient information can be obtained from POS transaction receipts in order to make successful online shopping purchases.

IV. FINDINGS

This section details the findings of the investigation described in Section 3.

A. *POS transaction receipts*

This section provides an overview on the details printed on the merchant and customer copies of the POS transaction receipts collected. It also includes illustrations showing how sensitive information is disclosed on the POS transaction receipts. The integrated POS devices were mostly encountered at large merchants or chain stores, like clothing stores, super markets, pharmacies etc. The standalone POS devices were more popular amongst smaller stores, trade show stalls and restaurants.

1) *Successful transactions*

The studied transaction receipts differed due to the use of different POS devices. Specific information combinations were discovered on the merchant and customer copies of the transaction receipt after successful transactions which are detailed in Table 3. Note that the information contained in this table is not exhaustive and that it provides the cases where the most information on transaction receipt was disclosed. There will be cases where the information will differ, especially in the "Independent service provider" group.

TABLE 3: INFORMATION COMBINATIONS: SUCCESSFUL TRANSACTIONS

Service Provider	Integrated POS		Standalone POS	
	Merchant receipt	Customer receipt	Merchant receipt	Customer receipt
Bank A	PAN Expiry date	Truncated PAN Expiry date	PAN	Truncated PAN
Bank B	PAN Expiry date	Truncated PAN Expiry date	PAN Name Signature req.	Truncated PAN
Bank C	PAN Name	Truncated PAN Name	PAN Name	Truncated PAN Name
Indepen-dent	PAN Expiry date Signature req.	Truncated PAN Expiry date	PAN Expiry date Signature req.	Truncated PAN Truncated expiry date

All merchant copies of transaction receipts for successful transactions contained the full PAN on the credit card used (see Figures 3 and 4). In addition, some of the merchant copies contained the full card expiration date or the name of the card holder. Certain copies which contained the PAN and the expiration date also required the card holder to sign, as shown in Figure 3. The information disclosures on the merchant copy of a POS transaction receipt thus include the following credit card information:

1. PAN.
2. PAN and expiration date.
3. PAN and card holders name.
4. PAN, expiration date and requested card holder's signature.

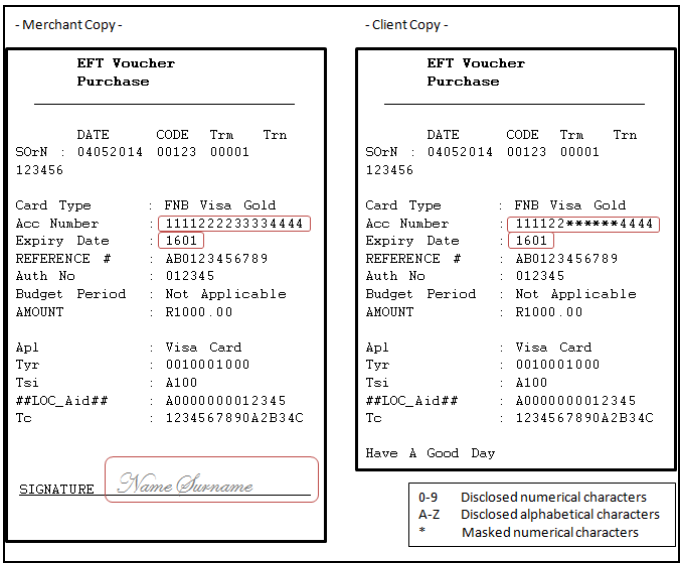

Figure 3: First example of credit card POS transaction receipts

The customer copies of POS transaction receipts for successful transactions always contained a truncated PAN showing only the last four digits (Figure 4) or showing the first six and the last four digits (Figure 3 client copy), therefore never divulging the unique account number. In some cases, however, the customer copy did provide the card expiration date or the card holder's name. The information disclosures on the client copy of a POS transaction receipt for successful transactions thus include the following credit card information:

1. Truncated PAN.
2. Truncated PAN and expiration date.
3. Truncated PAN and card holders name.

Figure 3 shows an example of the merchant copy of the transaction receipt that contained the most information as well as the equivalent customer copy. From the receipt in Figure 3 it can be seen that if the credit card holder has a clear, legible signature, the PAN, card expiration date and the card holder's name will be available to the merchant.

An example of the client copy of the transaction receipt that contained the most information as well as the equivalent merchant copy are shown below in Figure 4. It can be seen from Figure 3 and Figure 4 that although the client copy of the transaction receipt does not provide full details of the PAN, it does, however, show the name of the card holder (Figure 4) or the expiration date (Figure 3).

2) Unsuccessfull transactions

The transaction receipts printed for unsuccessful transactions differed due to the use of different POS devices. The information combinations discovered on printed receipts after unsuccessful transactions are detailed in Table 4. Note that the information contained in this table is not exhaustive and that it provides the cases where the most information on transaction receipt was disclosed.

As with the successful transactions, the transaction receipts differed due to different POS devices used. In the cases where an integrated POS device from one of the three banks were used, no sales receipt was printed for an unsuccessful transaction. For a standalone POS device provided by one of the three banks, a sales receipt was printed, but limited information was provided. This corresponds to the Card Acceptance Guidelines for Visa Merchants [24] and Mastercard Transaction Processing Rules [22], which states that when a transaction is not approved, no sales receipt has to be printed.

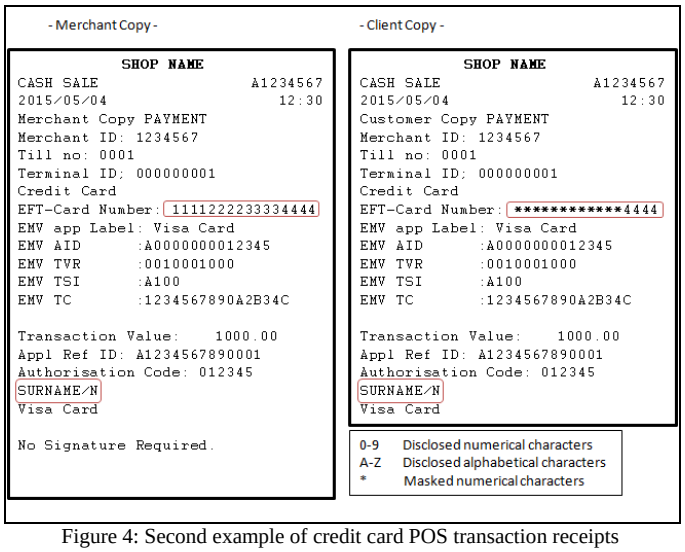

Figure 4: Second example of credit card POS transaction receipts

In the "Independent service provider" group, the receipts were different in most of the cases. The following information combinations were discovered on the receipts belonging to the POS of independent service providers after an unsuccessful transaction:

1. No sensitive information.
2. PAN.
3. PAN and expiration date.
4. PAN and card holders name.
5. PAN, expiration date and card holder's name.

Of all the unsuccessful transaction receipts recorded throughout the study, the receipt recording the PAN, expiration date and card holder's name was only obtained once. An example of this transaction receipt is shown in Figure 5.

TABLE 4: INFORMATION COMBINATIONS: UNSUCCESSFUL TRANSACTIONS

Service Provider	Integrated POS Receipt	Standalone POS Receipt
Bank A	No Slip Printed	Truncated PAN
Bank B	No Slip Printed	Truncated PAN
Bank C	No Slip Printed	Truncated PAN Name
Independent	Truncated PAN Name	PAN Expiry date Name

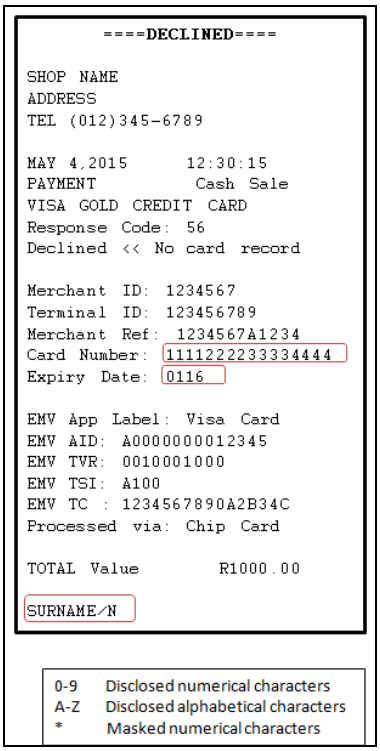

Figure 5: Example of failed credit card POS transaction receipt

3) Discussion

The guidelines put forth by the credit card brands, discussed in Section II C, only states that the transaction receipt must not reflect the PIN or CVV [22-25]. All collected receipts adhered, but not all followed the recommendation to print a truncated PAN on the merchant copy of the transaction receipt.

The merchant copy of the transaction receipts reflected a combination of the card holder's name, card PAN and card expiry date. The researcher also determined that not one merchant refused the card holder the opportunity to take a photo of the merchant copy.

B. Online shopping requirements

This section includes the findings of the research performed into the requirements for online shopping purchases. Local and international online shopping sites were visited and researched, where the transaction requirements differed from site to site. The information required by the vendor can be divided into roughly four categories:

1. Credit card number, expiry date, name of card holder.
2. Credit card number, expiry date and CVV.
3. Credit card number, expiry date, name of card holder and CVV.
4. Credit card number, expiry date, name of card holder, CVV and must be verified through an additional security step (e.g. Verified by Visa).

Due to the fact that no POS transaction slip printed the CVV number of the used credit card, no shopping sites that require the CVV can be used, therefore only shopping sites that falls in the first category listed above were further researched. With a simple Google search, multiple sites and forums listed online shopping sites where no CVV is required, which includes Amazon.com, Overstock.com and Victoriasecret.com.

A print screen of one of the online shopping sites is provided in Figure 6, which shows that no CVV number is requested for a purchase.

C. Online transaction using Transaction receipt information

In order to determine if successful online transactions can be performed by only the use of the information displayed on the transaction receipt, a purchase was at one of the online stores using only the information displayed on the collected transaction receipts. As it is assumed that the person who would commit this fraudulent activity would most likely not want to divulge his/her home address, a digital downloadable product was bought. Digital downloadable products include software, videos, e-books, digital art, templates, articles etc. These purchases are useful as these products are immediately made available for download after a successful purchase.

Through the online shopping site shown in Figure 6, a digital product was purchased and a successful payment was made using only the details found on the POS payment receipts. It was also determined that the site does not verify the card holders address against the provided billing address, as the researcher entered a business address as the billing address of the card holder, which is not the same as the residential address registered by the card holder at the financial institution. Note that the payment was made by the researcher with a credit card owned by the researcher using her legitimate name and a legitimate billing address, thus making a legal purchase.

V. THREATS AND CONSEQUENCES

This section discusses various threats and consequences associated with the disclosure of sensitive or confidential information on POS transaction receipts.

A. Online shopping fraud

From the experiment discussed in Sections 3 and 4, it can be seen that successful online transactions can be performed without the knowledge or presence of the credit card holder, using only the information disclosed by POS transaction receipts. As shown in Section 4, in some cases the merchant copy of the transaction receipt or the transaction receipt of an unsuccessful purchase provide all the information required to make online purchases at selected online shopping sites (category 1 sites).

Figure 6: Online transaction requested details

Various other online shopping sites only require the CVV number in addition to the disclosed information (category 2,3 sites). The CVV is a 3 digit number that can be quickly scanned by the merchant should he/she choose to do so. This will provide the merchant full access to active credit card details to use online at category shopping 2 sites.

Online shopping sites that implement an additional authentication service, such as Verified by Visa [11] and SecureCode by Mastercard [12] (category 4 sites), are the safest sites for online shopping as they require information additional to the credit card information from the user. This protects the user from fraud if somebody acquires their credit card details illegally.

B. Unsecured shopping sites

Upon researching online shopping sites, it was determined that there exist online shopping sites requesting sensitive information over an unsecure connection. Figure 7 shows a partial print screen of a South African online shopping site that does not use encryption.

It can be seen from Figure 7 that the URL does not begin with "https" and no padlock is displayed beside it. This shows that the sensitive information will not be encrypted or secured [28]. When entering sensitive information on an unsecured site, the user runs the risk that his/her sensitive information are disclosed to cyber criminals.

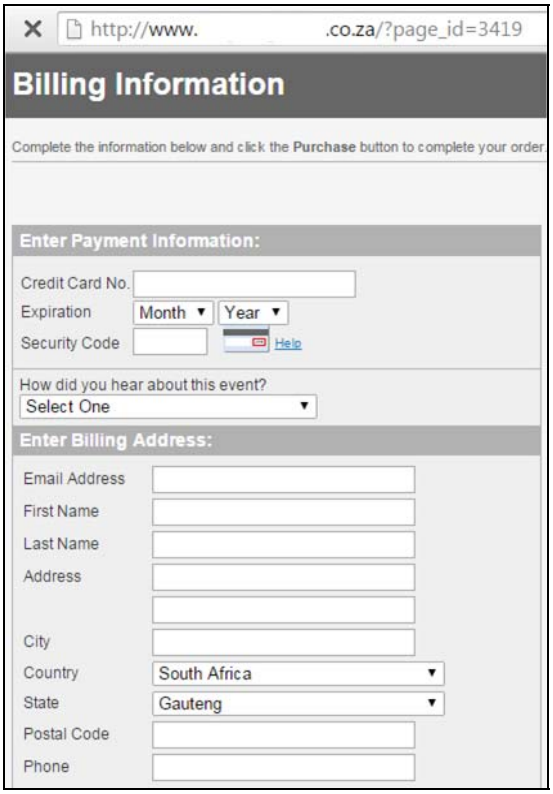

Figure 7: Unsecured online shopping site

C. Identity theft or fraud

Even though the customer copy of the POS purchase receipt only contains a truncated credit card number or card holder's name, which is not enough to use for purchases, it should still be treated as sensitive and confidential information. The truncated card information and card holder's name can be used in phishing scams in order to obtain complete account details. These scam artists can pose as the bank or the company where the purchase was made in an attempt to obtain the card holder's full details [29].

When these receipts are disposed of along with other personal files, criminals known as "dumpster divers" can collect even more information, such as names, addresses, phone numbers or ID numbers. Inadequate disposal of this information can allow identity thieves to create fraudulent accounts and make illegal purchases.

D. Merchant management of credit card details

It was established that a handful of small business at casual trading premises like flea markets and trade shows with no POS device available on site, would request the customer to fill in an order form which requires the client's credit card information. These order forms are later used by the business to bill the client for the requested goods. Figure 8 shows a partial scan of such an order form obtained at a trade show.

Figure 8: Order form of small business at trade show

The credit card holder has no knowledge of how the merchant will manage the confidential and sensitive information contained in such a form. If disposed of incorrectly, the merchant can provide criminals with the card holder's personal details.

VI. RECOMMENDATIONS

This section considers the measures that can be taken by a credit or debit card account holder in order to protect their credit or debit card information.

1. Dispose of credit card receipts and all other mail/documents containing sensitive information properly.
2. Check monthly credit and debit card statements for unrecognised or questionable purchases.
3. Never provide your credit card details on unprotected sites.
4. Never complete a printed order form asking for complete credit card details. If unable to pay cash, request the banking details of the business to perform an Electronic Funds Transfer (EFT).

5. Never disclose your credit card information to anybody requesting it through SMS, email or phone call. A bank will never request your information via phone, email or SMS.
6. Avoid visiting online banking services or any website storing or requesting your credit card information when using a public Wi-Fi or unknown connection.
7. Avoid entering sensitive information on unsecured web sites.

VII. Conclusion

The use of debit and credit offers consumers flexibility, convenience and eliminates the safety risk of carrying large cash amounts in person. Card transactions are a quick and convenient method to pay a business on site or online.

Financial services corporations have very strict rules and regulations for businesses relating to card-present or card-absent transactions. These regulations ensure that a card transaction is processed safely at a regulated POS device or online shopping site. There are, however, information reflected on certain POS transaction receipts that can be used for limited fraudulent online purchases. The sensitive information, when disclosed, can also be used by criminals for phishing attacks and possible identity theft.

VIII. References

[1] I.S. Da Silva, "Card payments overtake cash in South Africa," Moon of the South: News from Africa. (Accessed 20 Aug 2014) http://moonofthesouth.com/card-payments-overtake-cash-south/

[2] howstuffworks, "How Credit Cards Work," (Accessed 9 Sept 2014) http://money.howstuffworks.com/personal-finance/debt-management/credit-card1.htm

[3] Absa, "Credit Cards', (Accessed 17 April 2015) http://www.absa.co.za/Absacoza/Individual/Banking/Credit-Cards/Platinum-Credit-Card

[4] Standard Bank, "Safety Tips", (Accessed 17 April 2015) http://www.standardbank.co.za/standardbank/Personal/Banking/Credit-cards/Learn-about-the-card/Safety-tips

[5] FNB, "Security Centre", (Accessed 17 April 2015) https://www.fnb.co.za/security-centre/index.html

[6] Nedbank, "Card fraud, (Accessed 17 April 2015) https://www.nedbank.co.za/website/content/CrimeAwareness/cardfraud.asp?page=card

[7] M.W. Byrne, "How to Process Credit Cards from a Booth or Flea Market", Top Ten Reviews, (Accessed 10 April 2015) http://credit-card-processing-review.toptenreviews.com/how-to-process-credit-cards-from-a-booth-or-flea-market.html

[8] S Howard, "Why your flea market stand needs to accept credit & debit cards", The Official Groovv Blog, (Accessed 10 April 2015) http://www.groovv.com/blog/credit-card-machine-can-boost-business-selling-flea-markets/

[9] A Goldstuck, "Internet Matters: The Quiet Engine of the South African Economy", World Wide Worx, 2012

[10] T Holmes, Chasing the e-tail a costly investment", Mail and Guarduian, (Accessed 10 April 2015) http://mg.co.za/article/2014-06-26-chasing-the-e-tail-a-costly-investment

[11] Visa, "Verified by Visa", (Accessed 9 April 2015) http://www.visaeurope.com/making-payments/verified-by-visa/

[12] MasterCard, "MasterCard SecureCode - Enhanced Security For Online Shopping", (Accessed 9 April 2015) http://www.mastercard.us/securecode.html

[13] N Nessar and G Miller, "Method for Secure Credit Card Transaction", International Conference on Collaboration Technologies and Systems (CTS), pp 180-184, 2013

[14] South African Government News Agency, "Sharp increase in bank card fraud", (Accessed 9 April 2015) http://www.sanews.gov.za/business/sharp-increase-bank-card-fraud

[15] Staff Writer, "How criminals steal your credit card info", mybroadband, (Accessed 10 April 2015) http://mybroadband.co.za/news/banking/114873-how-criminals-steal-your-credit-card-info.html

[16] J.M. Simon, "What are those numbers on my credit card?", creditcards.com, (Accessed 10 April 2015) http://www.creditcards.com/credit-card-news/credit-card-appearance-1268.php

[17] D Addison, "Anatomy of a credit card number and the utility of the BIN", The Dirigo Blog, (Accessed 10 April 2015) http://www.dirigodev.com/blog/ecommerce/anatomy-of-a-credit-card-number/

[18] Investopedia, " Bank Identification Number - BIN", investopedia.com, (Accessed 12 April 2015) http://www.investopedia.com/terms/b/bank-identification-number.asp

[19] J MacDonald, "How the 'Luhn formula' validates credit card numbers", creditcards.com, (Accessed 10 April 2015) http://www.creditcards.com/credit-card-news/luhn-formula-credit-card-number-system-1273.php

[20] CVVnumber.com, "CVV Number location and information" (Accessed 10 April 2015) https://www.cvvnumber.com/

[21] First Data, "Payments 101: Credit and Debit Card Payments", White Paper, October, 2010.

[22] MasterCard, "Transaction Processing Rules", 2014.

[23] MasterCard, "Security Rules and Procedures - Merchant Edition", 2015.

[24] Visa, "Card Acceptance Guidelines for Visa Merchants", 2014.

[25] Visa, "Chargeback Management Guidelines For Visa Merchants", 2014.

[26] Network Solutions, "What is Ecommerce?", (Accessed 11 April 2015) http://www.networksolutions.com/education/what-is-ecommerce/

[27] Shopsite, "How does E-Commerce Work?", (Accessed 11 April 2015) http://www.shopsite.com/help/quickstart/ecom-intro-03.html

[28] National Cyber Security Alliance, "Online Shopping", StaySafeOnline.org, (Accessed 6 May 2015) https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/online-shopping

[29] M Warnick, "9 things you should know about your credit card receipt", creditcards.com, (Accessed 21 April 2015) http://www.creditcards.com/credit-card-news/9-things-to-know-about-credit_card-receipts-1273.php