Confidentiality

This research report is submitted for academic evaluation for the Masters of Business Leadership only and contains factual, sensitive information.

This research report and its contents may not be disclosed, reproduced, published, distributed or used without the express authorization from its author.

Declaration

I hereby declare that this research report is true, correct and my own work. All references have been acknowledged in this work.

_____

Richard Bernard de Matos

Acknowledgements

Numerous people deserve to be thanked for their assistance in contributing to this study. I am particularly grateful to my wife Michele whose patience, fortitude and perseverance enabled me to complete this work. Further contributors whose input and insight assisted in this research include:

- The Standard Bank of South Africa Ltd (Card Division Merchant Services and Group IT)
- Diners Club International
- SABRIC
- MasterCard International
- Visa International
- ABSA
- First National Bank
- Nedbank
- Investec
- ConnectNet Broadband Wireless (Pty) Ltd
- Fair, Isaac
- Bankserv
- Retail Decisions
- Computer Software Consultants
- X-Link

These various entities professionalism and dedication were instrumental in assisting in this research.

Executive Summary

Credit card fraud losses within the South African credit card market in 2006 exceeded R257M. A portion of these losses (R179M) are within the borders of South Africa and its common monetary area partners. This represents a startling 70% of credit card fraud on magnetic stripe cards used within the borders of South Africa.

The South African credit card industry adopts floor limits at certain merchants and merchant categories. South Africa is one of a few countries in the world that still adopt floor limits on credit cards within its payment card industry. Credit card transactions on magnetic-stripe cards conducted below the merchant's designated floor limit do not go to the issuing bank for authorization. The first time the issuing bank acknowledges these transactions is when they are settled on average two days later. The rationale for not adopting zero floor limits within the South African credit card market is the supposed inability of the existing telecommunications infrastructure to handle the volume and frequency of data submitted by merchants for authorization. The impact of reduced fraud and bad debt losses through adopting a zero floor limit in relation to merchant operational costs is the basis of the research. The research also aims to examine the Proposition that the existing telecommunications infrastructure is unable to support a zero floor limit proposal.

Table of contents

Table of figures

Table of tables

Appendices

Appendix 1: Proposed floor limits in South Africa

Appendix 2: Survey questionnaire

Appendix 3: Transaction and volume profiling

Appendix 4: Actual and theoretical authorization volumes at Standard Bank

Appendix 5: MasterCard floor limit mandate

CHAPTER 1

1. ORIENTATION

1.1 The South African credit card fraud landscape

Credit card fraud has been prevalent since the inception of credit cards as a transactional product. According to Akers et al, the present day credit card industry originated in the nineteenth century. In the early 1800's merchants and financial intermediaries provided credit for agricultural and durable goods. In the late 1950's, the Bank of America began the first general purpose credit card program.

Guerin, D, 2003 states in his executive summary on Fraud in Electronic Payments that the continued growth in fraud is a real threat to revenue growth and consumer confidence. The attitude is changing where the payment card industry sees "fraud as an annoying and inescapable cost, to seeing fraud as a real threat to profitability".
Miscreants have used various techniques and technologies to defraud issuing and acquiring banks and their respective customers. The credit card product has evolved not only in terms of its conventional value proposition and customer-oriented design, but also in terms of its aesthetic and technological features in an effort to thwart fraudsters. Bank-issued credit cards in the South African industry are either individually-branded by the issuing bank (proprietary cards) or co-branded under the auspices of international Associations (MasterCard International, Visa, Diners Club International or American Express). Should a credit card be dually-branded by the Association and issuing bank, the respective product would need to conform to the franchise regulations pertaining to the card features, technology and acceptance criteria. In research performed by Akers et al, Visa and MasterCard together held about 70 percent of the market share of the general-purpose card market.

LexisNexis Butterworths (2002:42) define fraud as "the unlawful and intentional making of a misrepresentation (lying) which causes actual harm or which could harm another person".

LexisNexis Butterworths (2002:43) define forgery and uttering: “Forgery is committed by unlawfully making a false document with the intent to defraud (cheat). This must lead to the harm or possible harm to another person. The crime known as “uttering a false document” is committed when a person unlawfully offers, passes off or communicates a forged document with the intent to defraud, to the actual prejudice of another person”.

For the purposes of this research report, we use the common law crime, fraud, as this is the case where another person masquerades as the true cardholder and commits this crime by prejudicing another party financially.

An inherent limitation of South African bank-issued credit cards is that they have a magnetic stripe which is easily compromised by fraudsters. Contained within the magnetic stripe is sensitive card and cardholder data notwithstanding card numbers, card expiration dates and unique card identifiers. This information can be readily retrieved by miscreants and used to perpetrate fraud. Most credit card products within South Africa are signature-based. The signature on the reverse of the credit card is compared to the cardholder-signed sales voucher by the merchant. Apart from the cosmetic security features built-into the credit card (holograms and unique security characters/features), the merchant’s only reliance that the presenter of the card is the lawful cardholder is the signature verification which takes place during the sale. This verification is open to substantial subjectivity and does very little to ensure that the presenter is *bona fide*.

Coupled to the product limitations in reducing risk exposure, it operates in an environment where floor limits are assigned to select transaction types or merchants (or categories of merchants) which participate in the franchise arrangement and are signed-up by the acquiring bank to accept the products. Transactions conducted below the merchant’s assigned floor limit do not go to the issuing bank for authorization and are only acknowledged by the issuing bank on average 1 to 2 days later during settlement. This is the first time that the issuing bank is able to detect questionable transaction behavior and take preventative steps to curtail further fraud. Albeit those issuing and acquiring banks have invested in chip and PIN technology, the roll-out has been lethargic and magnetic-stripe technology is expected to be a feature of the card until all card acceptance channels have been converted to accept this technology.

According to Ward S. 2007, in her guide to small businesses under the topic of credit card fraud, states that a questionable behavior on the part of a card presenter is one where they “ask what the floor limit is – and then either make purchases to just fall under the floor limit or ask to have items processed separately, so their credit card purchase doesn’t exceed the floor limit”.

1.2 How credit Cards work

According to Wikipedia (http://en.wikipedia.org), a credit card is a payment product, whereby the issuing bank lends money to the consumer. A credit card is different from a debit card in that it does not subtract money from the customer’s account after every transaction. It also differs from charge cards (Diners Club and American Express) in that it does not require that the balance outstanding be paid in full at the end of each month. A credit card “revolves” in that the balance outstanding can accrue interest with a minimal payment being due after every cycle (up to 55 days). A cardholder generally pays a nominal fee (usually 7.5% in South Africa at the time of this report) on the outstanding debit on the account. A cardholder receives a credit card after the facility has been approved and granted by the credit provider. The card is then used to make purchases from merchants who accept credit cards up to a pre-established credit limit. When a purchase is made by the customer, they agree to pay the credit card issuer. The sale is authenticated when the cardholder signs the sales voucher or keys-in a PIN number. The merchant’s point-of-sale machine allows merchants to verify that the card is valid and that the cardholder has sufficient credit to effect the sale by dialing up to the acquiring bank for authorization. The acquiring bank has a commercial engagement with the merchant and will route this authorization request to the issuing bank for authorization. According to Wikipedia (http://en.wikipedia.org), “electronic verification systems allow merchants to verify that the card is valid and the credit card customer has sufficient credit to cover the purchase in a few seconds, allowing the verification to happen at the time of purchase. The verification is performed using a credit card payment terminal or point-of-sale (POS) with a communications link to the merchant’s acquiring bank. Data from the card is obtained from a magnetic stripe or chip on the card”.

The credit card issuer sends a statement indicating the purchases made by the customer which includes any accrued and outstanding fees. The cardholder must pay a predetermined amount or portion of the bill on a due date agreed with the card issuer. The credit card issuer charges interest on the outstanding balances that have revolved and includes this finance charge on the statement.

From a merchant's perspective, the credit card transaction is regarded as a reasonably secure form of payment (in comparison to cheques) as the issuing bank commits to pay the merchant once the transaction is verified and acknowledged by the issuing bank. The acquiring bank charges the merchant a commission for processing the merchant's sales (performing the accounting where the merchant is credited and a settlement tape is sent to the issuing bank to financially adjust their customer's accounts accordingly). A merchant may be penalized (or "charged-back") if the merchant did not process the transaction as prescribed by certain regulations and rules.

The credit card process involves the following parties:

- **The cardholder**: the legal owner of the card who has received a line of credit from the issuing bank
- **The merchant**: The business which sells goods and services and accepts the credit card as a means of payment.
- **The acquirer**: the financial institution or other organization that provides financial services to the merchant.
- **The Card Association**: A network such as MasterCard or Visa (and others) that acts as a gateway and intermediary between the issuing and acquiring bank for authorizing transactions and switching settlement files between the issuer and acquirer. (In South Africa, some intra-country (domestic) transactions are switched via a local switch).
- **The Issuer**: the financial institution that provides credit via a credit card to the customer.

The flow of information and money between the abovementioned parties is known as interchange and consists of the following processes (http://en.wikipedia.org):

1. **Authorization**: The cardholder transacts at the merchant (who performs some risk assessment) and depending on whether the transaction is above the merchant's prescribed floor limit, may send the transaction on-line to the issuing bank for authorization. The issuer may provisionally debit the funds from the cardholder's credit account (until the merchant banks or settlement has occurred).

2. **Batching**: Once the transaction has been successfully conducted on the merchant's point-of-sale, it is stored in a batch, which the merchant sends to the acquirer during a predetermined schedule to receive payment. The batch is processed by the acquiring bank and a settlement tape is created which is sent to the issuing bank to financially adjust their customer's accounts.

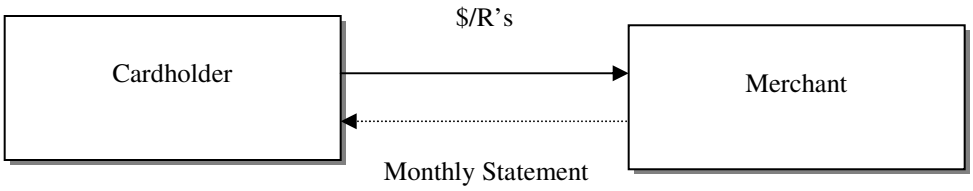
3. **Clearing and Settlement**: Once the acquiring bank has been paid by the issuing bank, the acquirer credits the merchant's account for the sales. The amount which the merchant receives is equal to the transaction amount minus the discount which the acquiring bank takes off for processing the respective sales. In the event of a chargeback, the issuing bank returns the transaction to the acquirer for resolution and in the event that the chargeback is valid, the merchant must accept the chargeback or contest it further.

   The entire process from authorization to funding usually takes about three days. The interchange process is depicted in the next section which illustrates the fraud problem where transactions are used below the merchant's floor limit. The section commences with an illustration of the entire authorization, clearing and settlement process.

1.2.1 Settlement delay contributing to the "below floor-limit" fraud problem

The functioning of credit card networks is based on the models illustrated by Akers et al:

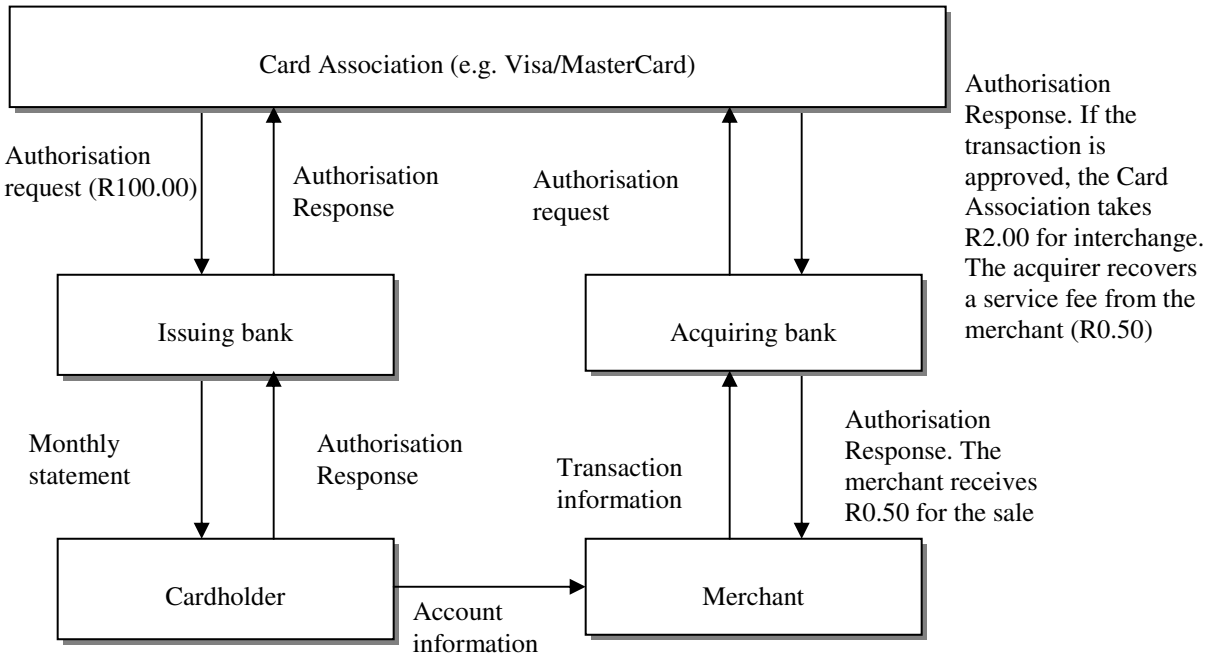
Figure 1: The bilateral model



Source: Akers, D, Golter, J, Lamm, B & Solt, M, 2005.

This figure illustrates the simplest bilateral model where funds flow between a merchant and a cardholder. In this instance the merchant extends credit and on a monthly basis the merchant will tender a bill to the customer for payment.

Figure 2: The multiple card issuer model



Source: Akers, D, Golter, J, Lamm, B & Solt, M, 2005.

Figure 2 illustrates the complex multiple card issuer model as depicted by Akers, D, Golter, J, Lamm, B & Solt, M, 2005. The model contains the Card Association, many cardholders, many merchants and many banks. In this model, the Card Association imposes rules and regulations for the issuance of credit cards, the clearing and

settlement of transactions, advertising and promoting the Association's brand, authorising the respective transactions and fees and revenue between the model participants. Each participant in the model has a financial incentive for participating in the model. *Figure 2* illustrates the following process:

The cardholder purchases a product or service from the merchant. A credit card is tendered for payment. In the event that the transaction is above the merchant's designated floor limit, the merchant will transmit the account details and transaction details to the acquiring bank. The acquiring bank will then route this information via the Association to the issuing bank for authorisation. The issuing bank will then authorise or deny the transaction and send this response back via the Association to the acquiring bank and then to the merchant. If the transaction was approved, the issuing bank also sends to the acquiring bank, via the Association, the transaction amount less an interchange fee. The interchange fee is established by the Card Association. An example of the interchange process is illustrated by the model (arbitrary amounts have been used). In the example, the purchase price was R100.00 and R2.00 was deducted by the Association for payment to the issuing bank. The acquirer deducts R0.50 for processing costs and the merchant receives R97.50. The issuing bank bills the customer for the full R100.00 and receives payment from the cardholder. The Card Association receives a small fee for each transaction which the issuing bank pays.

Acquirers engage in a commercial relationship with merchants to accept credit cards and depending on the nature of the merchant and the infrastructure and technology the merchant has available, the acquirer may give the merchant credit card facilities. The acquirer or an agent acting on their behalf (third-party processor) will then process the transactions on behalf of the merchant. The merchant's point-of-sale facility (in the case of a "face-to-face" merchant) is programmed to dial-up to the acquirer to bank the credit card proceeds during a predetermined schedule. The merchant may also elect to do this manually. The acquirer will then credit the merchant for the sales (subject to cleared effects) and send settlement files to the issuing banks (whose cardholders transacted at the merchant) who in turn will financially reimburse the acquirer and financially account to their respective cardholder's accounts. The process is schematically represented in *figure 3*. The arrows depict the sequence of events as follows:

Step 1: The point of sale transmits the transactional data to the acquiring bank for processing during a predetermined scheduled which is programmed in the device's software.

Step 2: The acquiring bank financially reimburses the merchant for the transactions as part of their commercial engagement (subject to cleared effects).

Step 3: The acquiring bank then identifies the entire issuing bank's transactional data and compiles a settlement tape.

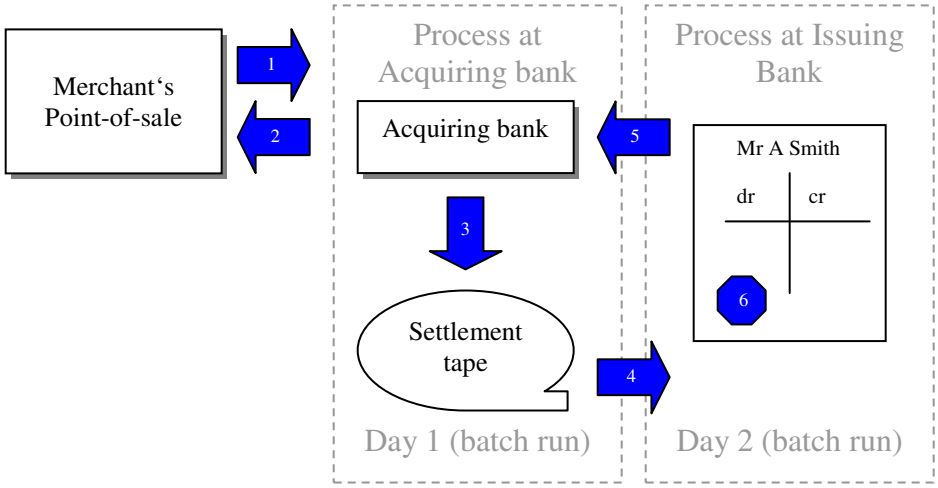
Step 4: The settlement tape is then sent to the issuing bank so that it can financially account to the cardholder's account.

Step 5: The issuing bank financially reimburses the acquiring bank for the transactions its cardholders concluded.

Step 6: The issuing bank then credits the cardholder's account (in the case of a refund) or debits the cardholder's account (in the case of a sale).

The entire process takes on average two days in the case of the acquiring bank and the issuing bank being separate institutions. The delay is attributed to two separate batch runs, one batch run for the acquiring bank to obtain its merchant's sales and create a settlement file for the issuing bank, and one batch run for the issuing bank to financially adjust their cardholder's accounts. Batch runs do not normally take place during normal office hours. If the issuing bank and the acquiring bank are the same institution, this process generally takes one day.

Figure 3: The settlement delay where the issuing and acquiring bank are separate entities



As most acquiring banks brand their merchant's point of sale devices, fraudsters are able to easily differentiate between acquiring banks. Fraudsters are aware of the two day settlement delay between an acquirer and issuer (in the case where they are two separate institutions) and thus use compromised cards at these establishments below the merchant's assigned floor limit. The issuing bank will only acknowledge the sale after the transactions has been processed to the cardholder's account two days later. No amount of investment in fraud detection and prevention software from an issuing banks' perspective will be able to prevent or identify questionable card activity before the transaction is settled. Fraudsters are able to thus use the account's funds in excess of the card's allocated credit limit. This not only poses a fraud risk but also a credit risk in that the settlement delay can invariably create "additional" credit which is not catered for by the issuing bank. The settlement delay and the concomitant fraud/credit risk life cycle are depicted below:

Figure 4: The fraud/credit risk life cycle where the issuing and acquiring bank are separate entities

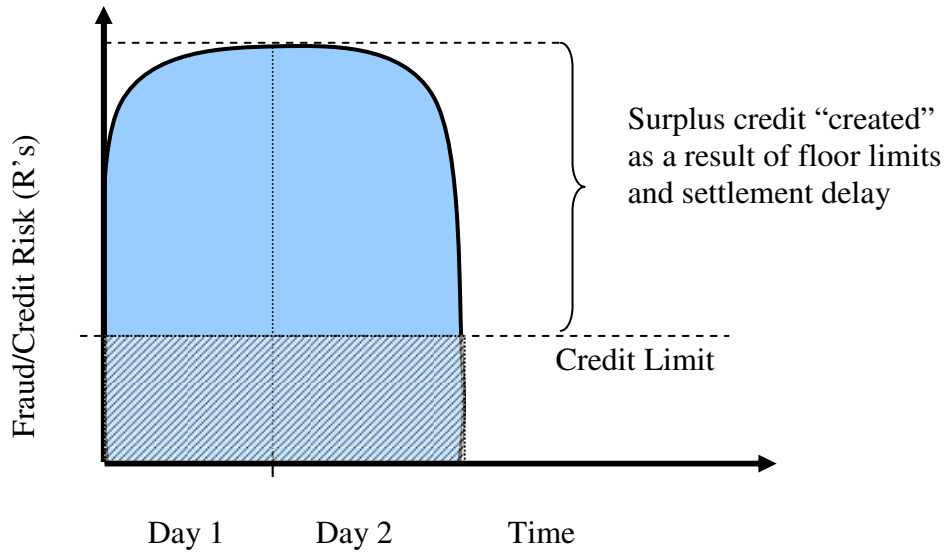


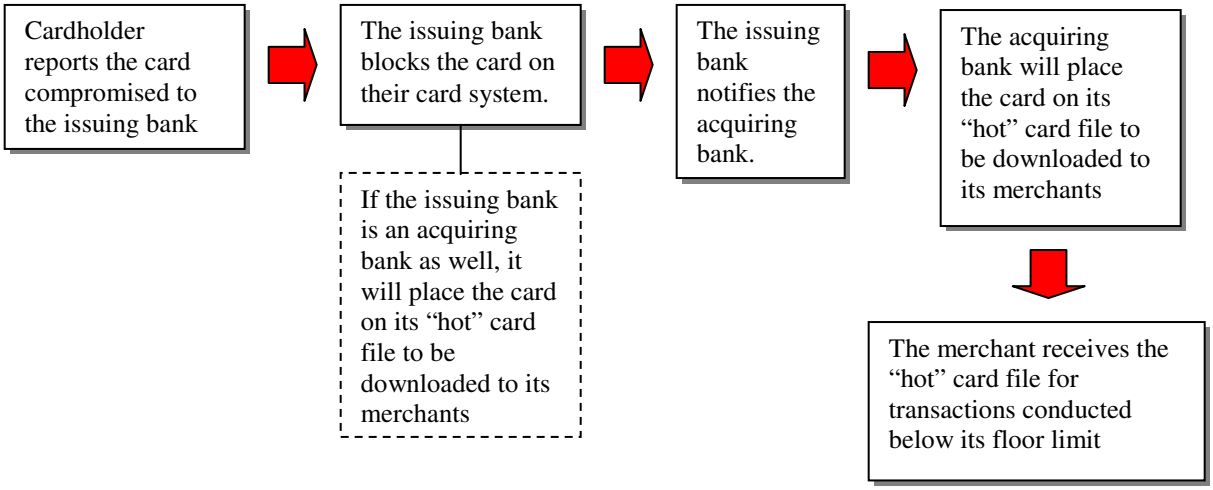
Figure 4 above illustrates the two-day fraud life cycle. The area below the shaded area represents the credit limit assigned to the cardholder based on their qualifying criteria on card application. The area above the shaded region is the surplus credit "created" and abused as a result of the merchant's floor limits and the settlement delay. This scenario holds true in instances where the issuing bank and the acquiring bank are not synonymous.

1.2.2 "Hot" card files

As credit cards can be used fraudulently below a merchant's designated floor limit, the issuing banks are at risk as they do not see or acknowledge the transaction(s) until they are settled up to two days later. In an effort to control the risk, "hot" card files have been created by terminal vendors of point-of-sale machines which enable a predetermined amount of compromised cards to be stored within the point-of-sale software. Issuing banks communicate the compromised cards to acquiring banks which in turn transmit this data to the merchant's point-of-sale during batch run when the device dials the acquiring bank's front-end processor to do its banking. The storage capacity of the point-of-sale for "hot" or compromised cards is limited. The acquiring bank and issuing bank enter into an arrangement as to what the issuing bank's allocation is for "hot"

cards. The acquiring bank has an obligation to its merchant to safeguard it against potential fraud and as such obtains issuing bank's compromised cards from all over the world. Due to the point-of-sale's storage limitations, cards are systematically purged from the "hot" card files after a passage of time. The purge is based on an aging process (generally first-in, first-out) or is done so by the issuing bank. Guerin, D, 2003 confirms that issuing banks only list the "most current and high-risk, hot-listed cards before being sent for authorisation, so that stolen cards may be rejected even if the transaction is below floor limit". In South Africa, compromised cards can be loaded on merchant's point-of-sale devices for up to 60 days where after they automatically purge. The hot card file process is depicted in *figure 5* below:

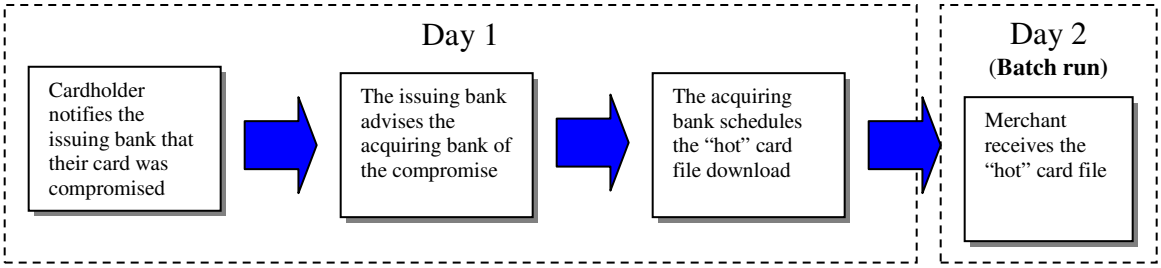
Figure 5: "Hot" card file process



The "hot" card file is somewhat different for merchant's who do not have a conventional point-of-sale and who use their own integrated solution which is linked to an inventory control system. These merchants typically get an extended "hot" or exception file from the acquiring bank as they have the hardware and software to accommodate more exception card numbers.

It can take the issuing bank up to two days to close the point-of-sale channel for compromised card numbers. If the issuing bank and the acquiring bank are the same institution, the compromised card can be stopped from being used at point-of-sale the next day. In the event that the issuing bank and the acquiring bank are not synonymous, it takes up to two days (or longer) for the acquiring bank's merchants to receive the compromised card(s). The delay is depicted below:

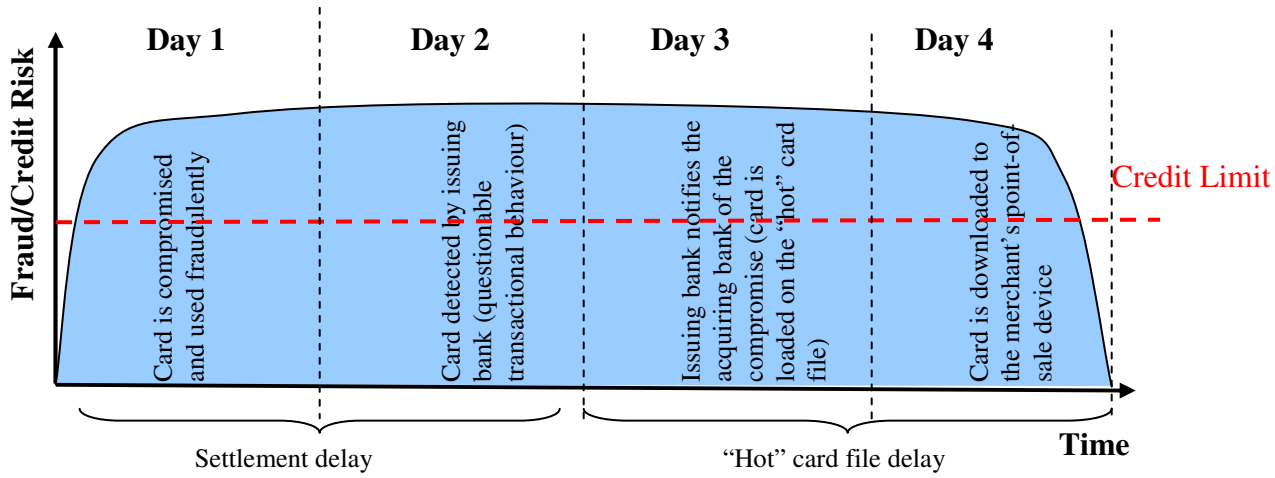
Figure 6: “hot” card file delay



The issuing bank has to prioritize the listing of its hot cards. All issuing banks in South Africa have more compromised cards that the “hot” card allocation which acquirer’s allow them on their merchants’ point-of-sale devices. Compromised cards may not necessarily be South African – issued cards but might include foreign cards as well.

The two-day delay of ensuring that the issuing bank’s compromised card is loaded on the “hot” card file increases the fraud life cycle as illustrated in *figure 7*. If one combines the settlement delay with the delay in sending the hot card file to the acquirer’s merchant’s point-of-sale (assuming the two institutions are not synonymous), the following life cycle is apparent:

Figure 7: Extended fraud life cycle



The illustration above depicts the extended fraud life cycle as a result of the settlement and the “hot” card file delays. It is through these delays that fraud perpetrated below the

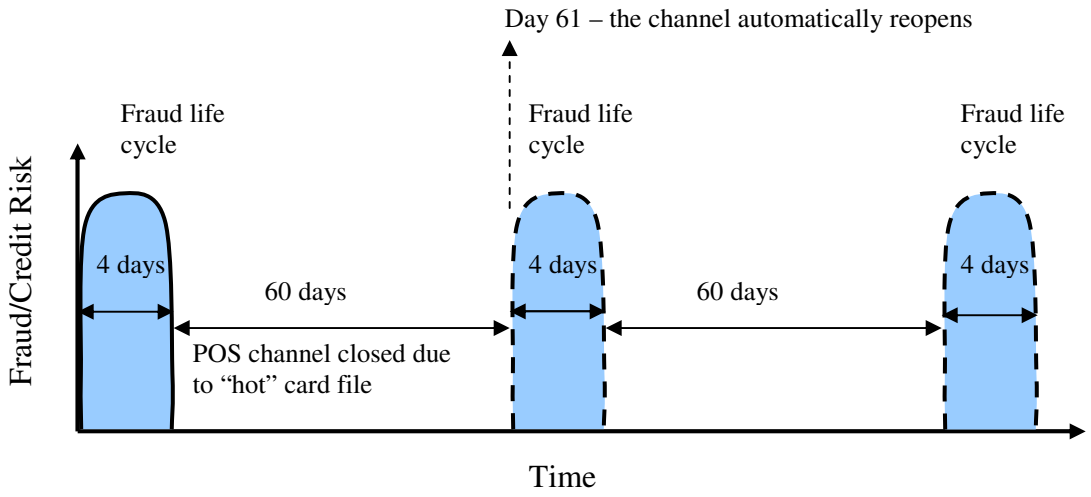
merchant's floor limit can exceed the credit funding on the account and result in substantial fraud losses to the issuing bank. There are also associated costs of managing this "hot" card file which includes staff costs, operational costs and costs to the acquirer via charge backs which are discussed under the next heading. The 4-day fraud life cycle may be extended in instances where the issuing bank's fraud detection systems or operational constraints do not detect the questionable transaction behaviour on day 2 (during settlement). The longer the issuing bank takes to authenticate the questionable behaviour with its customers, the longer the fraud life cycle can be extended. Albeit that the "hot" card file can forewarn merchants that the credit card has been compromised and in so doing avert any further potential losses to the issuing bank, the aging of the credit card from the point-of-sale due to capacity constraints further exacerbates the losses. This can be illustrated in *figure 8* below.

The card can only be loaded on South African merchant's "hot" card files for a period of up to 60 days where after it purges. This means that the point-of-sale channel cannot be permanently closed and automatically reopens after 60 days. Fraudsters are currently aware of this constraint and use the card for its 4-day life cycle until it is loaded on each merchant's point-of-sale. The miscreants then retain the card until it has purged from the "hot" card file (day 61) and then reuse it, perpetuating the fraud life cycle.

An article published by Levi, M et al (1991) confirm this in the following statement "Patterns of fraudulent use reveal that after initial use within the first day of theft, some fraudsters wait months until they expect that the card has been removed from the "hot file" and then reuse it"

According to Smith, R.G, 1997, it has been suggested that floor limits which apply to cards be reduced in order for transactions other than those involving very small amounts. Smith advocates that one of the main strategies used to prevent point-of-sale fraud has been to lower floor limits. This means that many more transactions will now require bank's approval.

Figure 8: perpetuating fraud life cycle



Guerin, D, 2003 states in his publication on Fraud in Electronic Payments that fraudsters generally make as many purchases as possible within a window of time until the card is reported stolen by the customer to the issuing bank who in turn blocks the card. In some instances, the cardholder may not be aware that the card is missing (which is especially the case for *Lost fraud*) which in turn provides more time for the fraudster to transact. Guerin, D, 2003 goes on to state "Authorisation floor limits are amount thresholds used in dual-message environments below which purchases do not have to be authorised by the merchant, introduced to reduce the cost of merchant phone calls. In some European countries, knowledgeable fraudsters will specifically target stores with a transaction amount that is just below the merchant's authorisation floor limit to maximise the usage of the card even when it is blocked by the card issuer". This underscores the life cycle presented and discussed above. He goes on to state further that "Eventually, such cards may be sold abroad for use in countries with **poor telecommunications networks**".

South Africa currently deploys a service known locally as the Industry Negative Card File (INCF) The service is hosted by Retail Decisions, a leading card-based transaction services business providing fraud prevention to the finance, telecommunications, retail and e-commerce sectors. An article by www.finextra.com contextualizes this service by stating "card transactions are screened against the Industry Negative Card File (INCF), a national database of lost, stolen and delinquent cards. Retail Decisions will collate and update the INCF for the banks and retailers using information gleaned from the

Prism system. The INCF currently contains more than 2 million records from South African card issuers and over 5 million records from other international card issuers".
This service was introduced due to the inordinate amount of fraud taking place at large merchant establishments (commonly referred to as "Blue Chip" merchants) and franchises. Fraudsters target these retail outlets due to the variety of goods sold and the probability that the fraudster's anonymity will be preserved as a result of the multiple purchase points (tills). The fraudster could shop at these merchants multiple times without anyone noticing the irregularity of this purchasing trend.

The large retailers also had an infrastructure to accommodate an industry negative card file. Conventional merchants, when signed-up by an acquiring bank, are issued with a point-of-sale device to facilitate processing credit card sales. Larger merchants have their own computer infrastructure that does not necessitate the installation of a point-of-sale device. More often than not, the computer infrastructure (referred to as an integrated solution) for these "host" merchants are more than a point-of-sale in that the merchant's inventory control system and ancillary financial services are hosted on a computer system. This infrastructure is supported by in-store client servers which allow the merchants to store more exception cards (fraud cards, collections-statussed cards, etc). These host merchants generally connect directly to the bank via dedicated telecommunications (leased lines). It is through this infrastructure and the burgeoning nature of credit card fraud at these establishments that Retail Decisions have offered to host an industry negative card file. The large banks in South Africa subscribe to this service which is aimed at reducing post-statussed fraud and bad debt. The post-status nature of these exception credit cards mean that transactions still take place below the merchant's designated floor limit after the card is statussed by the issuing bank (as the issuing bank does not "see" the transactions until they have received the settlement tapes from the acquiring bank). In order to mitigate these losses (post-statussed exception cards), the local issuing banks send their exception cards to Retail Decisions on a predetermined schedule, who in turn host the service or send the information to the large retail stores (which have the hardware and software infrastructure to accept larger volumes of these cards). Transactions concluded below the merchant's floor limit is referenced against this file and if the card is listed on the requisite file, the transaction is declined or the merchant is prompted to call the issuing bank.

Retail Decisions have confirmed that in January 2007, the total fraud frustrated as a result of this service totaled 3.35M. This is illustrated in the table below:

Table 1: Retail Decisions frustrated fraud per issuing bank in January 2007:

Card Clear Service: Declines by Issuer January 2007									
	Lost/ Stolen/ Fraud	%	Refer to Bank	%	Delinquent	%	Total	Total Fraud	Fraud %
ABSA	R 493,102.46	22.57%	R 28,238.60	1.29%	R 1,663,285.60	76.14%	R 2,184,626.66	R 521,341.06	23.86%
SBSA	R 489,318.61	52.89%	R 434,335.62	46.95%	R 1,467.00	0.16%	R 925,121.23	R 923,654.23	99.84%
Nedcor	R 148,116.57	23.86%	R 0.00	0.00%	R 472,696.48	76.14%	R 620,813.05	R 148,116.57	23.86%
FNB	R 939,471.95	63.69%	R 535,642.89	36.31%	R 0.00	0.00%	R 1,475,114.84	R 1,475,114.84	100.00%
FNB Debit	R 40,097.57	63.40%	R 0.00	0.00%	R 23,151.36	36.60%	R 63,248.93	R 40,097.57	63.40%
Amex	R 132,220.92	57.91%	R 0.00	0.00%	R 96,110.53	42.09%	R 228,331.45	R 132,220.92	57.91%
Diners	R 1,224.75	2.72%	R 42,833.82	94.96%	R 1,048.06	2.32%	R 45,106.63	R 44,058.57	97.68%
Investec	R 58,256.61	61.85%	R 15,848.73	16.83%	R 20,088.55	21.33%	R 94,193.89	R 74,105.34	78.67%
Total Reported	R 2,301,809.44	40.84%	R 1,056,899.66	18.75%	R 2,277,847.58	40.41%	R 5,636,556.68	R 3,358,709.10	59.59%
Total Estimate	**R 3,107,442.74**	**40.84%**	**R 1,426,814.54**	**18.75%**	**R 3,075,094.23**	**40.41%**	**R 7,609,351.52**	**R 4,534,257.29**	**59.59%**

Source: Retail Decisions 2007

Table 2: Retail Decisions service 2006

	December 2006			Year-to-date 2006		
	Actual	Budget	Variance	Actual	Budget	Variance
Nº Merchants				23 (131)	23	0
Nº Declines	30,653	10,000	20,653	242,479	120,000	122,479
Estimated Value of Declines	R7,112,466	R2,500,000	R55,710,352	**R30,000,000**	R25,710,352	
% Fraud	67.15%	60%	7.15%	76.01%	60%	16.01%

Source: Retail Decisions 2007

From *table 2*, the estimated value of declines at subscribed merchants totaled R30M (year-to-date 2006) which bears testament to the value provided by this service to the South African card market and lends further credence to the floor limit problem. As can be seen from *table 2* above, only 131 merchants subscribe to this service, yet R30M estimated credit losses and fraud was curtailed at these establishments in 2006.

1.2.3 Charge-backs

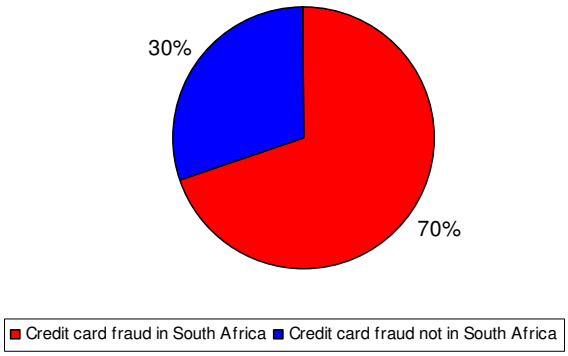
As mentioned previously, acquirers engage in commercial agreements with merchants. For a negotiated fee, acquirers process the merchant's transactions and arrange for the

merchant to be financially reimbursed for the sales concluded on credit cards and recover this money from issuing banks whose cardholders transacted at the respective merchant. As part of the commercial agreement between the acquiring bank and the merchant, (and in accordance with predefined franchise rules governed by the Associations, namely, MasterCard International, Visa, American Express or Diners Club International), it is prescribed that should the merchant transgress their commercial agreement with the acquirer, it may incur the financial loss attributed to the disputed sale. Issuing banks also have financial recourse to the acquiring bank in cases where the merchant did not follow prescribed Association rules. This financial recourse to the acquirer or merchant is termed a “charge-back”. An example of an Association rule regarding the acceptance of the credit card is that a merchant must not process a sale if the card is listed on a “hot” card file or in the event that the transaction is referred to the issuing bank for authorization and the issuer responds that the card is “hot”. Should the merchant then process the transaction regardless of the exception status of the card, it will be liable for a charge-back by the acquiring bank and/or the issuing bank. Merchants are required to follow prescribed procedures to avert charge-backs. The complexity of cardholder and card authentication, coupled to the differentiated nature of the card products (branding, credit, debit, pre-paid, loyalty cards, etc), make it very risky for merchants to accept credit cards. The issuing bank has the responsibility to ensure that its product has sufficient inherent risk controls in order to mitigate fraudulent use. This is sadly not the case as the current cardholder authentication is signature which is too subjective to avoid fraud risk. The security features contained on the aesthetics of the card and that which are personalized to the magnetic strip are insufficient to mitigate fraud risk. Undue onus is placed on merchants to police the issuer’s and acquirer’s risk.

1.3 Fraud Statistics

Credit card fraud has increased alarmingly on South African bank-issued credit cards. The total fraud in 2006 which is the respective representative sample of this research totaled R257M over this period (Source: SABRIC, 2006). The researcher has further differentiated between credit card fraud perpetrated within South Africa and compared this to fraud perpetrated abroad on South African bank-issued credit cards. The following pie chart reflects this differentiation:

Figure 9: South African-issued credit card fraud (domestic and international)

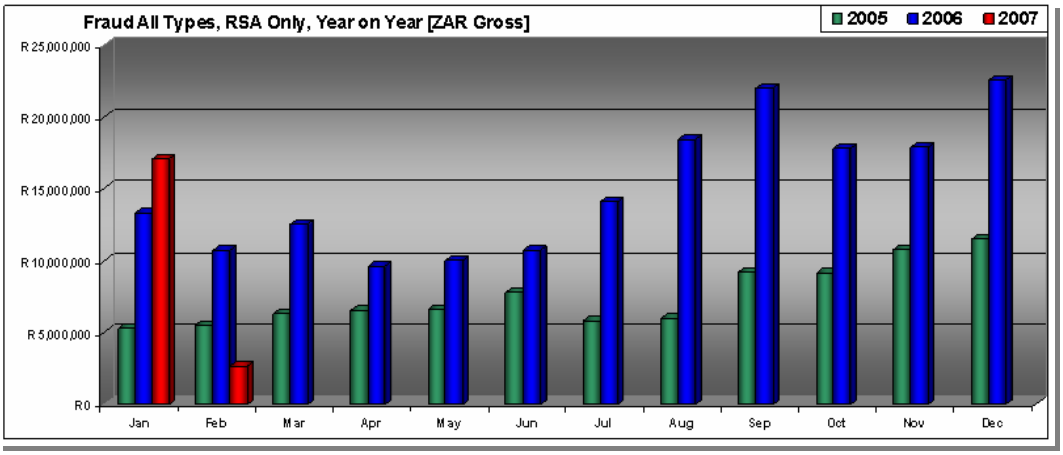


Credit card fraud in South Africa	R 179,341,309.06
Credit card fraud on S.A bank-issued cards abroad	R 77,536,387.60

The pie chart illustrates that 70% of the South African bank-issued credit card fraud was perpetrated in South Africa. The large retail infrastructure in South Africa coupled to the fact that floor limits are in use and the product is magnetic stripe technology with signature as a cardholder authentication mechanism makes South Africa a lucrative country for fraudsters to apply their trade.

Credit card fraud in South Africa had increased at a burgeoning rate in 2006. *Figure 10* illustrates this growth year-on-year since 2005. This data was extracted on 20 February 2007 and illustrates a substantial growth in credit card fraud between 2005 and 2006. This worrisome trend is expected to continue in 2007. (Source: SABRIC, 2006).

Figure 10: South African credit card fraud year-on-year growth (in R's)



A Geographical analysis of the credit card fraud perpetrated within South Africa is illustrated in *figure 11*. The majority of fraud as a transaction amount is perpetrated in Gauteng with Kwa-Zulu Natal and the Western Cape being the second and third largest concentrations of credit card fraud. The economic prosperity and relative size of the retail goods and services sectors of these metropolitan areas lends itself to the volume of credit card fraud perpetrated here. *Table 1* comprises the top 10 high risk towns/cities in terms of fraud volume in Rand in 2006 which gives further insight to the fraud perpetrated in large metropolitan areas. (Source: SABRIC, 2006).

Table 3: Top 10 high risk towns as a fraud amount for 2006

City	Fraud Sum	City	Fraud Sum
JOHANNESBURG	R 28,239,690.56	RANDBURG	R 5,321,512.76
PRETORIA	R 11,979,679.19	ROODEPOORT	R 5,078,364.66
SANDTON	R 11,234,818.99	BOKSBURG	R 3,516,826.07
DURBAN	R 10,780,031.78	KEMPTON PARK	R 3,268,735.36
CAPE TOWN	R 8,097,703.04	CENTURION	R 2,531,799.77

Source: SABRIC 2007

If one had to consider incrementally reducing floor limits, the cities and towns mentioned above would be the best place to start.

Figure 11: A geographical representation of credit card fraud in South Africa.

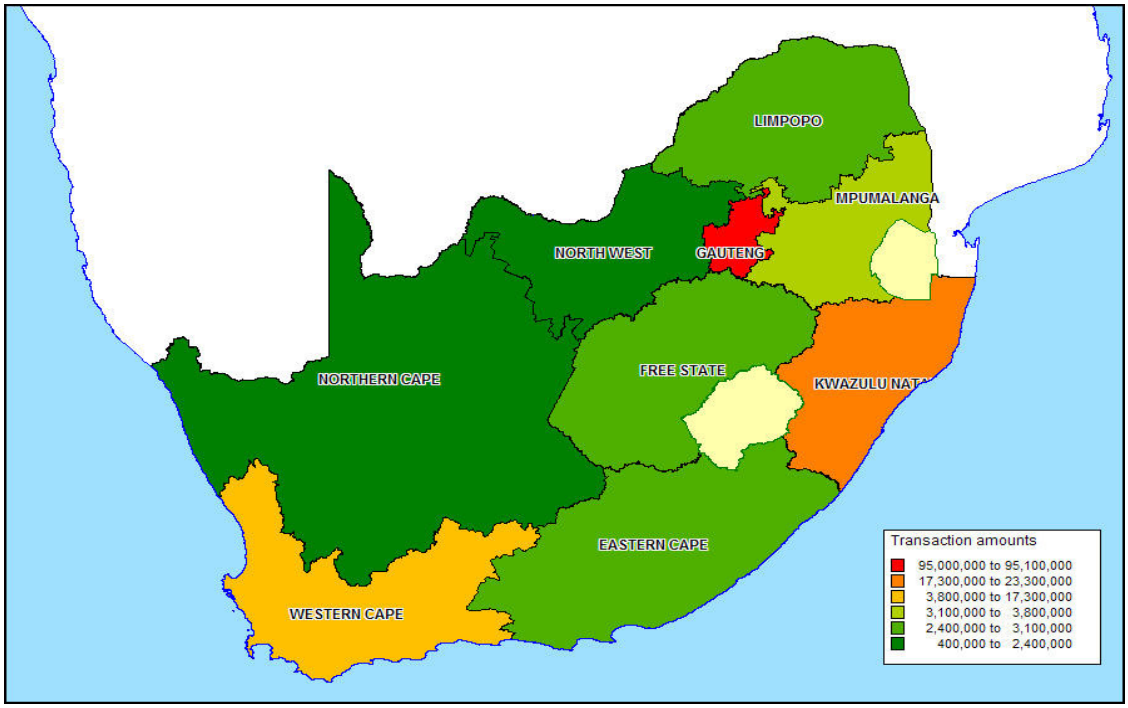


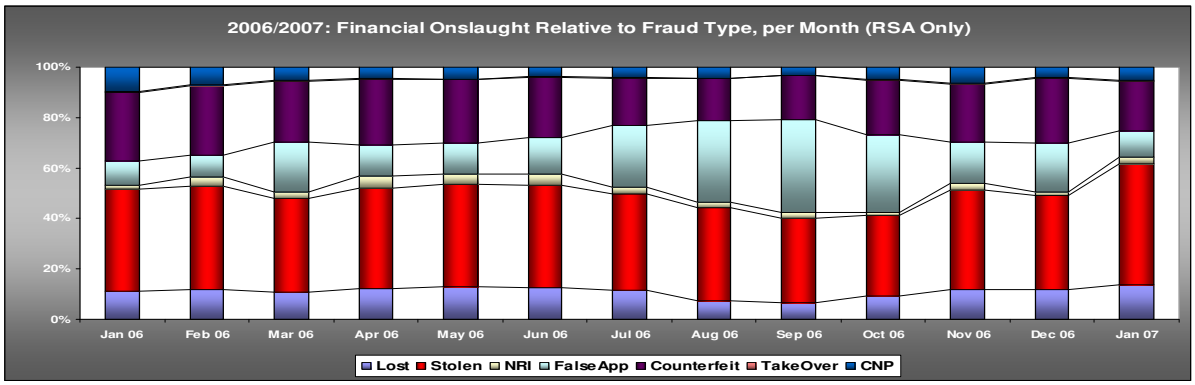
Table 4: Credit card fraud in South Africa per top 10 merchant category in 2006

Description	Total
Grocery Stores and Supermarkets	R 17,749,223.63
Department Stores	R 13,550,846.39
Service Stations	R 13,450,314.50
Family Clothing	R 8,215,591.31
Men's and Boy's Clothing and Accessories Stores	R 5,761,266.15
Package Stores Beer, Wine, and Liquor	R 5,748,439.43
Eating Places and Restaurants	R 4,936,593.36
Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks	R 4,756,085.21
Financial Institutions (Manual Cash Disbursements)	R 4,447,530.63
Financial Institutions (Automated Cash Disbursements)	R 4,133,097.30
TOTAL	**R 82,748,987.91**

Source: SABRIC 2007

Table 4 categorizes the credit card fraud per the top 10 merchant categories in 2006. These merchant categories may move up or down the fraud-risk hierarchy from time to time but generally predominate year-on-year.

Figure 12: Credit card fraud in South Africa by fraud type



Source: SABRIC 2007

Figure 12 illustrates the different types of fraud perpetrated with credit cards in South Africa over the period January 2006 to January 2007 as a rand value per fraud type (Source: SABRIC, 2006). This analysis is pertinent as certain fraud type *modus operandi* is perpetrated below merchant's assigned floor limits. The fraud categories are a broader classification based on the following factors:

(a) How the card plastic, cardholder authentication (Personal Identification Number) and/or card data was obtained,
(b) The method used by the miscreants to perpetrate the fraud via the various financial channels (point-of-sale, internet, automated teller machines (ATM), mail order, telephone order, cash disbursement within the banks points of representation (branches))

Certain transactional channels enjoy floor limits whereas others have a compulsory zero floor limit as mandated by Visa, MasterCard or the local banking industry rules (governed by the local banking industry). The transactional channels which do not have an assigned floor limit (i.e. zero floor limits) are those where:

(a) The card and/or cardholder are not present at the time of the transaction. These transactions are deemed "card-not-present" or "non face-to-face" transactions. The respective channels where these transactions originate are:
    i. Internet purchases
    ii. Mail order transactions
    iii. Telephone order transactions
(b) Transactions which involve cash disbursements, namely:
    i. Cash disbursed via automated teller machines
    ii. Cash disbursed "over the counter" within financial points of representation (branches)

Floor limits are assigned to "face-to-face" transaction channels (where the card and cardholder are present). This excludes transactions which involve cash disbursements as mentioned above. The traditional "face-to-face" channels are points of sale.

Floor limits are generally assigned to merchant categories (with points of sale) based on the nature of the product they sell (the average ticket values of the goods or service) and the risk propensity of the business. The issuing bank determines the floor limit based on the merchant category and the current industry standards as governed by the local Association of Bank Card Issuers in South Africa (Source: MasterCard). The issuing bank funds the risk on the product they issue. The risk-funding is inherent within the interchange that the acquirer pays the issuing bank for every sale (detailed later in this

document). Interchange is generally set to 1.71% of the sale. There are two main categories of risk in this funding, namely credit risk and fraud risk. Fraud risk funding in the interchange (1.71%) is roughly 0.12%.

The following analysis was done on credit card fraud perpetrated in South Africa from a banking industry perspective. The information was extracted and collated from Nedbank, First National Bank, Standard Bank, ABSA, Investec and Mercantile Bank (Source SABRIC 2007). The first bar chart represents fraud as a transaction cumulative amount within transactional value bands. Lost and stolen fraud comprises the majority of fraud as a cumulative total. Most of the lost and stolen fraud is transactions which are perpetrated below the merchant's designated floor limit. Merchant floor limits are assigned on the basis of the nature of the merchant and their respective merchandise or service. The issuing bank also determines the floor limit with regard to the nature of the product. Credit card products that are at the lower end of the market segment enjoy a generic floor limit of between R200.00 to R300.00 which is in line with the merchant's assigned floor limit. Products at the higher end of the market segment (i.e. Gold and Platinum cards) have a floor limit which is double that of the conventional products. This implies a floor limit of between R400.00 and R600.00 (Source SACFF, 2007).

Figure 13: Fraud types per Rand value band over December 2006 to February 2007:

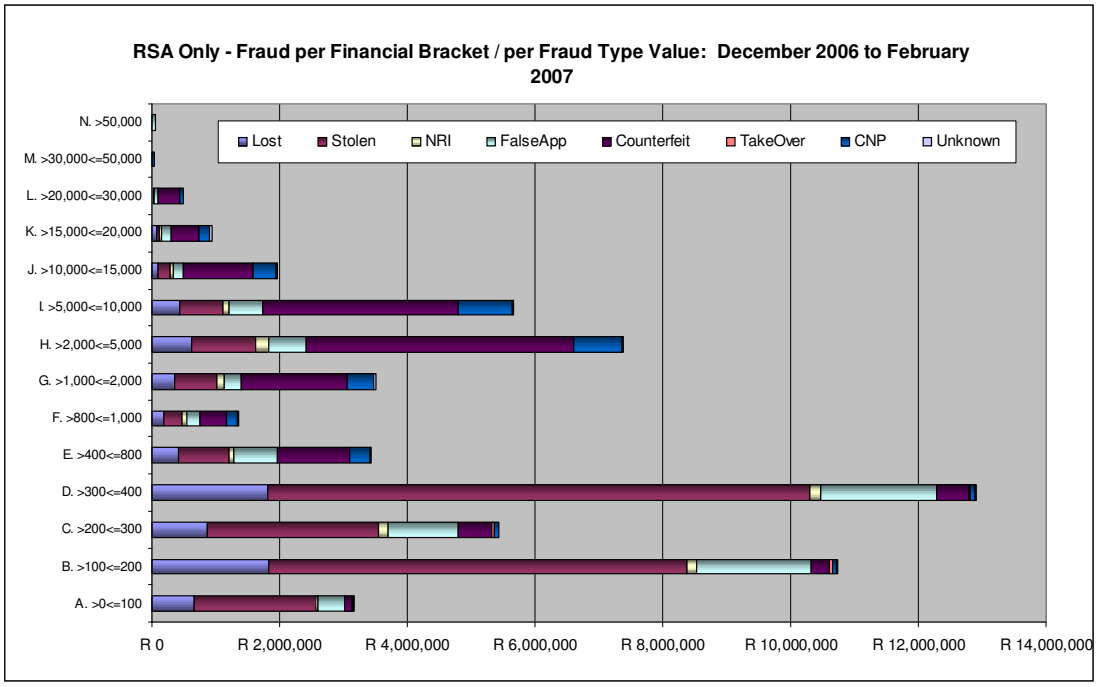


Figure 13 illustrates that most of the fraud as a cumulative total is within these mentioned floor limits on lost, stolen and false application fraud. The X-axis represents the cumulative amount of fraud as a Ran value and the Y-axis represents the transaction amounts within predefined value bands.

Figure 14: Fraud types as a count of transactions per value band over December 2006 to February 2007:

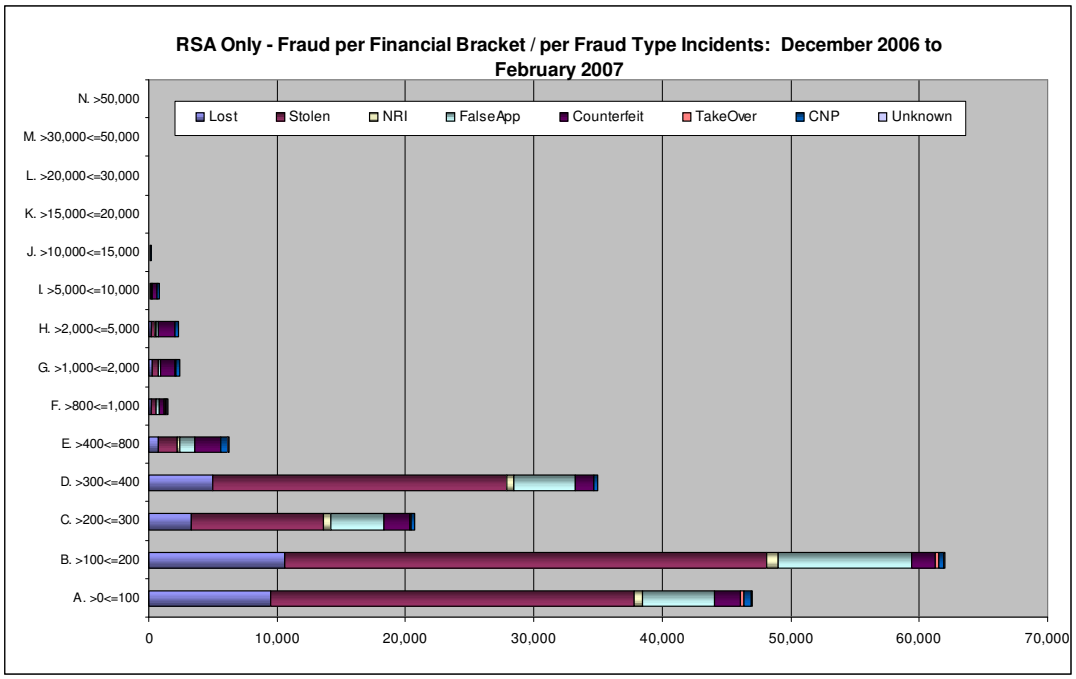
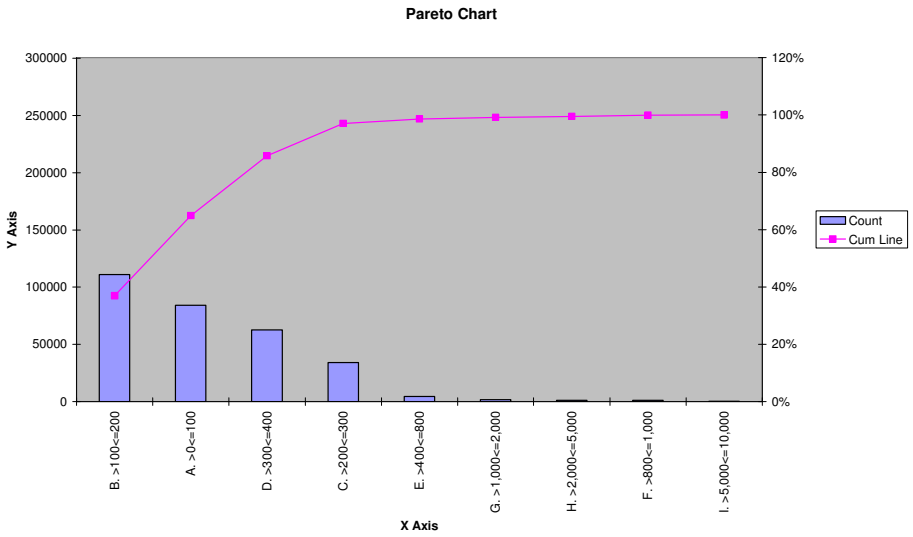


Figure 14 illustrates that the number of fraud incidents within the selfsame value bands also concentrates within the R200.00 to R600.00 category. The X-axis represents the cumulative number of fraud transactions and the Y-axis represents the transaction amounts within predefined value bands. This lends further weight to the argument that most fraud is perpetrated below the merchant's designated floor limit.

The following Pareto chart was constructed by taking "stolen" fraud over this period and categorising the transaction counts within the value bands:

Figure 15: Pareto chart on “stolen” fraud over the period December 2006 to February 2007



The Pareto chart above shows that most stolen fraud is perpetrated below the merchant’s floor limit.

1.4 Benefits of the Study

Credit card fraud perpetrated below merchant’s designated floor limits within South Africa has been increasing alarmingly over the last two years. In 2006, card fraud perpetrated in South Africa alone exceeded R179M (Source: SABRIC, 2006) of which a substantial portion was attributed to below floor limit spending by miscreants. Discussion and collaboration with local bank credit card issuers at industry forums has identified the need to move to a zero-floor limit environment. The main quoted stumbling blocks to achieve this objective are the following:

- The inability of the local telecommunications infrastructure to sustain a zero floor limit due to the envisaged increase in authorization traffic,
- The inability of the issuing bank to process the anticipated volume of authorizations which would be the case in a zero-floor limit environment,
- The potential negative impact to cardholders due to longer queues and delays at the point-of-sale,
- The high operational costs that merchants will incur as telephony is an overhead that they pay for in fulfilling an authorization request.

The benefits of this study will be in the research to obtain the relevant facts to entertain a viable business case to move to a zero floor limit credit card infrastructure. This in turn should reduce recurrent fraud losses on credit card products and enable issuing banks to detect questionable cardholder behaviour earlier as they will now “see” all the transactions. The quoted stumbling blocks and Propositions will also be tested via a survey to choice industry participants

1.5 Problem Statement

South African-issued credit cards are fraudulently used mostly below the merchants floor limit in South Africa. This operating model perpetuates the fraud life cycle as the issuing bank only sees this transaction after an average of 2 days once the settlement process has occurred (this applies to cases where the issuing bank and the acquiring bank are not the same institution). As a result of this operating model, “hot” card files are stored on the merchant’s point-of-sale which place the issuing bank’s cards at the merchant location. Size constraints of these files and the delay of loading these exception cards further perpetuate the fraud life cycle.

The problem statement is that floor limits assigned to merchants in South Africa for credit card products issued by South African banks continues the fraud life cycle as the point-of-sale channel cannot be effectively closed for credit card use.

1.6 Objectives of the Study

The objective of this study is to analyse the effects that merchant floor limits have on bank-issued credit card fraud in the South African credit card industry and compare this to the ability of telecommunications to sustain a zero-floor limit environment. The objectives include the telecommunications capacity-handling from the point-of-sale to the issuing bank as well as the issuing bank’s capability to process the transactions emanating from a zero floor limit. In fulfilling these objectives, the researcher will be able to propose a case for reducing or zeroing floor limits with an end in view of lessening credit card fraud perpetrated below the merchant’s floor limit. The researcher also acknowledges and supposes that fraud will migrate to other channels.

1.7 Sub Problems

Sub-problem 1: The first sub-problem is to analyze the effect of merchant floor limits in South Africa with their impact on bank-issued credit card fraud.

Sub-problem 2: The second sub-problem is to determine the ability of current telecommunications technology to sustain a zero floor limit environment.

Sub-problem 3: The third sub-problem is to determine the costs associated with current telecommunications technology in sustaining a zero floor limit environment.

Sub-problem 4: The fourth sub-problem is to analyze and interpret the data so as to evaluate the feasibility of introducing zero floor limits in South Africa considering telecommunications technology and costs.

1.8 The Propositions

Proposition 1: The first Proposition is that merchant floor limits in South Africa have an adverse impact on bank-issued credit card fraud.

Proposition 2: The second Proposition is that South African telecommunications can sustain a zero floor limit.

Proposition 3: The third Proposition is that the cost of introducing a zero floor limit in South Africa is negligible in relation to the fraud which floor limits sustain.

Proposition 4: The fourth Proposition is that local banks infrastructure and technology can accommodate an increase in authorisations as a result of a zero floor limit environment.

1.7 The Delimitations

The study will not include credit cards issued by retailers. In-store cards are not part of the *multiple card issuer model* proposed on *page 4*. These proprietary cards generally assume a zero floor limit at store level and can be readily blocked by the retailer to prevent further use.

The study will not include debit cards issued by local banks or retailers. Debit cards which enjoy PIN as a cardholder authentication imply a zero floor limit as the issuer will authenticate the PIN at host (issuer) level. Should the PIN not be authenticated by the card issuer, the transaction will be declined. In the event that the merchant processes the transaction in spite of the decline response by the issuer, it stands the risk of charge backs or being terminated by the acquiring bank if this trend persists.

The study will be limited to bank-issued credit cards in South Africa. As mentioned and illustrated, foreign-issued cards used in South Africa naturally assume a zero floor limit. This case also holds for South African-issued credit cards used abroad.

The study will be limited to the current telecommunications which point-of-sale devices use in sending transactions for authorisation. This includes telephone, radio pad and GPRS technology. The merchants who deploy this type of technology and enjoy floor limits comprise the majority of the fraud. The exceptions to this rule are those merchants which have integrated point-of-sale software where post-statussed fraud can be contained and prevented by using the industry negative card file.

The study will be limited to those point-of-sale devices that have a pre-programmed floor limit (card present, “face-to-face” environment). All card-not-present, non face-to-face transactions have a zero floor limit.

This study will not intricately delve into the explicit costs of telecommunications as there are multiple service providers and vendors with various product differentiations, value propositions and associated rates.

This study will not include credit losses originating from arrears and delinquent accounts (bad debts). The analysis pertaining to the fraud losses equally applies to bad debt

losses; however, the banks have recourse to the cardholders via sequestration, liquidation or other legal remedies. To include this aspect as part of the research report will be too time-consuming and complex.

The fraud funding the credit card interchange in relation to the fraud losses experienced is not discussed in this research report due to the competitive nature of the calculations and the complexity of the various interchange rates and fees per product type.

1.8 Assumptions of the Study

The first assumption is that floor limits will continue within the South African credit card market. Albeit that chip cards will be introduced over a period of 2 to 3 years in the South African market, floor limits will still be entertained in the South African industry. The chip cards will allow for off-line PIN (PIN authentication where the chip validates the PIN at point-of-sale), and the fraud risk is expected to reduce, however, proprietary cards issued by the banks (which fall out of scope for the chip roll-out) will still be a risk.

The second assumption is that the telecommunications infrastructure in South Africa is contemporary with that which exists in most developed markets. South Africa's cellular market is the fourth fastest growing market in the world (Economic Profile of South Africa (2005)).

The third assumption is that credit card transactions conducted below the merchant's floor limit follows the same distribution as those conducted above the merchant's floor limit. This assumption is based on the purchasing habits of credit card holders and their purchasing times within a representative week. This assumption is construed to be reasonable as below and above floor limit spend is correlated to spending peaks and troughs within conventional spending hours.

The fourth assumption is that the South African Banks that issue credit cards will have a transactional distribution which is the same as Standard Bank's. This assumption is related to the one above in that competitor credit cards are issued to the same market segments as those of Standard Bank. The spending habits of these customers will be

largely synonymous with Standard Bank's cardholders as the merchant base and spending patterns (from a time or hours within a day perspective) is the same.

CHAPTER 2

2. Foundation of the study

2.1 Introduction

In collaboration with fraud risk managers from various local banks, the rationale for not adopting zero floor limits is varied and the following Propositions have emerged:

- The telecommunications network cannot support the authorizations volumes anticipated as a result of zero floor limits. This includes the questionable ability of local issuing banks that process the authorization requests that would originate in a zero floor limit environment.
- The fraud school of thought where fraud risk managers aim to reduce or zero select floor limits at certain merchant categories where fraud is prevalent and sales are not voluminous to risk technical problems associated with a supposed zero floor limit environment.
- The operations school of thought from an acquiring perspective which questions the merchant's operational costs associated with entertaining a zero floor limit and the ownership of the merchant's selected telecommunication network.

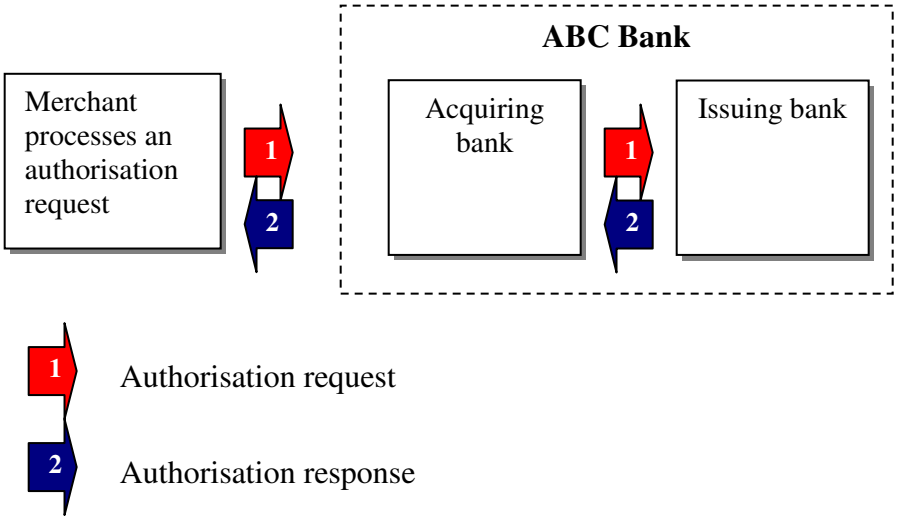
These various views are not necessarily secular or individual to one group of theorists who may share all the views or discount some of them. The intention of the researcher (after collaborating with industry stakeholders in South Africa) is to position the various views and analyze the merits of each case and combine them to determine the limitation landscape of adopting zero floor limits. A survey will be used to determine the merits of these postulated views.

2.2 The technology school of thought

There are some industry business participants that question the ability of the current telecommunications infrastructure (which facilitates data transmission to issuing banks) to support zero floor limits. The researcher aims to collect data on authorization volumes (and their anticipated increase) which would be expected due to a zero floor limit and the

anticipated increase in transactions per second which is a key metric to ascertain whether issuers' front-end processors can handle the anticipated increase in transaction volumes. The analysis will be extended to all system intermediaries in the authorization data flow (which will include data switches). The figures below illustrate the system participants from a macro perspective:

Figure 16: Authorization requests where the issuing and acquiring bank are synonymous



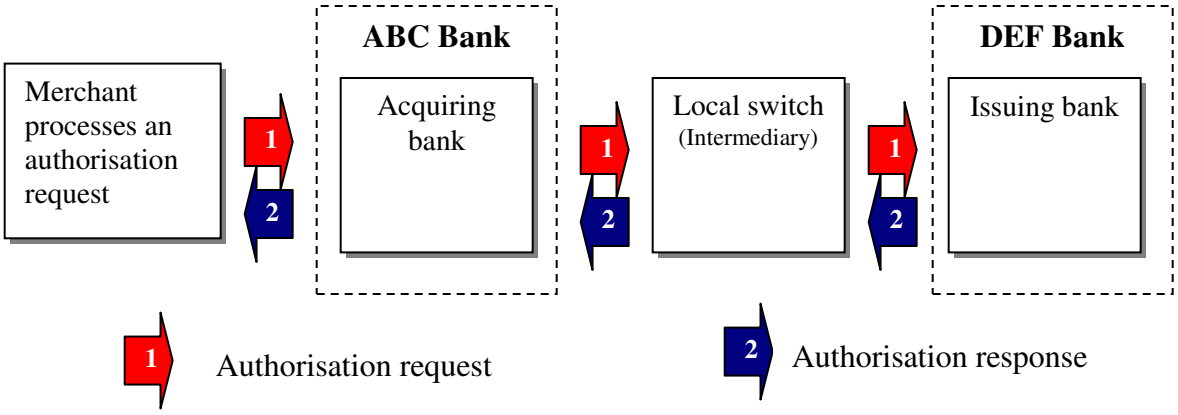
Step 1: The merchant processes a sale in excess of the assigned floor limit which will route the authorisation request to the acquiring bank.

Step 2: The authorization request gets routed from the acquiring bank (via a front-end processor) to the issuing bank (which are the same institution).

Step 3: The issuing bank acknowledges the authorization request, processes it and sends the authorization response back via the channels it originated from.

The example above shows the authorization request and response routes for domestic credit card transactions. The illustration above pertains to authorization requests and responses where the issuing and acquiring bank are the same institution.

Figure 17: Authorization requests where the issuing and acquiring bank are not synonymous



Step 1: The merchant processes a sale in excess of the assigned floor limit which will route the authorisation request to the acquiring bank.

Step 2: The authorization request goes to the acquiring bank which routes it to a local switch.

Step 3: The local switch routes the authorization to the issuing bank.

Step 4: The issuing bank acknowledges the authorization request, processes it and sends the authorization response via the channels it came in on.

The example above shows the authorization request and response routes for domestic credit card transactions. The illustration above pertains to authorization requests and responses where the issuing and acquiring bank are not the same institution. In these instances a domestic switch is used to transport the transaction between the acquiring and issuing bank. The domestic switch in the South African credit card industry is Bankserv.

The researcher aims to identify whether the current point-of-sale technology (microwave (radio pad), GPRS and telephone lines) have the capability to send more transactions online to the issuing bank without degrading service delivery from a merchant and cardholder's perspective

2.3 The fraud school of thought

The fraud school of thought centers on the fraud functions within the various divisions in the respective banks. These theorists maintain that a zero floor limit will curtail credit card fraud losses within their respective organizations. The losses on lost, stolen and not received instances are expected to be reduced dramatically. The impact of zero floor limits on these types of fraud will be analyzed by the researcher by taking below floor limit fraud for 2006 as a representative sample and comparing this with a "what-if" analysis had zero floor limits been introduced over the same period. The Proposition that fraud losses on credit cards will reduce substantially is questionable due to the potential migration to other fraud types by miscreants – i.e. counterfeit fraud, card not present fraud (the miscreants generally use the internet) and false application fraud. It is anticipated that fraud efforts will escalate on these fraud types which will necessitate further controls on the part of the issuer. The fraud may be easier to identify as the issuer will now see all the transactions as they are occurring (whilst the customer is at the point-of-sale) as opposed to transactions conducted below the merchant's floor limit as discussed under the topic of settlement delay. The fraud types mentioned above are briefly described hereunder:

Lost Fraud: The cardholder reports that the card had been lost. The loss of the card has resulted in fraud on the account.

Stolen Fraud: The cardholder reports their card was physically removed from their person or that they are aware of the person(s) that took the card. The fraud then took place as a result of the card being stolen.

CNP (Card not present) Fraud: The card number, expiry date and unique card values are compromised and used in a non-"face-to-face", or card-not-present channel**.** These channels are traditionally the internet, mail order or telephone order.

NRI (Not Received Instances) Fraud: A card dispatched to a cardholder is intercepted before receipt and subsequently used fraudulently.

Counterfeit Fraud: Fraud perpetrated on a card where it "is an instrument or device embossed, printed, or otherwise bearing MasterCard (or branding marks) marks, so as to purport to be a MasterCard (or proprietary or other Association) card issued by a

member or affiliate; but that is not a MasterCard (or proprietary or other Association) card because the embossing or printing thereon was not authorised, or because the MasterCard (or proprietary or other Association) card has been altered or re-fabricated, even though it was issued initially.

False App (False Application) Fraud: A credit card application is made to an Issuer containing misleading or false information which is intended to induce a positive decision to grant a payment card facility.

2.4 The operational school of thought

The operations school of thought is related to the acquirers and their rationale for not adopting a zero floor limit. These entities argue that a zero floor limit will increase the merchant's operational costs. Merchants generally decide on the network and communication technology they will adopt (GPRS, radio pad, telephone line). Acquirers who engage in a commercial agreement with merchants give guidelines and advice on the data communication methods. As the merchant pays for these overheads and subscribes to a communications service provider, they ultimately decide on the data transmission mechanism. The respective decisions are generally based on the following criteria:

- The cost of the subscription (a fixed cost)
- The cost of sending transactions for authorization (in some instances this is a variable cost)
- The speed and efficiency of the communication method and scalability
- The geographical coverage and reliability of the service

The acquirer currently pays the issuing bank an interchange fee as part of the economic business model. The fee that the acquirer pays the issuer in the South African credit card market is 1.71% of every sale. The interchange process is holistically explained in chapter 1 using *figure 2* as a contextual model. According to Akers et al (2005) interchange fees are a source of irritation to merchants and can be among the largest and largest-growing costs of doing business for many retailers. The interchange fee (regulated by the Associations and South African credit card industry) is a surcharge on every sale. This fee allows the issuing bank to:

- Cover its cost of funds to fund the credit from the Reserve Bank
- Cover fraud and bad-debt costs
- Cover operational costs in supporting the credit transactions (Authorizations, Lost Cards, etc)

Acquirers in turn, charge a commission to the merchant (for processing the sales) which covers the interchange fee that they have to pay to the issuing bank. According to Wikipedia, (http://en.wikipedia.org), "the interchange fee that applies to a particular merchant is a function of many variables including the type of merchant, the merchant's average ticket amount, whether the cards are physically present, if the card's magnetic stripe is read or if the transaction is hand-keyed, the specific type of card, when the transaction is settled, the authorised transaction amounts, etc".

Acquirers argue that the interchange fee has an inherent fraud loss funding mechanism and that by reducing or zeroing floor limits, the merchant is prejudiced in that their operational costs will increase (due to the additional authorization traffic which will increase the communication costs) whilst the fraud funding in the interchange model remains the same. They argue that the merchant would need to be compensated in the form of a reduced interchange (which the acquirer recovers from the merchant and pays the issuing bank) to cater for the increased operational costs. Akers et al (2005) state that credit card transactions have higher interchange rates than signature debit card transactions, whose rates are higher than PIN debit card transactions. The rationale for this is to compensate for the higher levels of fraud risk associated with credit cards. Akers et al (2005) further confirm that merchants view interchange fees as an unnecessary and growing cost over which they have no control. Banks are issuing credit cards with higher interchange fees and in line with Association regulations; the merchants are unable to refuse transactions conducted with these cards. Merchants thus view issuing banks as earning revenue at their expense.

2.5 The technology paradox

MasterCard International has mandated that all international transactions be subject to a zero floor limit (MasterCard International Incorporated, 2005 *Global Operations Bulletin* No. 12 (59-75)). In the event that a cardholder, with a foreign issuing bank's product,

uses the product in South Africa, it must be subject to a zero floor limit. The same principle applies when a South African-issued credit cardholder uses their card abroad. This mandate applies to “face-to-face” transactions and there are no exemptions to this rule. This operating regulation has been adopted in the South African credit card market for some time. This card usage is substantial in the South African credit card market and is paradoxical to the technological school of thought. In line with this argument, the local banks in South Africa are adopting chip and PIN which through the nature of technology may induce more authorization traffic.

CHAPTER 3

3. Literature Review

3.1 Introduction

The literature review will include three areas: (a) Empirical studies relating to merchant floor limits and its effect on credit card fraud in South Africa, (b) telecommunications technology in South Africa and its ability to sustain a zero floor limit and (c) the costs and efficiency of telecommunications technology within South Africa. The present review is limited to credit card fraud below merchant floor limits in South Africa.

3.2 Empirical Studies relating to merchant floor limits

Anonymous (1993:3 (*Proquest*)) quotes that “Visa USA is softening its policy that every transaction be authorized after a flurry of complaints from merchant acquirers. The VisaNet network will give reports to acquirers showing chargeback risks from unauthorized transactions”

This article is an early barometer of the inadequacies of floor limits within foreign markets. The charge backs to merchants associated with fraud perpetrated at merchant establishments where the card was loaded on the “exception file” was a worrisome concern.

Anonymous (1993:3 (*Proquest*)) further quotes that “The electronic reports will highlight transactions of under $50 at paper-based merchants that would have been flagged had VisaNet's so-called exception file been checked. The purpose is to help acquirers decide if the merchant should get a terminal, use voice authorizations, or take a chance and continue with $50 floor-limit transactions. Visa wants every transaction authorized because the exception file lists vastly more bad cards than the paper bulletin”. The paper warning bulletin was a predecessor to its local counterpart in South Africa, the hot card file. This was a paper hot card file which listed compromised cards and was distributed to merchants by acquirers. The delay in printing and distributing this bulletin, in line with the costs and growth in size constrained its life cycle. The article states further that “The

exception file, updated daily, lists 6 million stolen, expired or otherwise invalid Visa cards that issuers want picked up by the merchant should they be presented for payment, compared to only 489,000 in the paper bulletin. The bulletin costs Visa and MasterCard $20 million a year to produce. The paper bulletin lists only the worst cards because it costs issuers more to list card numbers there than in the electronic file, although figures on how much more were unavailable". Visa's intention to promote zero floor limits was to prompt merchants and acquirers to send the transactions online to the issuing bank for authorization. These transactions would be switched via the VisaNet system wherein the electronic exception file would reside. The exception file would contain compromised cards listed by the issuing bank. The rationale for this incentive was to reduce charge backs acquirers and merchants were receiving from the issuing banks due to cards they had loaded on the warning bulletin and which had not been cross-referenced by the merchant. A hot card file or paper warning bulletin is a direct result of floor limits being assigned to merchants.

Anonymous (1993:3 *(Proquest)*) goes on to state that "Some paper-based merchants still could continue making floor-limit transactions after April 1994. Card issuers will have charge back rights for unauthorized transactions only if a card was listed in the exception file on the transaction date. But the number of unauthorized transactions is likely to plummet, because, with the exception file being so much bigger than the warning bulletin, issuers will be getting much more charge back protection than they have now. Thus, acquirers, to protect themselves from charge backs that wouldn't occur with the warning bulletin, will have a new incentive to encourage authorizations".

In another article by Anonymous (1994:28(*Proquest*)), Visa, MasterCard and Europay had a medium term initiative (period 1993-1996) to roll-out a national "hot card file". Anonymous (1994:28) states that "The introduction of lower floor limits across all merchant sectors is being pursued by APACS' Plastic Card Prevention Forum". APACS is an acronym for the "Association for Payment Clearing Services". Anonymous (1994:28) states further that "Some 5,000 cards are lost or stolen every day; paper lists cannot keep pace, so the electronic transmission to the point of sale - by broadcast technology, where possible, of hot card data makes a good deal of sense. But this requires new terms to be negotiated between acquirers and retailers, which is never the easiest matter. Next, the introduction of lower floor limits across all merchant sectors (and the consequent increase in authorization) is being pursued by APACS' Plastic Card

Prevention Forum. Once again, hard bargaining is involved between acquirers and retailers and between some issuers and acquirers".

In 2005 MasterCard International published the following mandate to all its members (MasterCard International Incorporated, 2005 (*Appendix 5*)) "Effective 8 April 2006, MasterCard will require a card acceptor *(acquirer)* to obtain an authorization from the issuer for:

- All non face-to-face transactions, regardless of the transaction amount,
- All face-to-face transactions, card-read or key-entered, occurring at a location with a point-of-sale (POS) device that has both online and magnetic stripe-read capability, regardless of the transaction amount"

MasterCard along with the card industry introduced this rule in an effort to reduce fraud and credit card losses. This mandate followed the earlier Visa initiative in 1993.

The MasterCard's mandate further stated that "As the industry continues to evolve, it is apparent that the current environment now is receptive to additional online authorizations to address those merchant locations that have online, magnetic stripe-read capable devices".

MasterCard states further that "These changes will have a nominal effect on most merchants, as most acquirers endorse existing practices in many cases and do not require face-to-face merchants to purchase new terminals or to replace existing devices".

MasterCard published that recent analysis done by MasterCard on member's authorization and settlement showed that authorization rates exceed 90% in all regions for face-to-face transactions. This is demonstrated by the following table:

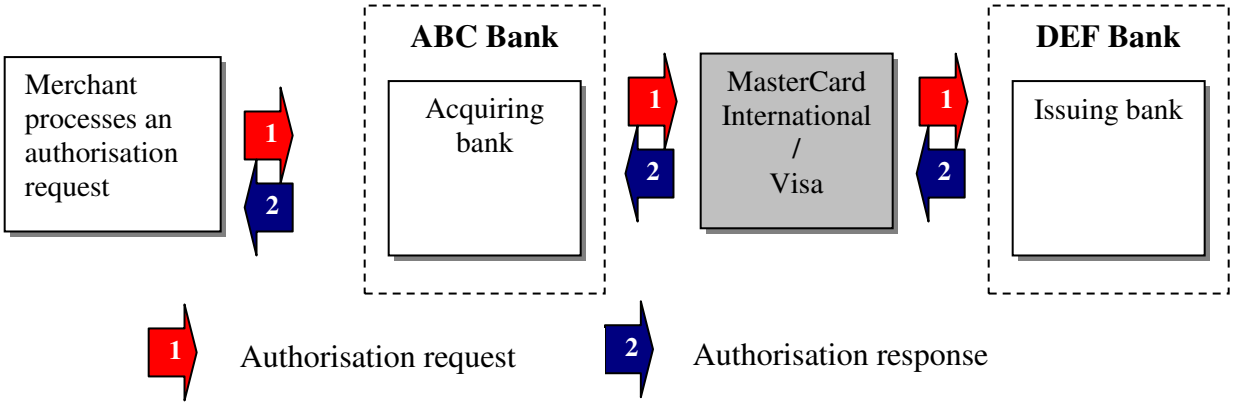
Table 5: The authorization volumes as a percentage that were switched via MasterCard in 2005

Region	Percent of Face-to-Face Transactions Authorized
Asia/Pacific	96.7%
Canada	95.9%
Europe	93.3%
Latin America and the Caribbean	99.6%
South Asia/Middle East/Africa	99.3%
United States	99.6%
Global	98.2%

Source: MasterCard International Incorporated, 2005 *Global Operations Bulletin* No. 12

South Africa falls within the South Asia/Middle East/Africa region (SAMEA). If one looks at the summary statistic of 99.3%, it assumes that no floor limits exist within the South African credit card market. It is prudent to mention that all foreign-issued credit cards have an applied zero floor limit at point-of-sale. This was introduced in the South African credit card industry in the late 1990's. Furthermore, South African-issued credit cards used abroad generally enjoy a zero floor limit in foreign countries. However, not all locally-issued credit cards are switched via MasterCard. The following illustration serves to further define this situation:

Figure 18: South African-issued MasterCard/Visa credit card used internationally



In the illustration above, a South African-issued MasterCard or Visa credit card is used internationally and switched via MasterCard or Visa to the issuing bank in South Africa

for authorization. The clearing and settlement of these transactions by MasterCard or Visa is one of the services that they provide to issuing and acquiring banks. These transactions automatically enjoy a zero floor limit.

Figure 19: South African-issued MasterCard/Visa credit card used locally

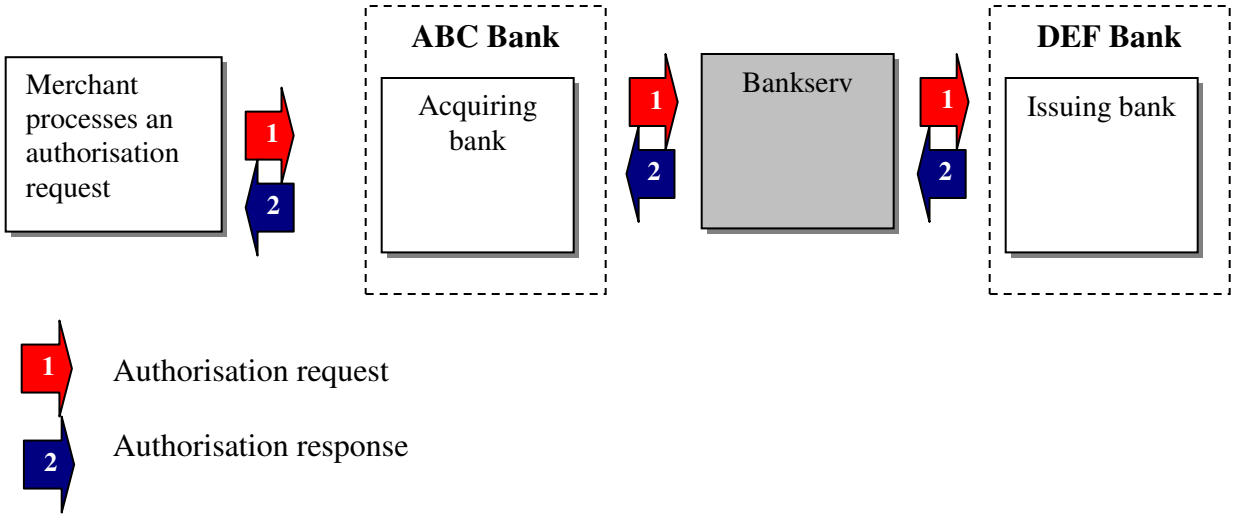


Figure 19 illustrates the transaction routing by the local switch where the issuing and acquiring bank are not synonymous.

In the illustration above, a South African-issued MasterCard or Visa credit card is used domestically and switched via a local switch (Bankserv) to the issuing bank for authorization. These transactions do not enjoy a zero floor limit. The scope of this research report falls within the ambit of this architecture where fraud has been prevalent below the merchant's floor limit. Thus the 93% summary statistic applies to cross-border transactions only. The largest majority of domestic authorizations are switched via Bankserv. The assumption that MasterCard has made in terms of the nominal effect of increased authorizations is the subject of this research.

MasterCard International Incorporated, 2005 *Global Operations Bulletin* No. 12 (62) states "When a card acceptor *(acquirer)* does not authorize transactions in accordance with the online authorization requirements, issuers may process a charge back".

The acquirer has to accede to this mandate as the mandate applies to issuing banks. The following exemption applied as stated in the bulletin "MasterCard will not require an online authorization in the following instances:

Domestic transactions when issuer representing at least 75% of a country's issuing volume reach an agreement. Issuers that represent at least 75% of a country's issuing volume may establish a domestic (such as, intra-country) floor limit for face-to-face transactions at a POS device with both online and magnetic stripe-read capability. Issuers must report this exception to MasterCard Fraud Management staff if adopted.
However, the online authorization requirement will apply to all cross-border transactions". "Cross-Border" transactions pertain to South African credit cards used abroad or foreign cards used domestically.

In line with these requirements the local banks got together (MasterCard and Visa were in attendance) in 2006 at the SACFF (South African Credit Fraud Forum) industry committee. It was resolved that issuers would not adopt zero floor limits until the necessary research had been done to determine the impact of the mandate. A revised list of floor limits was proposed which the participating banks agreed to adopt (*Appendix 1*) once the impact to the customer and the issuing bank (and their ability to process the transactions including the infrastructure) was determined. It was also resolved at the SACFF that the adoption of reduced or zero floor limits would extend to Visa products as well. The rationale for this is that the fraud would be expected to naturally migrate to the Visa products should MasterCard-branded products enjoy a zero floor limit.

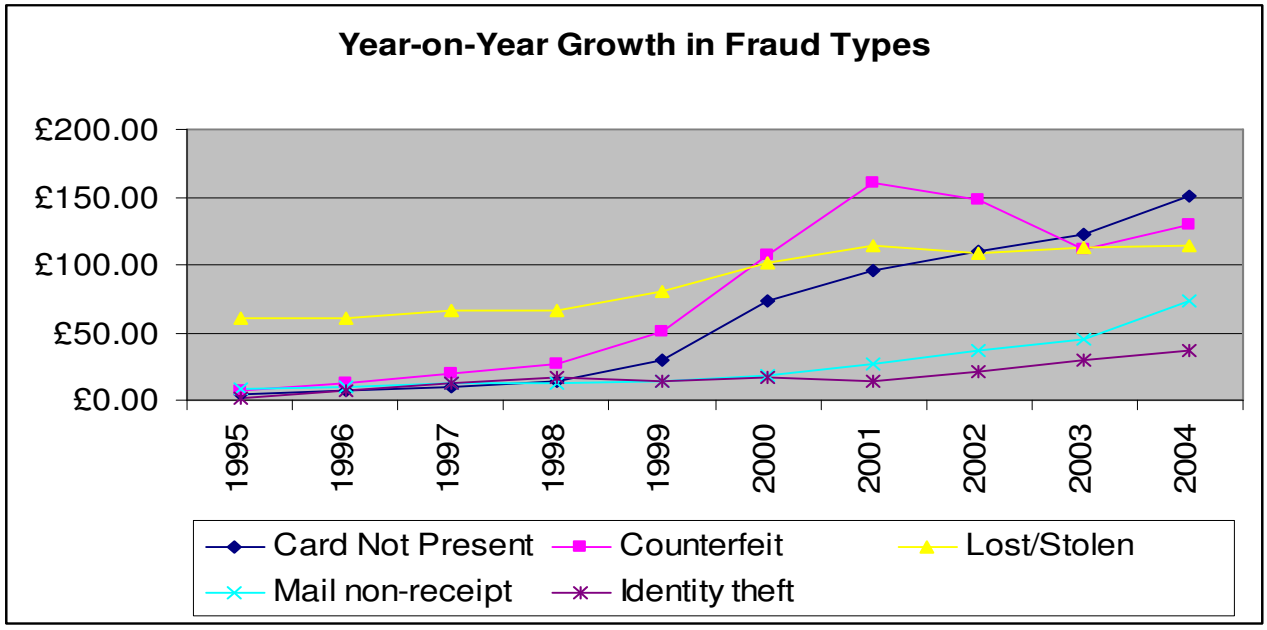
Research on international trends has further typified the floor limit debacle.
According to Card Watch (www.cardwatch.org.uk), fraud on credit and debit cards has a high cost to society as the proceeds are often used to fund serious organized crime such as drug trafficking and terrorism. Fraud on UK-issued cards grew from 97.1 million British Pounds sterling in 1996 to 504.8 million British Pounds sterling in 2004. This equates to a growth rate of 420% over the eight years. Card Watch, in their article on the cost of card fraud; advocate that a means of preventing card fraud is the reduction of merchant floor limits.

Table 6: Fraud by fraud type year-on-year in the UK

	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	**Total**
Card Not Present	£4.60	£6.50	£10.00	£13.60	£29.30	£72.90	£95.70	£110.10	£122.10	£150.80	**£615.60**
Counterfeit	£7.70	£13.30	£20.30	£26.80	£50.30	£107.10	£160.40	£148.50	£110.60	£129.70	**£774.70**
Lost/Stolen	£60.10	£60.00	£66.20	£65.80	£79.70	£101.90	£114.00	£108.30	£112.40	£114.40	**£882.80**
Mail non-receipt	£9.10	£10.00	£12.50	£12.00	£14.60	£17.70	£26.80	£37.10	£45.10	£72.90	**£257.80**
Identity theft	£1.80	£7.20	£13.10	£16.80	£14.40	£17.40	£14.60	£20.60	£30.20	£36.90	**£173.00**
	£83.30	**£97.00**	**£122.10**	**£135.00**	**£188.30**	**£317.00**	**£411.50**	**£424.60**	**£420.40**	**£504.70**	**£2,703.90**

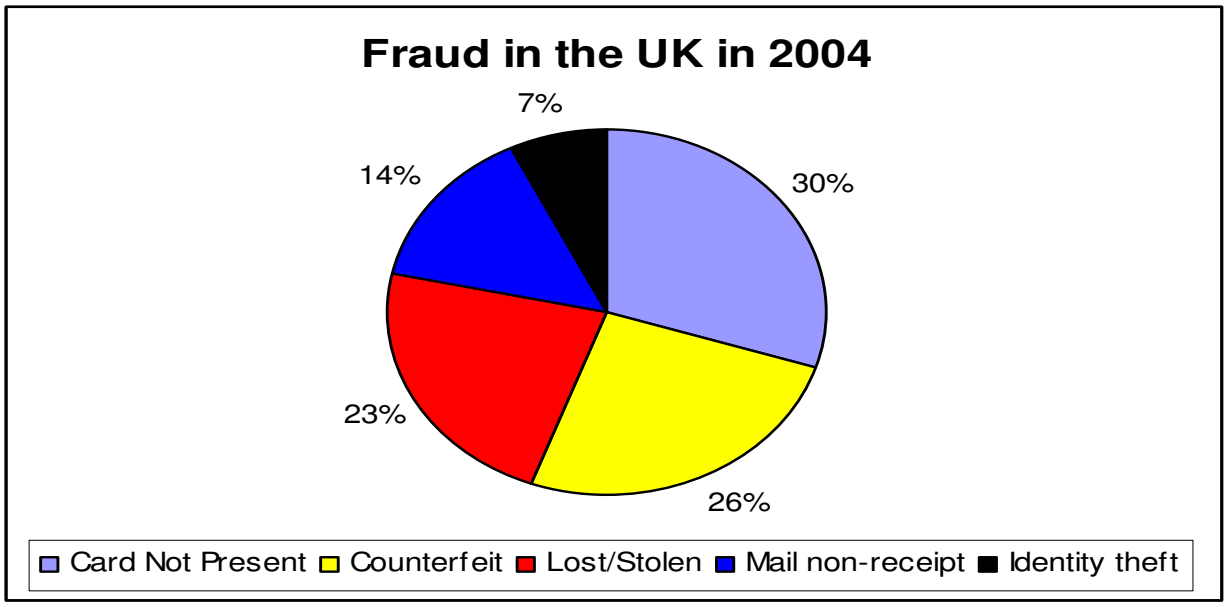
These figures were confirmed by a study done by APACS (the UK payments association) with the following results (reference: www.APACS.org.uk):

Figure 20: Year-on-year growth in fraud types



If one differentiates between the fraud types comprising card losses in the UK for 2004, the following pie chart results:

Figure 21: Fraud losses in the UK per fraud type in 2004 (Pounds Sterling)



In quoting the nature of APACS, as publicized by themselves and to put Card Watch into perspective, “APACS – the UK payments association, is the trade association for payments and provides the forum for the UK financial institutions to come together on non-competitive issues. At the forefront of reducing card fraud is APACS’s Plastic Fraud Prevention Forum (PFPF), which includes representatives from all the UK major card issuers and the international card schemes, including MasterCard and Visa. It develops and implements strategies to prevent card fraud and since the early 1990s has led Card Watch, the public awareness campaign”.

APACS state that most of the card-present fraud (whilst the card and cardholder are present at the time of the sale – “face-to-face”) has declined due to the advent of chip and PIN. The PIN is a more secure way of authenticating the presenter of the card than mere signature verification. The “chip” is a microchip on the card that stores card data more securely than the magnetic stripe making the card more difficult to counterfeit. If one considers this technology in the South African context, issuers and acquirers are looking at rolling-out this technology in 2007, but the roll-out over the entire card and merchant base will take at least two to three years.
APACS also endorse the adoption of lower floor limits to counter fraud losses. An industry hot card file (resident at the Association (MasterCard and Visa)) allows more transactions to be screened against known fraud cards. More than 80,000 retailers subscribe to this service in the UK which provides information on lost and stolen cards. The industry hot card file contains information on more than 6 million missing cards and over 440,000 cases of attempted fraud in 2004. This underscores the need to move to lowering or reducing floor limits and further emphasizes the nature of this research.

Levi, M et al (1991) confirm the hot card file capacities and zero floor limit debate in a study they undertook to determine the cardholder authentication at point-of-sale. They state in their article that in the hundreds of interviews they had had with store staff and sales assistants, the most successful fraud intervention and card apprehension occurs from authorization calls above the merchant’s floor limit. This, they suggest “improves the recovery of lost and stolen cards”.

A study was done in Australia on credit card fraud in 1991 (Bonney, R), which took the frequency of distributions of the average cost of fraudulent transactions per credit card. 67.5% of credit cards used fraudulently had an average ticket value less than $100. This was below the merchant's assigned floor limit. The average ticket values of the balance of the sample were fairly distributed between $100 and $1000. The article confirms that the authorization process protects both the merchant and the bank against the misuse of the credit card product. The data comprising the study were selected from the police on credit card offenses for the years 1989, 1990 and 1991. Cases could not be randomly selected due to the poor quality of the police's microfilm records. In all, 157 cases formed the basis of the study which took place in New South Wales. The 157 cases involved 1,932 separate transactions which were conducted at various merchant categories. The study showed the following results of transactions conducted and authorized:

Table 7: Percentage of transactions in which authorization was sought

Value of transactions ($)	Number of transactions	Number authorized	Percentage authorized
50 or less	754	1	0.1
51-100	1,034	1	0.1
101-150	46	13	28.3
151-200	22	16	72.7
201-300	19	15	78.9
301-500	24	22	91.7
501-1000	23	18	78.3
Over 1000	10	8	80
Total	**1,932**	**94**	**4.9**

The sample was also categorized in accordance to the type of merchant where the fraud took place. The following table reflects this:

Table 8: Fraudulent transactions by type of merchant.

Type of merchant	Number of transactions	%
Department Stores	683	35.9
Shops	440	22.8
Chain Stores	384	19.9
Liquor	177	9.2
Restaurants/Fast Food	112	5.8

Service Stations	39	2.0
Cash/Banks	32	1.7
Supermarkets	17	0.9
Other Business premises	17	0.9
Unknown	21	1.1
Total	**1,932**	**100**

The analysis shows that the majority of the fraud transactions took place at merchant categories that traditionally have a low average ticket value. In *table 7*, only 0.1 percent of transactions less than $100 were authorized. Since $100 was well below the floor limits for most department stores or large chain stores at the time, this was recognized as not being surprising.

Authorization was considered a fraud deterrent in this study. The article states that fraudsters "are frequently aware of what the various floor limits are and purposely buy goods which are below this limit".

Table 9: Fraud perpetrated in South Africa (at Standard Bank) by value band

Fraud Value Band	Fraud Amount	Cumulative (R's)	Fraud %	Cumulative %
R 0 - R 300	R 19,291,941.87	R 19,291,941.87	31.42%	31.42%
R 301 - R 600	R 15,392,198.36	R 34,684,140.22	25.07%	56.48%
R 601 - R 1000	R 4,432,266.88	R 39,116,407.10	7.22%	63.70%
R 1001 - R 2000	R 3,607,488.34	R 42,723,895.44	5.87%	69.57%
R 2001 - R 3000	R 3,266,372.67	R 45,990,268.11	5.32%	74.89%
R 3001 - R 4000	R 2,215,973.97	R 48,206,242.08	3.61%	78.50%
R 4001 - R 5000	R 1,937,115.79	R 50,143,357.87	3.15%	81.65%
R 5001 - R 6000	R 2,230,157.17	R 52,373,515.04	3.63%	85.29%
R 6001 - R 7000	R 1,802,028.48	R 54,175,543.52	2.93%	88.22%
R 7001 - R 8000	R 1,095,121.90	R 55,270,665.42	1.78%	90.00%
R 8001 - R 9000	R 960,740.85	R 56,231,406.27	1.56%	91.57%
R 9001 - R 10000	R 901,722.83	R 57,133,129.10	1.47%	93.04%
>= R 10001	R 4,275,973.44	R 61,409,102.54	6.96%	100.00%
Grand Total	R 61,409,102.54	R 61,409,102.54	100.00%	100.00%

The table above reflects the domestic fraud that took place within the borders of South Africa between 01st January 2006 and 31st December 2006. The fraud was categorized by value bands and as can be seen, the majority of the fraud took place between the value bands of R0.00 to R600.00 which comprises 56.48% of the fraud. The fraud

perpetrated at non “face-to-face” channels (internet, mail order, telephone order) have been removed from this analysis as these transactions automatically enjoy a zero floor limit. This contextualizes the dilemma of fraud perpetrated below floor limits in South Africa. The following bar chart graphically displays this segmentation:

Figure 22: Fraud by value band

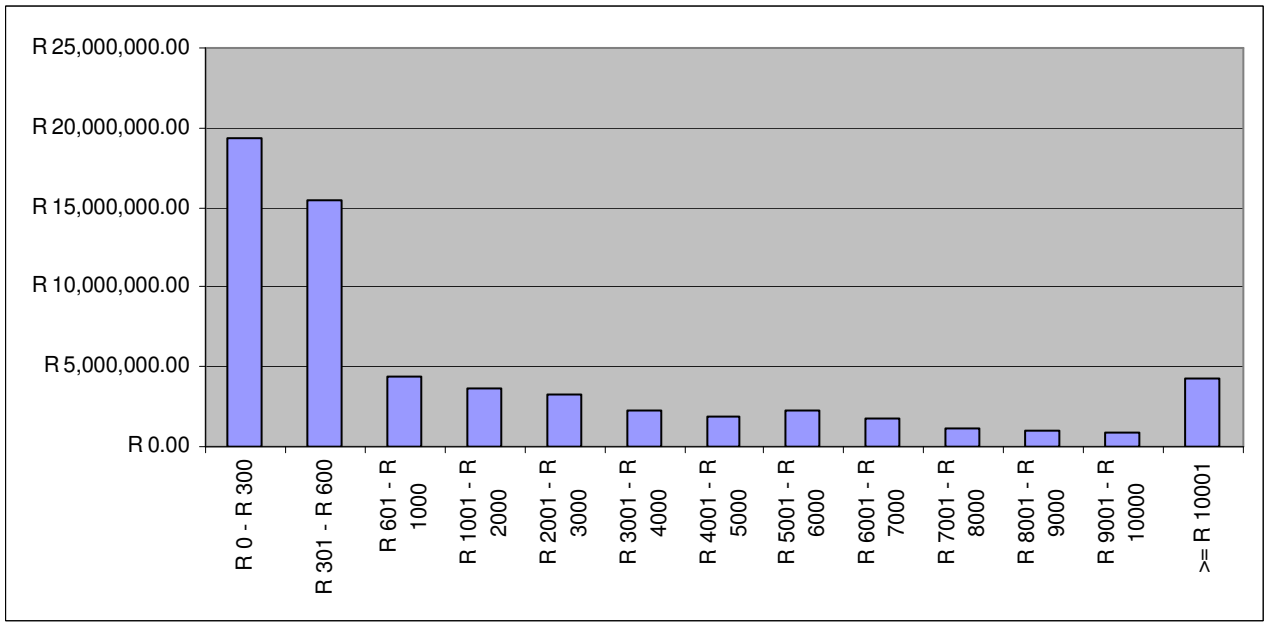


Figure 23: Fraud by Fraud Type in the R0.00 to R300.00 value band

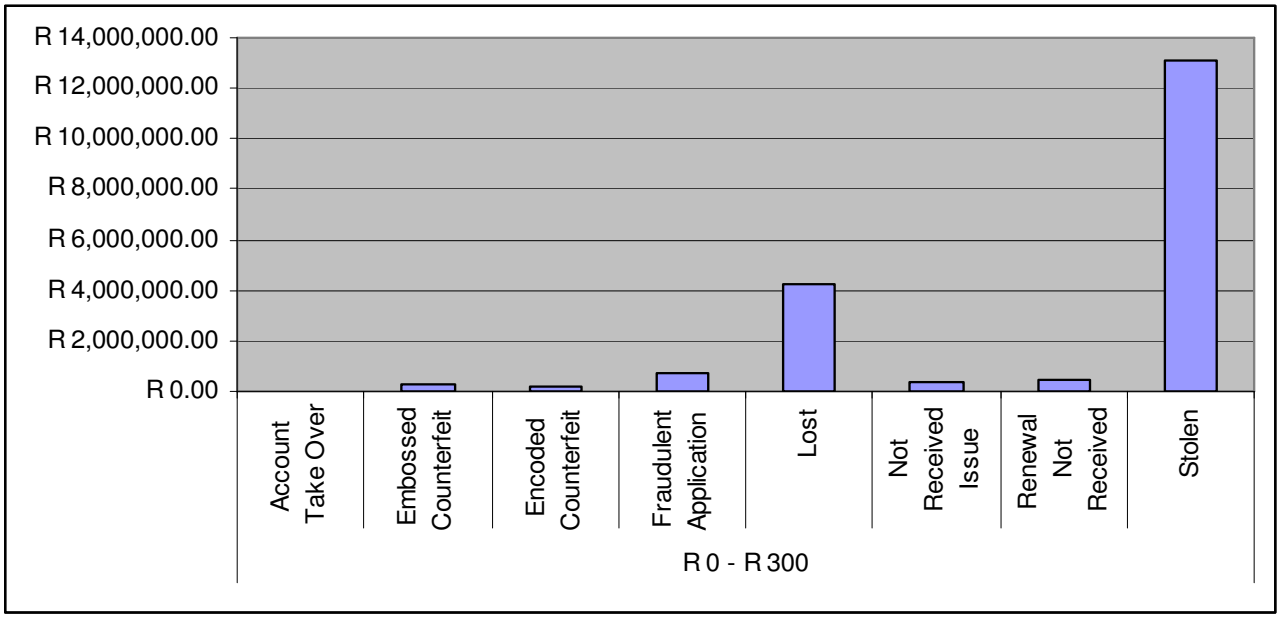
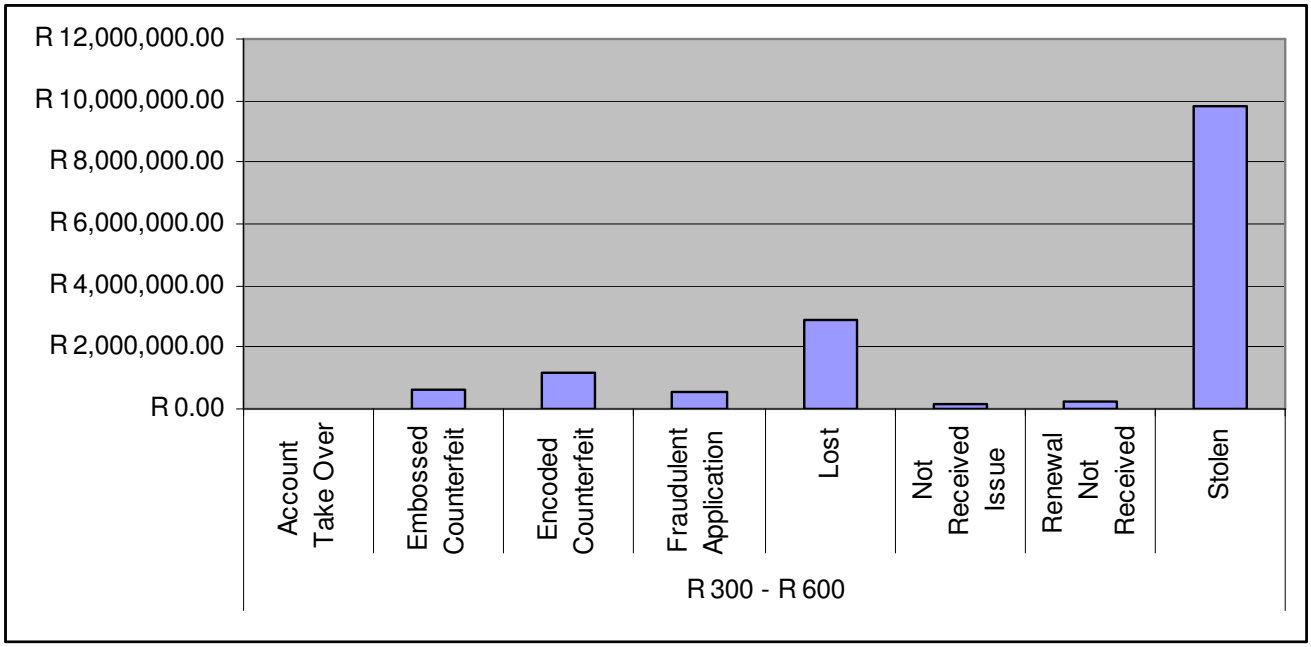


Figure 24: Fraud by Fraud Type in the R300 to R600.00 value band



As can be seen by figures *23* and *24* above, the majority of the below floor limit fraud experienced at Standard Bank between January and December 2006 was in the "lost" and "Stolen" fraud categories.

3.3 Telecommunications technology in South Africa

Telecommunications is defined by Newton H, 2002 as "The art and science of "communicating" over a distance by telephone, telegraph and radio. The transmission, reception and the switching of signals, such as electrical or optical, by wire, fibre, or electromagnetic (i.e. through-the-air) means"

A narrower definition of telecommunications according to Thornton et al (2006) is provided by the Telecommunications Act, which provides for the primary regulation of the telecommunications industry in South Africa. The definition states that telecommunications is "the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio or other electromagnetic waves, or any other agency of a like nature, whether with or without the aid of tangible conductors"

In line with the definitions above, telecommunications generally encompass the following forms of technology:

- Radio
- Telephone
- Television
- Data

Data communications, a specialized subset of telecommunications, refers to the electronic collection, processing, and distribution of data – typically between computer system hardware devices (Stair & Reynolds, (2001:213)). There are several types of communication links, each having its own unique features. The main types of communication links are, (i) coaxial cable, (ii) telephone cable, (iii) microwave channels, (iv) satellite transmissions, (v) fibre optics and (vi) wireless (Eccles, Julyan, Boot, van Belle, (2000:120)). Point of sale devices make use of the following types of telecommunications technology namely, telephone cable, radio pad (microwave channel) and GPRS. The respective communication channels have the following features (Eccles, Julyan, Boot, van Belle (2000:120)):

- Coaxial cable. This cable consists of a copper core enclosed within a metallic sheath to prevent electrical interference. Coaxial cable is normally used for short-distance transmissions within a building or office environment.

- Telephone cable: Standard voice-grade telephone lines are still the most common carriers of data communications, although they are mainly used for local connections from an office to the nearest telephone exchange. The line is mainly made up of a pair of copper wires wrapped around each other (commonly referred to as a *twisted pair*).

- Satellite transmission: Data is transmitted as low-frequency radio waves to the satellite, which has a stationary orbit at a very high altitude (36 000 km). Latest estimates suggest that the satellites will substantially reduce the time and cost of communications compared to the current ground networks.
- Fibre optics: Lasers transmit data in digital format thousands of times faster than other transmitters and with very few errors.

According to Thornton et al (2006), the constraints which involve the evolved telecommunications of today is the telecommunications device and the capacity of the conduit or medium. As communications devices get smaller and the data needs of users increase, the capacity of the pipe will increase.

In all telecommunications, signal strength weakens over distance due to resistance in the wire (or air). As a result, the signals need to be amplified periodically to maintain an adequate signal.

3.3.1 Circuit versus packet switching technologies

In the early days of telecommunications all telephones were analogue devices and in order to hold a conversation, a contiguous link (of copper wire) was required between two telephones. In order to ensure contiguity, the first “circuit switching” was achieved by people in manual telephone exchanges. These operators connected one line to another and facilitated the linking of the copper wire analogue telephone lines. This process became too onerous and human operators were replaced by electro-mechanical devices that determined the analogue pulses of a dialed number and connected callers to each other. The dialed individual numbers had their own pulse as those for the numbers closest to zero were short whereas those closer to nine were longer. The contiguity of the circuit switching has been labeled as inefficient. According to Thornton et al (2006), when we talk on this telephone line , a lot of time is spent saying nothing and the circuit is not being used for a large percentage of time. They state further that as technology has evolved, the copper wire that comes into the home can be used for more than one conversation at a time.

Thornton et al (2006) define the difference between circuit switching and packet switching. With the digital age came the concept of “packets” where a piece of data (a string of ones and zeros) could be broken up into envelopes (referred to as packets). These packets contain sender and receiver address information, headers and information about the packet. The packets are sequentially labeled. This technology thus enables the message to be broken into smaller constituents with each packet being capable of being sent via separate routes to their final destination. This can result in some packets arriving early and some late (and not necessarily sequentially). Packet

switching thus allows the content of a packet to be checked for completeness on arrival. It also enables packets to be stored for a short while at the sending end so that it can be resent in the event that the recipient does not receive or acknowledge receipt after a period of time.

3.3.2 The speed of transmission

Thornton et al (2006) state that one of the biggest advantages of technology is the speed of data transmission down the same bearer (copper wire, fibre cable, Ethernet cable, etc) has increased dramatically. For example, Ethernet (over a copper twisted pair) was originally introduced in 1976 and supported speeds of 10 Mbps. This progressed to 100 Mbps in 1997 followed by 1Gbps in 1998, and already 10 Gbps is available. This is a 100-fold increase in throughput in just a few years.

The home telephone line, originally installed to carry only analogue voice, is used to carry data, with the first modem speeds at 2,4 Kbps. This increased to 128 Kbps with the introduction of Integrated Services Digital Network (ISDN) and now, with the appropriate equipment, the same copper wire, using Asymmetric Digital Subscriber Line (ADSL), can simultaneously support a voice call and a download of data at a combined speed of about 512 Kbps.
The computer processor speed and its reducing costs have enabled the packaging, compression and data checking on data packets to be done in very short time frames.

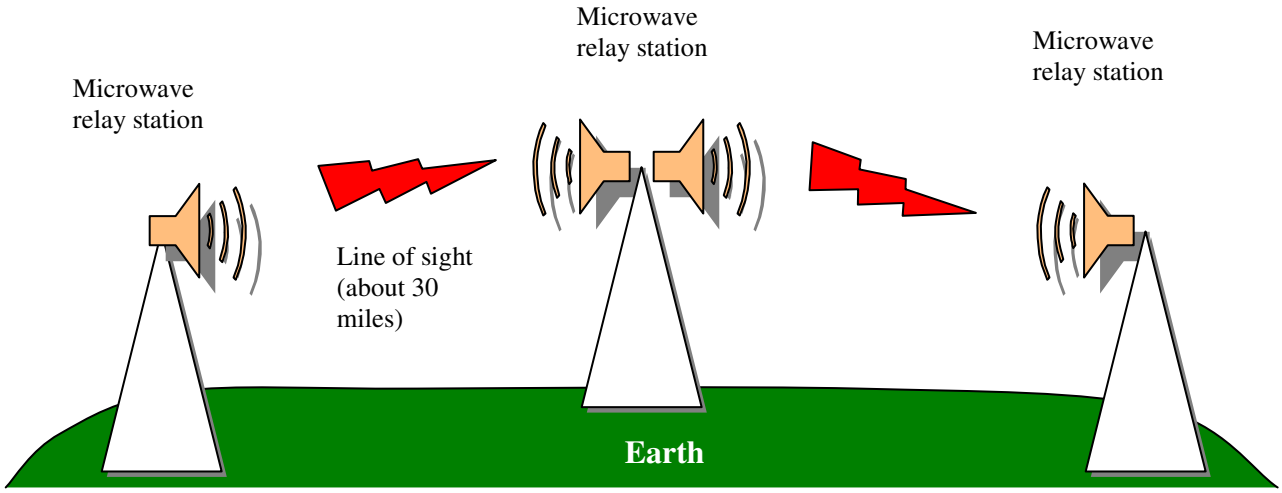
3.3.3 Microwave transmissions

According to Stair & Reynolds, (2001:215), microwave transmissions are sent through the atmosphere and space. Although these transmission media do not entail the expense of laying cable, the transmission devices needed to utilize this medium are quite expensive. Microwave is a high frequency radio signal that is sent through the air.
Microwave transmission is line-of-sight, which means that the straight line between the transmitter and receiver must be unobstructed. Typically, microwave stations are placed in a series – one station will receive a signal, amplify it, and retransmit it to the next transmission tower.

Thornton et al (2006) define microwave as “electromagnetic energy having a frequency higher than 1GHz (billions of cycles per second), corresponding to wave lengths shorter than 30cm. Microwave signals propagate in straight lines and the beams do not readily diffract around hills, mountains and large human-made structures. Some attenuation (loss of signal strength) occurs when microwave energy at longer wavelengths is affected to a degree by such obstacles”. The authors also state that the microwave transmission allows for a large bandwidth. The large bandwidth in turn translates into a higher data speed of transmission.

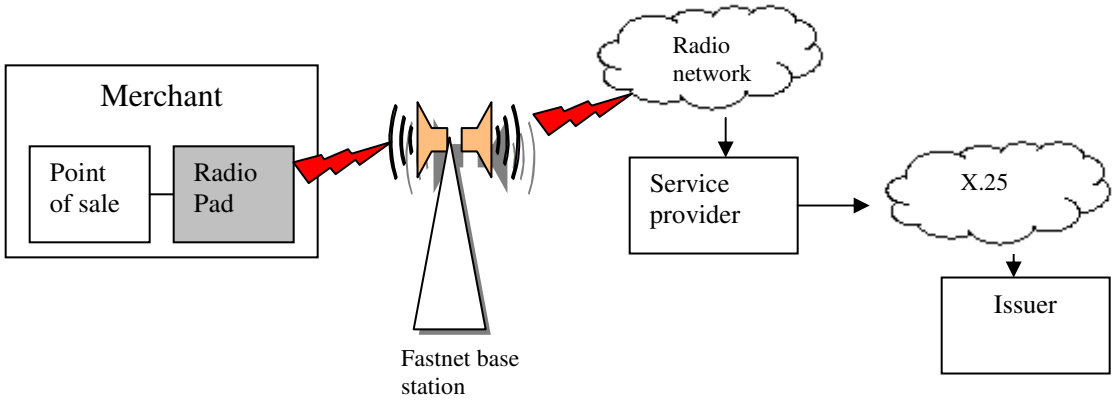
Bandwidth is an important consideration in ensuring that credit card sales are quickly authorized. MasterCard International require that an authorization request and response do not exceed 30 seconds. Albeit that fraud savings are proposed by a reduction in floor limits, one cannot discount the importance and overriding business argument of customer service fulfillment. The longer the authorization request and response rate, the greater the customer inconvenience and experience at the point of sale.

Figure 25: Microwave Communications



The current communication methods available to POS devices consist of the SAPONET Telkom network or alternatively through a wireless network (microwave). Following is a brief description of both.

Figure 26: Microwave transmission



The radio pad interacts with a base station where it is routed through the service provider's network before being delivered to the bank via the X.25 network. Service providers have base stations installed in all the major cities and towns across South Africa.

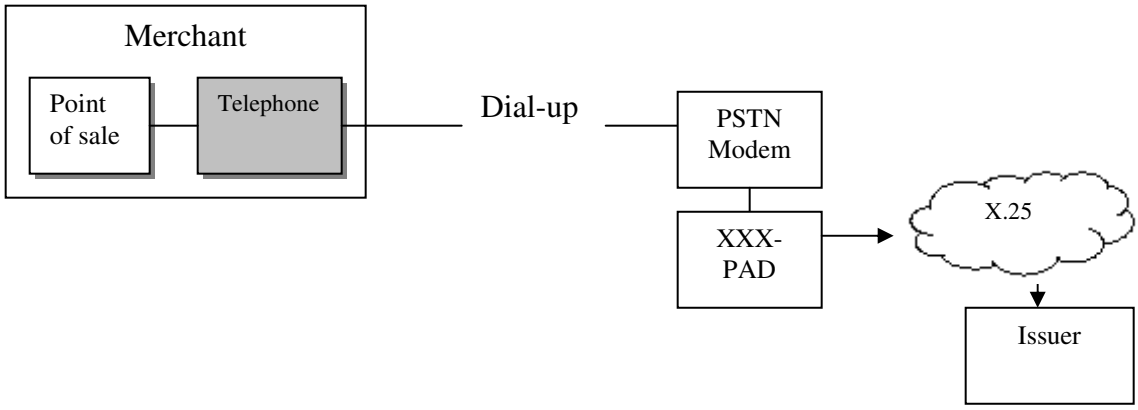
Microwave transmissions via radio pad are currently used in the retail industry where it is linked to point-of-sale devices. A small radio-communication device provides an efficient radio communication link between the point-of-sale terminal and the banks' computers by replacing the telephone line. This technology allows for rapid card authorization which in turn improves customer satisfaction and reduces queue delays at the checkout point, whilst delivering a cost-saving to the business owner. (http://www.fastnet.co.za).

Fastnet is a service provider of this technology. The network typology of this service is illustrated in *figure 26* above. The radio pads are linked to a number of "base stations" - currently numbering over 35 - dotted around the Western Cape, Gauteng and parts of Natal. The Fastnet base stations, each of which have a range of 25 km, are linked via high speed leased lines to Telkom's existing X.25 fixed line packet data system. Each base station is capable of supporting 800 simultaneous users in peak access periods and around 1,200 in off peak periods.

3.3.4 Telephone Communications

The telephone communications network for point-of-sale is illustrated in *figure 27* below:

Figure 27: Telephone Communications



The point-of-sale device will telephone a local telephone number and will connect to the X.25 network by connecting to a modem that is connected to a XXX-pad. The XXX-pad has a direct interface to the X.25 network, from where the POS device will then connect to the host system. According to Wikipedia (http://en.wikipedia.org/wiki/X.25), X.25 is a protocol suite for wide area networks using the phone or ISDN system as the networking hardware. The general concept of X.25 was to create a universal and global packet-switched network on what was then the analog phone system. X.25 was developed in the era of dumb terminals connecting to host computers. Instead of dialing directly “into” the host computer (which would require the host to have its own pool of modems and phone lines, and require non-local callers to make long-distance calls), the host could have an X.25 connection to a network service provider. Now dumb-terminal users could dial into the network's local “PAD” (Packet Assembly/Disassembly facility), a gateway device connecting modems and serial lines to the X.25 link.

Having connected to the PAD, the dumb-terminal user tells the PAD which host to connect to, by giving a phone-number-like address in the X.121 address format (or by giving a host name, if the service provider allows for names that map to X.121 addresses). The PAD then places an X.25 call to the host, establishing a virtual circuit. Note that X.25 provides for virtual circuits, so it *appears* to be a circuit switched network, even though in fact the data itself is packet switched internally, similar to the way TCP

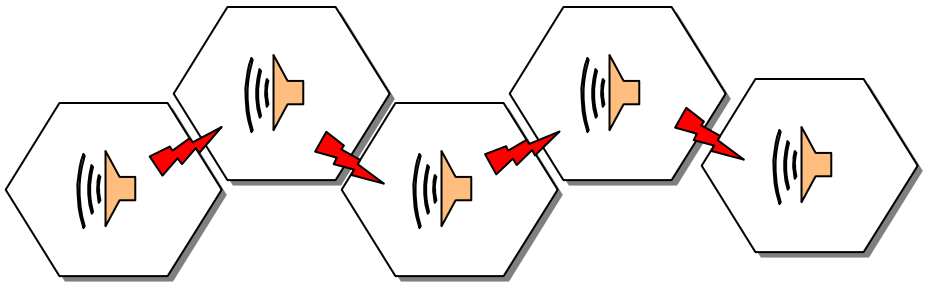
(Transmission Control Protocol) provides virtual circuits even though the underlying data is packet switched. Two X.25 hosts could, of course, call one another directly; no PAD is involved in this case. In theory, it doesn't matter whether the X.25 caller and X.25 destination are both connected to the same carrier, but in practice it was not always possible to make calls from one carrier to another.

X.25 networks are still in use throughout the world, although in dramatic decline, being largely supplanted by newer layer 2 technologies such as frame relay, ISDN, ATM, ADSL, POS, and Internet Protocol. X.25 however remains one of the only available reliable links in many portions of the developing world, where access to a Public Data Network (PDN) may be the most reliable and low cost way to access the Internet.

3.3.5 Cellular Transmission (GPRS)

According to Stair & Reynolds, (2001:217), a local area, such as a city is divided into cells. The signals from the cells are transmitted to a receiver and integrated into the regular phone system. Cellular transmission uses radio waves and by combining cellular transmission with other devices, it opens up the power of networks, communication and the internet.

Figure 28: Cellular data communication

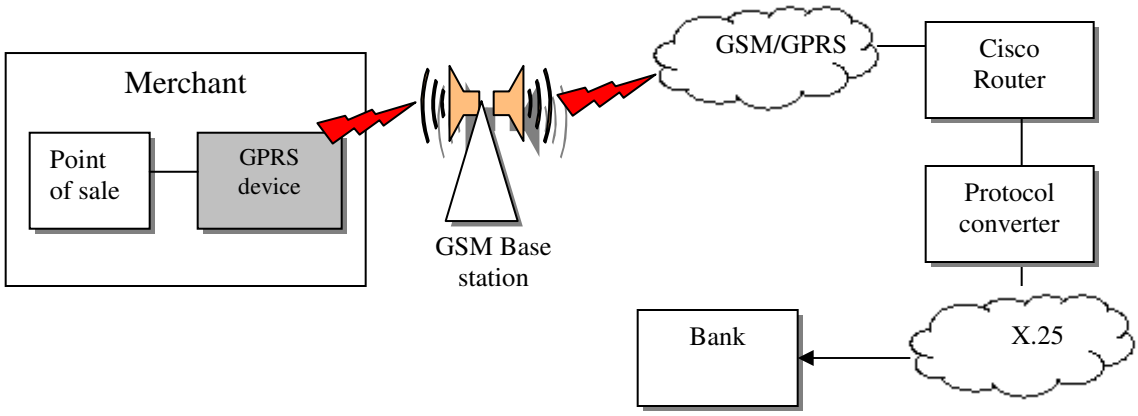


GPRS is defined by Http://WWW.GPRS.Org: GPRS or the General Packet Radio Service is a non-voice value added service which allows you to send and receive data across a mobile phone network. It provides a supplement to today's CSD (Circuit Switched Data) and Short Message Service – commonly known as SMS.

GPRS is defined by Thornton et al (2006) as “GPRS is a radio technology for GSM (Global Systems for Mobile Communications) networks that supports packet-switching protocols like IP across cellular networks. It is usually charged on volumes of data rather than on connected time. It is an always-on technology, as a user can remain connected for long periods without transmitting any data. This technology is often referred to as 2.5G, as it is emulating packet based data communication over cellular links, rather than true 3G, which is a true packet based communication means”.

GPRS should not be confused with GPS – the global positioning system – a similar acronym sometimes used in mobile context. GPRS has several unique factors such as the speed. The maximum speed of a GPRS connection is around 171.2 kbps when using all 8 of the GPRS timeslots at the same time. This is around three times as fast as the usual data transmission speeds over today’s fixed telecom networks and ten times faster than the CSD or circuit switched data on the GSM Networks. GPRS works by allowing all the information to be transmitted more quickly, immediately and efficiently across the mobile network. GPRS is also less costly to send data than SMS and Circuit Switched Data. GPRS connects instantly so information can be sent and received immediately as and when the need comes up – depending on radio coverage. You do not need a dial up modem which is why GPRS is sometimes referred to as being “always connected” – This is an extremely important feature of GPRS as is needed for time critical applications such as authorizing credit cards when it would be considered unacceptable to keep the customer waiting a long time. There are various GPRS point-of-sale solution is the market. The following diagram illustrates how the GPRS technology works from a holistic level:

Figure 29: GPRS data communication



In an article on www.balancingact-africa.com, an Information Communication Technology specialist Grintek Telecom, a Grintek Limited company, has developed a 'smart' power supply unit for point of sale terminals, providing an integrated standard power supply, a GSM GPRS modem and lightning protection - all in one unit. The article states that “As the unit is GPRS based, it provides the merchant with an always connected' service which assists to reduce fraud with stolen credit or debit cards, eliminating the requirement to 'dial up' for authorization, reducing risk to financial institutions and saving money for the merchants, as the time and cost to connect to the banks is drastically reduced.” This technology alleviates the need for floor limits as the merchant is continually connected to the bank. Speed and reliability of service are key considerations in adopting this technology as already mentioned in this paper.

Grintek goes on to state that “all POS terminals have to communicate with the financial host or bank to clear a transaction before the slip is printed for the customer to sign. Traditionally, PSTN, dial-up X.25, GSM data and radio X.25 methods are used to dial up to the bank host, but they are expensive and slow. Financial institutions download a daily 'hot card' file to their merchants' POS terminals and as traditional communications systems do not include GSM technology, these files are usually downloaded at night. This provides potential fraudsters with the opportunity to use fraudulent cards during this 'window period', provided the amount does not exceed the floor limit - the limit on a card before authorization is required to process the transaction.” This statement lends further weight to the argument to look at telecommunications as the vehicle to move towards zero floor limits and a concomitant reduction in fraud losses. The cost-benefit argument from an acquirer and merchant perspective is further alluded to when Grintek states, “providing GSM 'always on' connectivity means that the hot card file located at the bank host is used, which is automatically updated in real time, eliminating the risk of fraudulent transactions. This functionality allows financial institutions to make substantial savings, since the merchant is not responsible for these types of fraudulent transactions”. The responsibility for the fraudulent transaction are only via charge backs where the issuing or acquiring bank have valid charge back reasons to the merchants. As mentioned, this is in instances where the merchant failed to honour their contractual obligations as set out by the acquiring bank. Charge back savings in themselves may not be a sufficient incentive to mitigate the costs associated with GPRS. If the costs (in comparison to telephone connectivity (“dial-up”) for every transaction or radio connectivity are

competitive and speed and reliability are not compromised, this may be a feasible solution. Grintek state that “therefore, the return on investment for this seemingly simple piece of equipment is significant. Grintek Telecom is able to add value to its customers in the retail environment through the prevention of fraud with this product and through lowering costs incurred by the merchant."

In consulting with various technical staff at Standard Bank (D, Els, N, Jansen, Network Architects – Infrastructure Solutions Design, 2007 Personal Interview, 06 August 2007, 5 Simmonds Street, JHB) , it was confirmed that the X.25 protocol is archaic and outdated. Standard Bank would be better positioned to service its merchants and their customers by using GPRS and receiving the transactions directly into its infrastructure and avoiding the X.25 protocol. This is illustrated in figures *30* and *31* below. *Figure 30* illustrates the use of the X.25 conversion protocol before the transaction enters the issuer’s infrastructure. *Figure 31* illustrates the intended disintermediation of this service which will allow for more efficiencies and speedier transaction transportability.

Figure 30: The current X.25 interface at Standard Bank (Macro view)

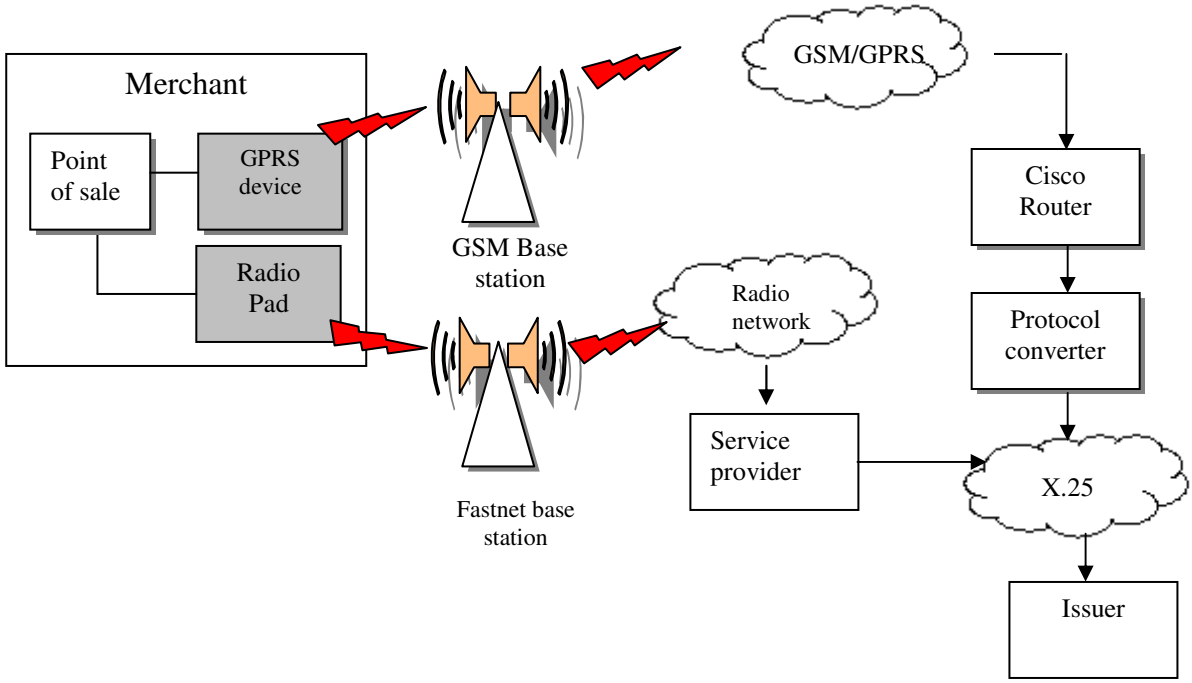
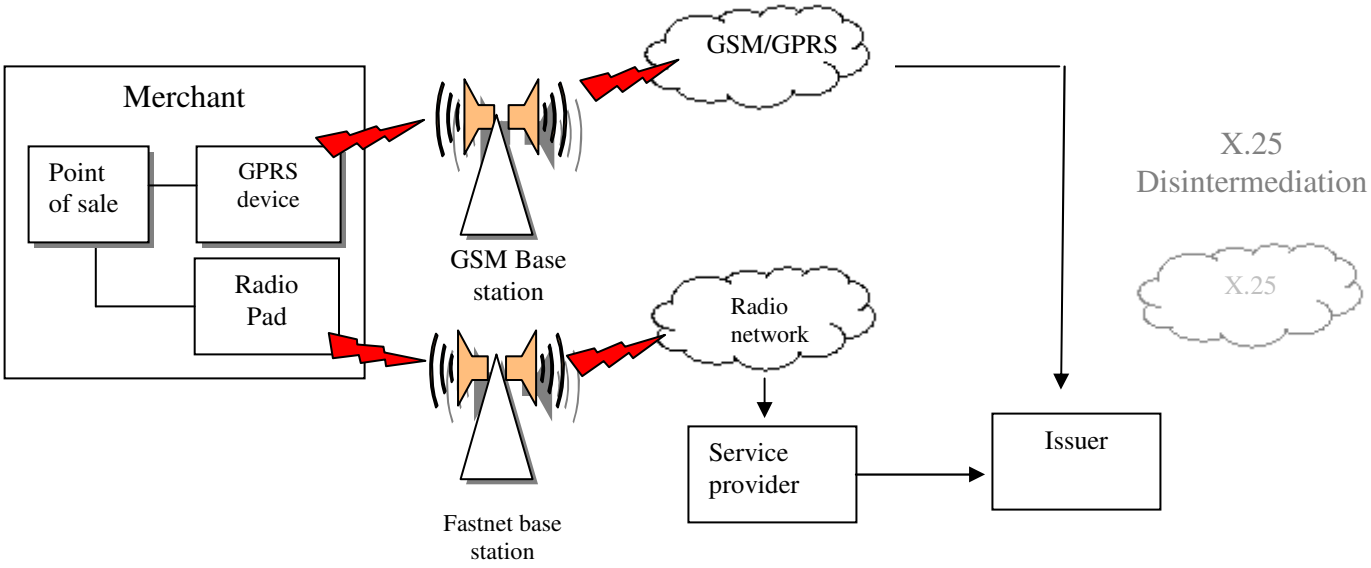


Figure 31: The proposed interface at Standard Bank (Macro view)



In a further article on www.biz-community.com, "*The benefits of wireless data communication*", The Look and Listen Group recently installed wireless data communication devices in 19 stores country-wide. The article states that "In order to reliably process debit and credit card payments, with minimal downtime and effective technical support, The Look and Listen Group recently installed wireless data communication devices. Apart from security and peace of mind, a cost saving in the region of 20 - 30% is possible on telecommunication costs associated with EFT (Electronic Funds Transfer) transactions". This GPRS device replaces the telephone line as a link between the point-of-sale and the financial institution. The article confirms that EFT payments are processed at high transaction speeds, with the risk of down-time minimized in even remote towns throughout South Africa. The article further states that transaction speeds are less than four seconds and that there is no trade-off between secure banking and increased sales turn over.

This article further lends weight to the speed and efficiency of current GPRS technology and further supports the capacity argument that some schools of thought may have in terms of transactional volumes at point-of-sale that would be associated with a zero floor limit.

3.3.6 The costs and efficiency of telecommunications in South Africa

According to www.southafrica.info (2003), "South Africa ranks 23rd in telecommunications development in the world. The country had approximately 4,92 million installed telephones and 4,3 million installed exchange lines at this time. This represented 39% of the total lines installed in Africa. National operator Telkom had met and exceeded its roll-out targets of over 1,6 million lines, 175 488 more than the cumulative target. South Africa has a large transmission infrastructure, necessitated by the country's vast geographical area of 1,2 million km². Covering about 156 million circuit-kilometres, the transmission network constitutes the backbone of all telecommunications services.

The network is almost entirely digital. Digital microwave and optical fibre serve as the main transmission media for the inter-primary network, interconnecting all major centres.

www.southafrica.info (2003) states that "South Africa, with the operators Vodacom, MTN and Cell C, is the fourth fastest growing GSM (Global Systems for Mobile Communications) market in the world and is growing at a rate of 50% per annum.

Market size was 14,4 million users in February 2003 according to Cellular Online and this could grow to 19 million by 2006. Market Share is Vodacom (7,5 million), MTN (5,22 million) and Cell C (1 million). It says that the SA market is currently worth R23 billion and could reach R45 billion by 2004.

Value-adding cellular growth rate network operators provide services such as Internet connectivity, electronic mail, protocol conversion, data processing and access to global databases. Complemented by expertise in network design, implementation and management, this gives South Africa one of the most advanced telecommunication systems of all emerging markets.

Khanna, (2004) states in the Toys R Us article that the retail chain decided to convert from its 10-year old point-of-sale terminals that used X.25 technology to the new IP protocols. This is in line with Standard Bank's approach to disintermediate this protocol as illustrated by figures *30* and *31*. Cost savings was one of the major business drivers for the move. The article states that POS terminals connected to IP networks have significant advantages over the old X.25 system. The advantages include extra

bandwidth to run other applications, its speed of data transfer and its continual connectivity to a host system. In the article, James Hicks, vice-president of product development and marketing for Toronto-based Global Payments Canada, which does the transaction processing for “Toys R Us”, also sings the praises of IP networks. "IP is an exciting thing that will continue to evolve over the next few years," he says. It's much faster than dial-up, which can take 10 to 20 seconds, depending on the transaction, IP can do a credit card transaction in four or five seconds.

Markowitz, (1994) states in an early article on Kmart “Credit authorization used to take anywhere from 15 seconds to 15 minutes, depending on the floor limit. Now, using point of sale (POS) terminals and the satellite network that gives the chain's 50,000 registers on-line access to credit centres, the process takes less than 7 seconds, most often under 4 seconds”. This early article lends weight to the floor limit debate and the speed and response of authorisation requests submitted electronically. The floor limit is a key determinant of the amount of data traffic that gets sent to the issuing bank via the network.

In an early article (Crockett, B, 1992), and in relation to the article by Anonymous (1993:3 *(Proquest)*) on Visa’s reduced floor limit ruling, the Visa mandate requiring merchants to obtain bank authorization for all Visa credit card purchases could reduce revenue for banks that acquire small retailers. The article by Crockett states “But with the new rule, these smaller merchants will either have to call the bank about every Visa purchase or install point-of-sale devices that handle authorizations electronically. Both options carry their costs. Telephone authorizations are subjected to a 40-cent fee from First Union (an acquirer – researcher). For a typical merchant on a typical transaction, this would raise the effective discount fee from about 5% to about 7% of the value of the purchase. Installing electronic point-of-sale terminals would enable merchants to avoid the steep telephone authorization fees, but the higher equipment costs can initially offset the savings”

Telkom SA tariffs as at August 1, 2006 (including VAT)) for business applications include:

Table 10: Telkom SA tariffs as at 2006

Service	Tariff
Business installation	R342.30
Monthly Rental	R132.75
Local calls (0-50km) – peak rates	
Minimum charge for the first unit of 89 seconds	R0.59
Long distance calls (> 50km) – peak rates (per minute)	R0.72
Outgoing calls to mobile network (1 minute)	R1.89
International calls to the United States – peak rates (per minute)	R1.20

Source: Telkom South Africa, BMI-T, 2006 (387)

Until 2002, Telkom's business, fixed and mobile, was driven largely by voice communications and traditional data services such as leased line provision. The Group has since been making strong inroads into data services, especially internet and managed data networking services, and is now moving up the Information and Communications Technology (ICT) value chain by providing higher levels of ICT services and products. The shift in strategy is spelt out in Telkom's vision, which is to be the leading customer and employee-centred provider of ICT solutions.

According to XLink (www.XLink.co.za), a cellular service provider, over 4500 retail establishments use GPRS as a technology to facilitate credit card transactions resulting in up to 30% savings in communication costs. This is one of many service providers that offer GPRS and they quote the benefits of high speed, cost efficiency and reliability.

Table 11: XLink tariffs as at 2007

	Lite	Standard	Express
Monthly charges (ex VAT)	R 175.00	R 195.00	R 295.00
Nº. of Transactions per month	600	1800	3000
Data Cap per month	0 - 1.5MB	1.5-2.5mb	2.5-10mb

Source: www.xlink.co.za

In a further article by www.biz-community.com, it was further agreed that the GPRS technology deployed to process debit and credit card payments resulted in a cost saving on telecommunication costs associated with EFT transactions between 20% and 30%. XLink, the supplier of wireless communications, deployed this technology within the Look and Listen Group in nineteen stores countrywide with the concomitant savings mentioned above. The article further explains the technology by stating "The XLink communicator is a device that replaces the telephone line as a link between the point-of-sale and the financial institution, connecting the two via GPRS over mobile networks MTN and Vodacom. The result: EFT payments processed at high transaction speeds, with the risk of down-time minimized in even remote towns throughout South Africa. The use of floor limits is avoided, as the XLink Communicator makes a connection and obtains complete authorization for every transaction. The device therefore provides a reliable and secure EFT link and is well-suited to the debit card environment, a market that is said to have surpassed that of credit cards in South Africa. The device is approved by the four major banking institutions in South Africa". This article further emphasizes the benefits associated with GPRS technology and the ability to conveniently and quickly process transactions conducted at the point of sale.

Table 12: Fastnet Radio Pad Tariffs

Purchased Radio PAD (becomes the property of the customer)

Option	Connection Fee (Once-Off)	Monthly Maintenance Fee	Call Charges (Peak Hours)	Call Charges (Off-Peak Hours)
Radical	R75.30	R30.75	11.5 Cents	11.5 Cents

Rented Radio PAD (Remains the property of FastNet)

Option	Connection Fee (Once-Off)	Monthly Maintenance Fee	Call Charges (Peak Hours)	Call Charges (Off-Peak Hours)
Benefit	R75.30	R80.50	43.5 Cents	18.0 Cents
Merit	R75.30	R126.40	31.5 Cents	18.0 Cents
Value	R75.30	R178.50	18.0 Cents	18.0 Cents

Source: www.fastnet.co.za

Table 12 lists the radio pad tariffs as published by the microwave service provider, Fastnet.

If one compares the three types of data communication technology purely from a price perspective, the following is apparent:

1 Telephone Line (Telkom)

Fixed costs (excluding installation)	R132.75 per month
Variable costs (range):	R0.59 per call to R1.20 per call
(The rate per minute has been discounted)	

2 Radio Pad (Fastnet)

Fixed costs (range):	R30.75 per month to R178.50 per month (depending on the option selected)
Variable costs (range):	R0.115 per call to R0.435 per call

3 GPRS (X-Link)

Fixed costs (range):	R175.00 per month to R295.00 per month
Variable costs:	**None**

Thus from a cost, efficiency and reliability perspective, GPRS is the most feasible solution to a zero or reduced floor limit for merchants that process a reasonable volume of credit card transactions. GPRS has not variable cost associated with the number of authorisation requests as it is “always connected” to the acquiring bank. The reliability of this service will be discussed as part of this research report.

CHAPTER 4

4. Research structure and design

4.1 Introduction

It is appropriate to repeat the statement of the problem and its sub-problems in this section with the respective hypotheses which will be tested.

The problem statement: The purpose of this study is to analyse the effect that merchant floor limits have on bank-issued credit card fraud in the South African credit card industry and compare this to the ability of telecommunications to sustain a zero-floor limit environment.

Sub-problem 1:
The first sub-problem is to analyze the effect of merchant floor limits in South Africa with their impact on bank-issued credit card fraud.

Sub-problem 2:
The second sub-problem is to determine the ability of current telecommunications technology to sustain a zero floor limit environment.

Sub-problem 3:
The third sub-problem is to determine the costs associated with current telecommunications technology in sustaining a zero floor limit environment.

Sub-problem 4:
The fourth sub-problem is to analyze and interpret the data so as to evaluate the feasibility of introducing zero floor limits in South Africa considering telecommunications technology and costs.

The Propositions are reiterated below:

Proposition 1:

The first Proposition is that merchant floor limits in South Africa have an adverse impact on bank-issued credit card fraud.

Proposition 2:

The second Proposition is that South African telecommunications can sustain a zero floor limit.

Proposition 3:

The third Proposition is that the cost of introducing a zero floor limit in South Africa is negligible in relation to the fraud which floor limits sustain.

Proposition 4:

The fourth Proposition is that the local banking infrastructure and technology can accommodate an increase in authorisations as a result of a zero floor limit environment.

4.2 Research methodology

The research methodology that will be used is a qualitative study based on a proposition. The proposition will be supported or rejected by making use of logical reasoning and induction. The research problem is of such a nature that it is difficult to test hypothesis with the data extracted as part of this research report. A set of propositions are used which is supported or rejected making use of logical reasoning and induction.

According to Leedy and Omrod (2005), qualitative research is typically used to answer questions about the complex nature of phenomena, often with the purpose of describing and understanding the phenomena from the participant's point of view. It is also mentioned that qualitative researchers seek a better understanding of complex situations and their work is often exploratory in nature. The nature of this research includes a strong component characterising exploration and interpretation of events and situations. Inductive reasoning is used in some cases based on the observations of events.

Leedy and Omrod state that quantitative research is used to answer questions about relationships among measured variables with the purpose of explaining, predicting and controlling phenomena.

4.3.1 Alternative research methodology considered

It was initially proposed that the researcher would do a quantitative research methodology. The methodology would have been applied in the following manner; the purpose of the research is to explain and predict how point-of-sale devices and front-end processors will handle a zero floor limit environment. The data is numeric and comprises a large representative sample. Statistical analysis would have been used to analyze the data and their meaning with a focus on objective interpretation. A parametric test would have been used (One-Sample Chi Square Test).

A **"goodness-of-fit"** test would have been used to compare the extent to which the observed (i.e. empirical) frequencies "fit" the expected (i.e. theoretical) frequencies. The anticipated increase in authorisation volumes due to a zero floor limit environment would have been compared with the ability of Standard Bank's front-end processor (Postillion) to handle the volume of transactions (measured by its transaction per second processing capability). According to Diamantopoulos, Bodo and Schlegelmilch (2000), the One-Sample Chi-Square test is the test which compares a set of observed frequencies with a set of theoretical frequencies. The observed frequencies (calculated from empirical data) would have comprised the increase in authorisations as a result of a zero floor limit. This would have reflected the actual distribution of the variable concerned in the data. The theoretical distribution which would have reflected the researcher's expectations of the variable in the population would have been compared to the actual distribution of transactions conducted below the floor limit. This would have been related to the ability of Standard Bank's front-end processor to process the increase in transactions. The hypotheses were:

H_0: There is no difference between the observed and theoretical distributions

H_1: There is a difference between the observed and theoretical distributions

A simulator would have been used to test the ability of the front-end processor to handle an increase in the number of transactions as a result of a zero floor limit.

4.3.2 Limitations of the research methods and study

A stress test (simulator) requires a project to be raised, prioritised and takes approximately 6 weeks of extensive testing. This was confirmed with the test manager within Standard Bank's Group IT. It is due to the considerable cost and time involved that an existing stress test (done in 2006) was used. To develop a simulator to test "what-if" scenarios would not be feasible due to the complexity and variability of the system architectural components and intermediaries. A simple simulation would not be sufficient to cater for all of these actors and concomitant variables and would not adequately prove the ability of Standard Bank's front end processor to handle zero or reduced floor limits.

Per Diamantopoulos et al (2000) (154), the One Sample Chi-Square test is used when one wants to compare a set of observed frequencies with a set of theoretical frequencies. The question arises is whether the differences between observed and theoretical frequencies are significant.

H_0: authorisations frequencies = postings frequencies

H_1: authorisations frequencies $\neq$ postings frequencies

Postings refer to transactions that took place below the merchant's floor limit and as such did not go to the issuing bank for authorisation. These transactions are posted to the customer's account during a batch run.

The distributions being tested are those of authorisations (which have a time stamp) in conjunction with postings (transactions conducted below the merchant's floor limit) which *do not have a time stamp* for this test. The time stamp is not stored for transactions conducted below the merchant's floor limit by Standard Bank. A large sample of data (transactions below the merchant's floor limit) is available from the Group's data mart but no time is stored. This makes the use of the chi-square test irrelevant for testing the assumption that posted transactions follow the same distribution as the authorised transactions.

4.4 Method of primary data collection

The representative sample for data collection will be the period 01 January 2006 to 31 December 2006. The primary data comprising the sample will be collected from within Standard Bank. The sample reflects a convenience sampling method in that the sample is chosen on the basis of the data being readily accessible. The following primary data will be collected for analysis over the period mentioned above:

- All credit card authorisations
- All transactions conducted below the merchant's designated floor limit (non-authorisations). As mentioned in the assumptions, it is assumed that the non-authorised transactions will follow the same distribution as the authorised transactions.
- The maximum transactions per second (TPS) processing ability of Standard Bank's front-end processor (Postillion).

The authorisation and non-authorised data is currently stored within Standard Bank's data warehouse. The front-end processing capability in transaction per second is available on the application itself.

Data collected from Bankserv (a local transactions switch) for 2006 will also be collected and analysed to ascertain the maximum load that these processors can handle (authorisations and postings). This primary data also constitutes a convenience sample (non-probabilistic). The reason for obtaining this sample is that all domestic transactions where the issuer and acquirer are not the same institution are switched via this entity. The transaction switching comprises a substantial volume and is representative of the domestic credit card market.

The researcher had conversations and interviews with technical and business personnel from the following companies:

- Fraud Managers from various local banks
- Fraud representatives from the Card Associations
- Managers from the Merchant Services functional area in Standard Bank.
- Standard Bank technical personnel in the IT and telecommunications field.
- Computer Software Consultants that install point-of-sale software

- Fair, Isaac, (a vendor of fraud predictive and analytic software based in the USA)
- Retail Decisions (a vendor that manages the industry hot card file (INCF)) and is involved in telecommunications with large retail outlets.
- Fastnet (the vendor that supplies radio pads to merchants for microwave transmission to the acquirer)
- XLink (the vendor that supplies GPRS solutions to merchants for transmission to the issuer)
- Connectnet (the vendor that supplies GPRS solutions to merchants for transmission to the issuer)

The semi-structured interviews with these people included the following kinds of questions:

1. Can the local telecommunications infrastructure handle a zero floor limit environment?
2. How reliable is Telkom in servicing a zero floor limit?
3. Can issuing banks handle the volume of transactions that would be attributable to a zero floor limit?
4. Can acquiring banks handle the volume of transactions that would be attributable to a zero floor limit?
5. What are the perceived costs of introducing a zero floor limit?
6. Is below floor limit fraud a problem or is it a necessary cost of doing business?
7. Which technology is best-suited to sustain a zero floor limit considering cost, speed, efficiency and effectiveness?

The researcher transcribed the interviews and added comments as it was reviewed.

4.5 Method of secondary data collection

All fraud transactions on credit cards are reported by the South African issuing banks to SABRIC. The differentiation between below and above floor limit fraud cannot be ascertained using SABRIC's data due to the product differentiation between the banks.

Standard Bank's issuing fraud data will be used as a representative sample of the fraud within the domestic industry. Standard Bank represent 25% market share from a credit card perspective (DI 900, Standard Bank, 2007). This secondary data will be obtained by the researcher over the representative period of 01 January 2006 to 31 December 2006. The data will be segmented into transactions which took place below the merchant's floor limit and that which took place over the merchant's floor limit. This analysis will show the potential fraud savings which would have occurred had the floor limits been reduced to zero over the representative period. This data will be used to induce the effect that zero floor limits would have had on credit card fraud (Proposition 1). The sampling method used is also judgemental sampling (non-probabilistic) based on the researcher's judgement.

The second and third Proposition will be exploratory and qualitative in nature in terms of the research findings.

Stress tests (simulated volume test data) will be collected from Standard Bank's data mart over the period May and June 2006. A stress test is a simulation whereby the system architecture, notwithstanding all system components and intermediaries, are sent volumes of data (authorisations and settlement) to determine the maximum capacity that these entities can process. The volume or stress test results will be discussed as part of this research.

4.5 Justification of method deployed

In light of the two main research constraints stated in section 4.3.2, a proposition will be used to reason the case for reduced or zeroed floor limits. According to Leedy and Omrod (2005:32); "In Inductive reasoning, people use specific instances or occurrences to draw conclusions about entire classes of objects or events. In other words, they observe a sample and then draw conclusions about the population from which the sample comes". The research comprises many dimensions and perspectives and as such a qualitative research methodology was decided upon.

4.6 Data validity and reliability

According to Leedy and Omrod (2005); “Reliability is the consistency with which a measuring instrument yields a certain result when the entity being measured has not changed. The validity of a measurement is the extent to which the instrument measures what it is supposed to measure”.

The respective samples being obtained comprise the following:

1. Data contained within Standard Bank’s data mart on all authorizations and postings from January 2006 to December 2006.
2. Data results from a stress test performed from May to June 2006
3. Data from Bankserv from January 2006 to December 2006.
4. Samples from a survey to determine attitudes and opinions relating to floor limits and telecommunications.

The first and third sample (data contained within Standard Bank’s data mart on all authorizations and postings from January 2006 to December 2006 and Data from Bankserv from January 2006 to December 2006) is considered to have content validity (sample validity is the extent to which the sample relates to the characteristic of interest). Criterion validity is based on the assumption that postings follow the same distribution as authorizations. This validity cannot be confirmed in that no time stamp for postings is available (only for that of authorizations). The concurrent validity is not going to be assessed due to this constraint (i.e. the extent to which a measure is related to another measure (the criterion) when both are measured at the same point in time. Construct validity (the extent to which a measure behaves in a theoretically sound manner) will be used within a theoretical framework. The test-retest reliability is the consistency of results of repeated measures to the same respondents. This is assumed in the sampling.

The second sample has content validity and criterion validity (predictive validity). The prediction of current authorization volumes under a stress test can be forecast to increased authorizations as a result of reduced floor limits. The construct validity of the theoretical behaviour of increased authorization traffic due to reduced floor limits is also true. The test-retest reliability is the consistency of results of repeated measures to the same respondents. This is assumed in the sampling.

The fourth sample has face validity and sampling validity (under the ambit of content validity) in that collaboration with experts in the fraud, telecommunications and business strata is a measure of the suitability of this method. The test-retest reliability is the consistency of results of repeated measures to the same respondents. This is assumed in the sampling.

4.7 Data analysis

Sampling

Four samples of data were taken in this research. The first sample pertained to a survey done to determine the attitudes and opinions of respondents regarding floor limits. The second sample was transactional data taken in 2006 to determine the increase in transactions per second in a hypothetical zero floor limit environment. The third sample comprised data from Bankserv (the domestic transaction switch) to ascertain their ability to handle a zero floor limit environment. The fourth sample comprised the stress tests that were performed on Standard Bank's front-end processor to determine whether the capacity to process increased transactions in a zero floor limit existed.

The attitudinal and opinion data comprises a cross-section of the credit card industry in terms of the key role players from a fraud, business and telecommunications perspective. The sample population is largely heterogeneous as already mentioned. The researcher has applied a judgmental sampling method to ascertain the motives behind the various schools of thought posited in chapter 2. The insight of the sample population would contribute to the rationale for adopting zero floor limits and the limitations that are supposed by the various theorists. The aim of the survey is to obtain the views from a broad range of credit card industry participants and discredit the myths attributed to the telecommunications fallibility in South Africa.

The second sample that comprised transactional data from Standard Bank's data warehouse was taken to determine the theoretical increase in authorization traffic had a zero floor limit been imposed. This will be compared with the ability of Standard Bank's front-end processor (the Postillion) and ancillary systems via a stress test to determine whether the system architecture could handle the theoretical increase in authorization traffic.

The Bankserv and stress test sample comprised a convenience (chunk) sample as the sample was done on the basis of being readily available.

Sample 1: Attitudinal survey

A five-point Likert scale was used to determine the attitudes and opinions of people associated with the credit card business to determine their disposition regarding credit card fraud and floor limits. The survey instrument is attached in Appendix 2.

2. The intention of the researcher was to obtain attitude and opinion data pertaining to the various schools of thoughts proposed by the researcher in Chapter 2 namely:

- The technology school of thought
- The fraud school of thought
- The operational school of thought

The questionnaire was designed in that the three proposed schools of thought were categorized within sections A, B and C.

The data set comprised the following format:

Units of analysis	**Variables**			
	Question 1	Question 2	Question 3	Question n
Respondent 1				
Respondent 2				
Respondent 3				
Respondent n				

The data that was collected was primary data which was collected with a specific purpose in mind, i.e. to test the attitudes and opinions of the various schools of thought. The data was cross-sectional in nature in than it comprised the respondents viewpoints at one particular time. The data is ordinal in nature and the intention is to record the mode of the data concerned.

The nature of the sample was that of a non-probabilistic sample. Practical considerations affected the choice of this sampling method. A suitable sampling frame would have been too time consuming and costly to obtain. The researcher had the aim of obtaining a “broad view” of the population that are largely heterogonous in nature. A convenience

sampling method was thus adopted (sampling members were chosen on the basis of their being readily available and accessible to the researcher).

The following groups of respondents are being surveyed (the sample population):

- Fraud Managers from various local banks, namely:
    - ABSA
    - First National Bank
    - Standard Bank
    - Nedbank
    - Investec
    - Mercantile Bank of Lisbon
- Fraud representatives from the Card Associations
    - MasterCard
    - Visa
- Managers from the Merchant Services functional area in Standard Bank.
- Standard Bank technical personnel in the IT and telecommunications field.
- Computer Software Consultants that install point-of-sale software
- Fair, Isaac, (a vendor of fraud predictive and analytic software based in the USA)
- Retail Decisions (a vendor that manages the industry hot card file (INCF)) and is involved in telecommunications with large retail outlets.
- Fastnet (the vendor that supplies radio pads to merchants for microwave transmission to the acquirer)
- XLink (the vendor that supplies GPRS solutions to merchants for transmission to the issuer)
- Connectnet (the vendor that supplies GPRS solutions to merchants for transmission to the issuer)

The sampling method is a non-probability sample and to reduce bias (selection error), a judgmental sample was used (sample members were chosen on the basis of the researcher's judgment as to what constitutes a representative sample for the population of interest). This judgmental sample includes fraud personnel from local banks, Card Associations, Telecommunication service providers and merchant services personnel).

There is a degree of heterogeneity in the sample as homogeneity with fraud staff would undoubtedly lead to bias.

The sample size is 30 people from the categories mentioned above. 50 Questionnaires will be sent to potential respondents for completion.

The company which the respondents worked for was coded along a nominal scale. This technique was used to assess whether the attitudes per organization were homogenous which was expected by the researcher due to the collaboration between the respondents in the normal course of work. The nominal scale that was applied to the various organizations is as follows:

Respondent	Respondent Classification
Standard Bank Fraud	1
ABSA Fraud	2
First National Bank Fraud	3
Nedbank Fraud	4
Investec Fraud	5
Mercantile Bank of Lisbon Fraud	6
MasterCard Fraud	7
Visa Fraud	8
Standard Bank Merchant Services	9
Retail Decisions	10
Fair, Isaac	11
Connectnet	12
Diners Club Fraud	13
CSC	14
MasterCard Operations	15
Standard Bank Front End	16

The classification technique used was as follows:

	1	2	3	4	5
Question 1 (Section A): The local telecommunications infrastructure (telephone, radio pad or GPRS) from the point of sale to the issuing bank during an authorization request have the ability to sustain a zero floor limit.					
Question 2 (Section A): TELKOM is a reason for not adopting zero floor limits.					
Question 3 (Section A): The reduction of floor limits will not have a negative impact on cardholders at the point of sale					

Question 4 (Section A): Local **issuers** have the technological capacity to entertain a zero floor limit environment in terms of handing an increase in authorization requests					
Question 5 (Section A): Local **acquirers** have the technological capacity to entertain a zero floor limit environment in terms of handing an increase in authorization requests					
Question 6 (Section A): An increase in authorization volumes attributable to a zero floor limit will adversely affect issuers in their ability to process the transactions.					
Question 7 (Section A): An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions					
Question 8 (Section B): Issuers and acquirers can wait for the full implementation of EMV as a solution to reduced fraud					
Question 9 (Section B): Below floor-limit credit card fraud is a cost of doing business on a credit card and is controllable in your institution					
Question 10 (Section C): Reduced floor limits will increase merchant's operational (telephony) costs as they have to now pay extra for the authorization request. This cost is greater for the merchant that the cost of charge backs and voucher retrievals.					
Question 11 (Section C): Floor limits should be incrementally decreased based on credit card fraud at certain merchant categories					

The Likert scale comprised the following value labels:

5 = Strongly agree

4 = Agree

3 = Neither agree nor disagree

2 = Disagree

1 = Strongly disagree

The number of surveys distributed totaled **50**

The number of responses received comprised **33**

The number of responses not received comprised the difference which was **17**

The response rate thus equates to **66%**

Sample 2: Transactional data

The second sample was taken from Standard Bank's data warehouse in order to confirm the following hypothesis as mentioned earlier:

H_0: There is no difference between the observed and theoretical distributions of transactions in a zero floor limit environment.

H_1: There is a difference between the observed and theoretical distributions of transactions in a zero floor limit environment.

The intention of the researcher was to compare the actual distribution of transactions against theoretical distributions of transactions to ascertain whether there was a substantial increase in authorization transactional data and compare this to the processing capability of Standard Bank's front-end processor. This analysis could not be performed as a date and time stamp would be necessary for posted transactions. Date and time stamps were only obtainable for authorized transactions. Posted transactions (i.e. those that were below the merchant's floor limit) did not have a time stamp which is a necessary prerequisite to determine the distribution of transactions. The data set comprised the following format:

Authorizations

Units of analysis	Variables			
	Transaction date	Transaction time	Transaction Amount	Authorization or posting
Card Number 1				
Card Number 2				
Card Number n				

Postings

Units of analysis	Variables			
	Transaction date	Transaction Time	Transaction Amount	Authorization or posting
Card Number 1		Unavailable		
Card Number 2				
Card Number n				

This data set refers to facts and comprises secondary data. The data is currently stored within Standard Bank's data warehouse and as such is considered to be secondary in nature. The data is longitudinal in that it represents a multiple time period. The representative sample includes the period January 2006 to December 2006. Probability sampling was used (simple random sampling). A large sample was taken due to the variability and heterogeneity of the population. The data is metric data (ratio) and a parametric test would have been used to test the hypothesis.

CHAPTER 5

5. Research Results

5.1 Introduction

The stress test performed on Standard Bank's front-end processor is detailed below. The objective is to determine whether the capacity to process increased transactions in a zero floor limit exists.

5.2 Test Objectives

1. These tests were performed specifically to test the capacity of the Generic Switch Terminal Application system and to determine the on-line transaction processing capability
2. This test was performed using a specific transaction and volume profile (Included in *Appendix 3*)
3. Unless otherwise noted, transaction rates quoted are stated as an average number of transactions per period
4. The test targets only the relevant Postillion (front-end processor) systems. In order to exclude factors arising from other Standard Bank systems (e.g. mainframe, Tandem) all connections were simulated.

The following table of definition defines the various systems components mentioned in the following test summation:

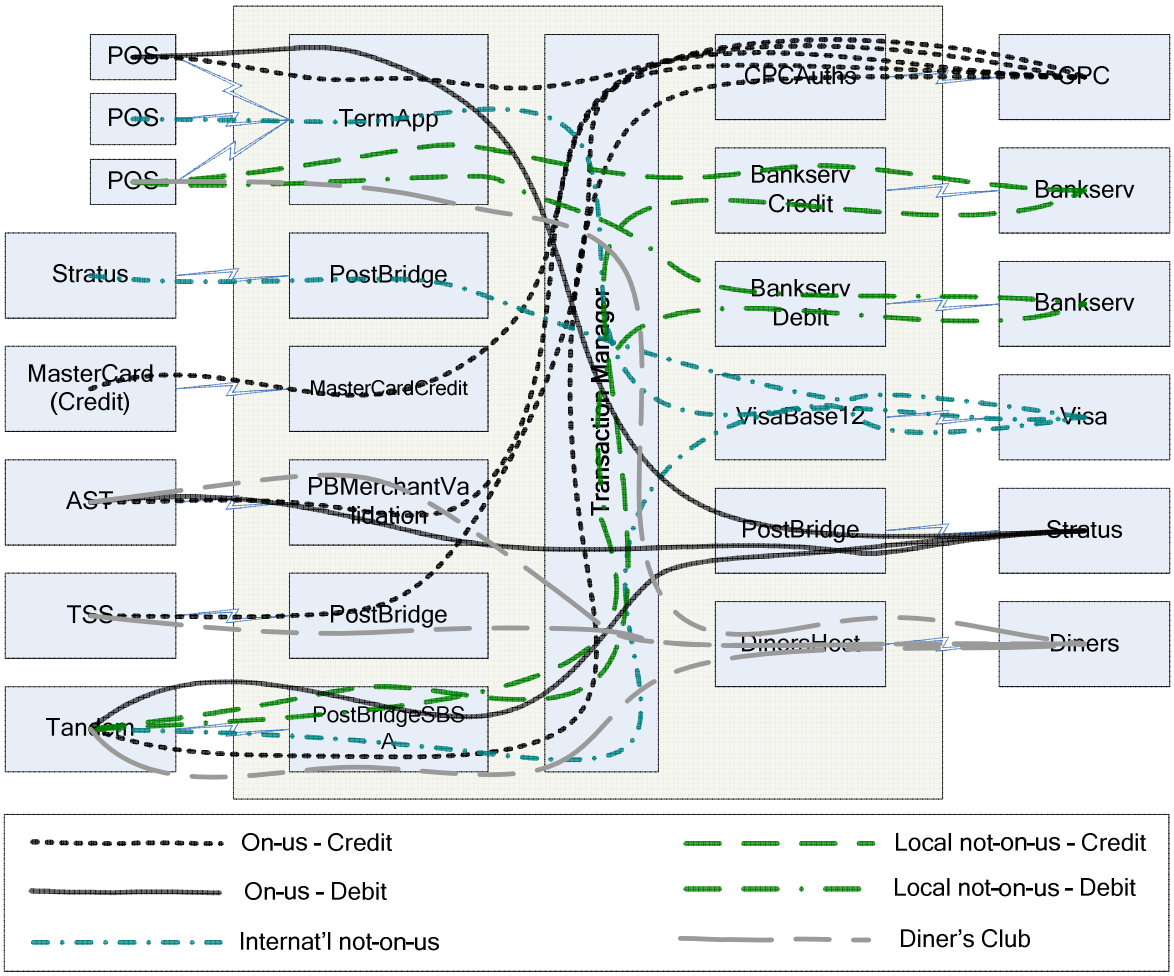
Table 13: Definitions used in the stress test

Term	Definition
CPC	Card Processing Centre – this term is used to refer to the systems that provide services to Card Division
CPC Auths	The system providing on-line authorization facilities to CPC
CPCAuths	Custom interchange handling transactions to and from the credit card authorization system.
CPS	Card Processing System
CPU	Central Processing Unit
Generic Switch	Refers to the Postillion system (Postillion Office and Postillion Real time) currently being used to switch the POS and Credit Card transactions
Interchange	Software entity within Postillion that uses a specific protocol to communicate with an external system. Interchanges can service a Source Node or Sink Node (or both) and are responsible for managing the external connection and translating messages into the internal Postillion format
JVM	Java Virtual Machine
KB	Kilobytes – 1024 Bytes
MB	Megabytes – 1024 Kilobytes
ms	Millisecond – a unit equal to one thousandth of a second
Node	A Postillion entity (consisting of a set of configured rules and parameters) that can be either a transaction source (see Source Node) or a transaction destination (see Sink Node)
not-on-us	Transactions executed at Standard Bank's point of representation but using another issuer's card
on-us	Transactions executed using Standard Bank issued cards and acquired at Standard Bank's points of representation
POS	Point-of-Sale
Postillion	The product name for the Mosaic/S1 software that forms the core of the Generic Switch and which will host the AutoBank and AutoPlus devices when Priora is implemented
Processor	See CPU
remote-on-us	Transactions executed using Standard Bank issued cards but acquired at another institution's point of representation
s	Second – (1000ms)
Sink Node	A node acting as a transaction destination within the Postillion system
Source Node	A node acting as point of transaction origination within the Postillion system.
Switch, the	See Generic Switch
Terminal Application	The S1 product that Standard Bank uses for POS terminal driving (the terminal Source Node). The software provides for management and supply of terminal parameters, authorization of terminal transactions and collection of batched terminal data
Terminal	Refers to a point-of-sale terminal used to acquire credit and/or debit card transactions, e.g. Standard Bank's Dione terminals
TPS, TPS	Transactions per second – the average number of transactions over a 1 second period
Transaction Manager (also TM)	The core transaction processor of the Postillion product. Transaction manager provides the central switching and persistence service to Postillion

5.3 Systems architecture

The diagram below depicts the environment to be tested. All transaction sources are shown on the left and all transaction destinations are shown on the right. To execute the test all transactions sources and destinations were simulated using the “Asset” test tool. This tool is a simulator that facilitates test scenarios and transactional volumes.

Figure 32 - Overview of Target Test System



5.3.1 Test 1 – Methodology

1. The highest overhead on the system emanating from a terminal source is the ‘banking’ session. The system’s ability to service a given population is thus

determined to a large extent by its ability to handle bulk ‘banking’ by the merchant’s point-of-sale , which consists of:

a. Parameter downloads
b. Transfer of the point-of-sale’s terminal’s batch of transactions
c. Download of “hot” card data
d. Download of card data
e. Download of EMV parameters
f. Download of miscellaneous other parameters

2. The vast majority of terminals perform this task during off-peak transaction hours (with high concentrations between 21:00 and 22:00 and 01:00 and 02:00).

3. The test determines the load on the system as follows:
    a. Transaction injectors sustain a background transaction overhead of 4 TPS to reflect the off-peak transaction volumes experienced on the system:
        i. 2 TPS from Terminal Application
        ii. 2 TPS from all other sources

    b. The Terminal Application simulator connects to Postillion (front-end processor) to perform banking. The simulated terminal represents the average point-of-sale device in the population:
        i. The card file is up to date (no download required)
        ii. The “hot” card file is one update behind which requires several insert and delete update blocks
        iii. The “hot” card update response from the terminal is deliberately extended using contrived delays to mimic the behaviour of terminals prior to version 62 (a version of software). This increases session concurrency dramatically
        iv. The EMV (card chip parameters) file is up to date (no download required)
        v. Each batch contains 20 transactions

    c. 5 scripts are executed to simulate banking:

i. Each script creates 80 concurrent terminal banking sessions for a total of 400 concurrent sessions which are sustained for the duration of the test

ii. Scripts are executed in an endless loop so that the desired load levels are sustained

4. The number of concurrent banking sessions was increased until average total system CPU utilization reached 50% at which point no further load was added.

5. Tests ran from 13:10:03 to 15:18:00 (elapsed time 02:07:57).

6. 24132 terminal banking sessions were successfully completed (a rate of 12841 per hour)

5.3.2 Test 1 – Results

1. Testing established a significant capacity surplus between current production volumes and that required to increase average CPU usage to 50%.

2. At this load level the system was processing more than 6 times as many banking sessions per hour as the highest recorded production peak. Intra-day spikes above the tested levels would also be easily absorbed by the unused capacity.

3. At a rate of 12841 terminals per hour the system is capable of servicing a considerably larger population of terminal devices than the current production count of just over 30000 devices:

    a. With 12 bankable hours per day the system is capable of servicing approximately 154096 banking sessions per day. This rises to 308193 for 24 bankable hours

    b. On average, terminals bank between 2-3 times daily. A 12 hour banking day therefore equates to a population of 61638 terminals. A 24 hour banking day equates to 123277 terminals.

4. The effect of increased volumes of banking on Terminal Application had a negligible effect on the rest of the system

Table 14 below contrasts peak activity in a production environment with the levels achieved during this stress test. The column "Factor" contains a multiplier indicating the magnitude (read as "number of times greater than live") of the tested results.

Table 14: Live vs. Tested Peaks (Terminal Application)

Test Scenario	Live	Tested	Factor
Maximum number of concurrent terminals banking	Not available	247	Not Available
Highest number of terminals banking in 1 minute	125	290	2.32
Highest number terminals banking in 1 hour	2118	12841	6.06
Transactions per second (emanating from Terminal Application)	15.4	163.5	10.62

The following sections contain a detailed analysis of the results using metrics from the system.

Figure 33: CPU Usage vs. Terminal Banking Load

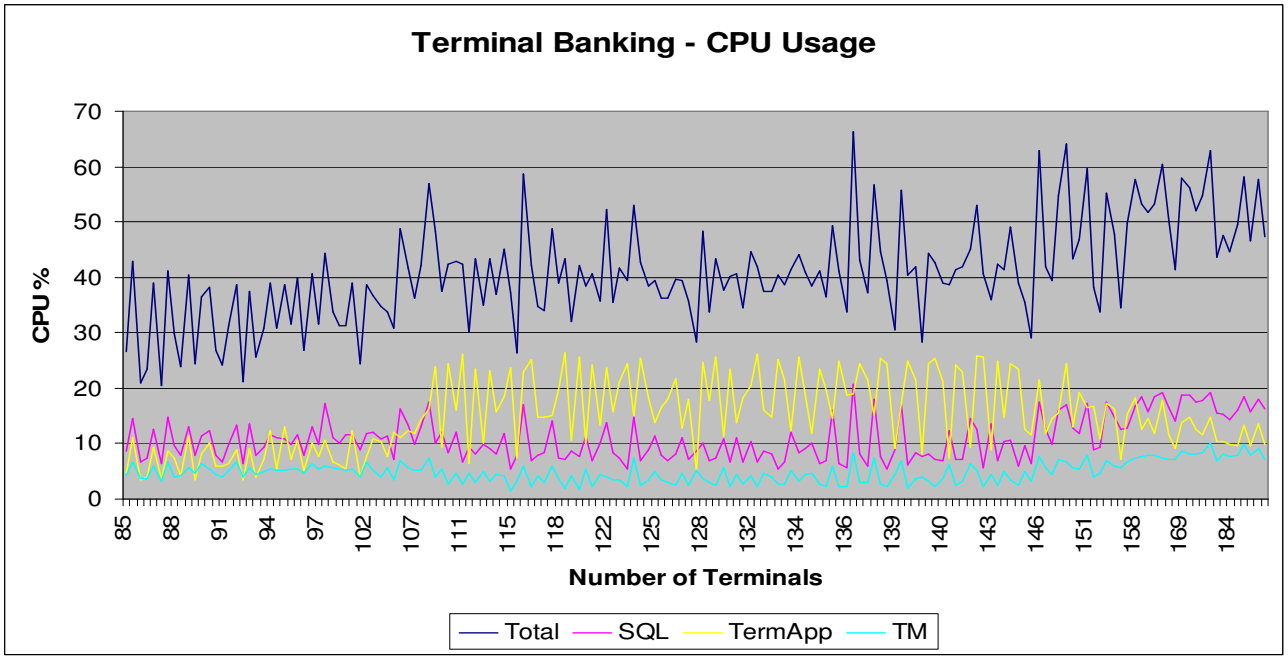


Figure 33 shows the relationship between CPU utilization and terminal banking activity. Total CPU usage rises as the number of concurrent devices increases. The artifact visible in the middle section of the graph (where Terminal Application's usage rises above 20%) is caused by an increase in the number of hot card downloads which form part of a typical banking session. With usage averaging 50% no problems were recorded.

5.3.2.1 Response Times vs. Terminal Banking Load

The response times reflected here are a measure of the level of service given by the system to the originator of a transaction. Since the response time includes the time taken for an upstream entity to authorize a transaction (e.g. on average 610ms for Bankserv), the actual values are less important than the effect of increased banking load on the response times.

Figure 34: Response Times vs. Terminal Banking

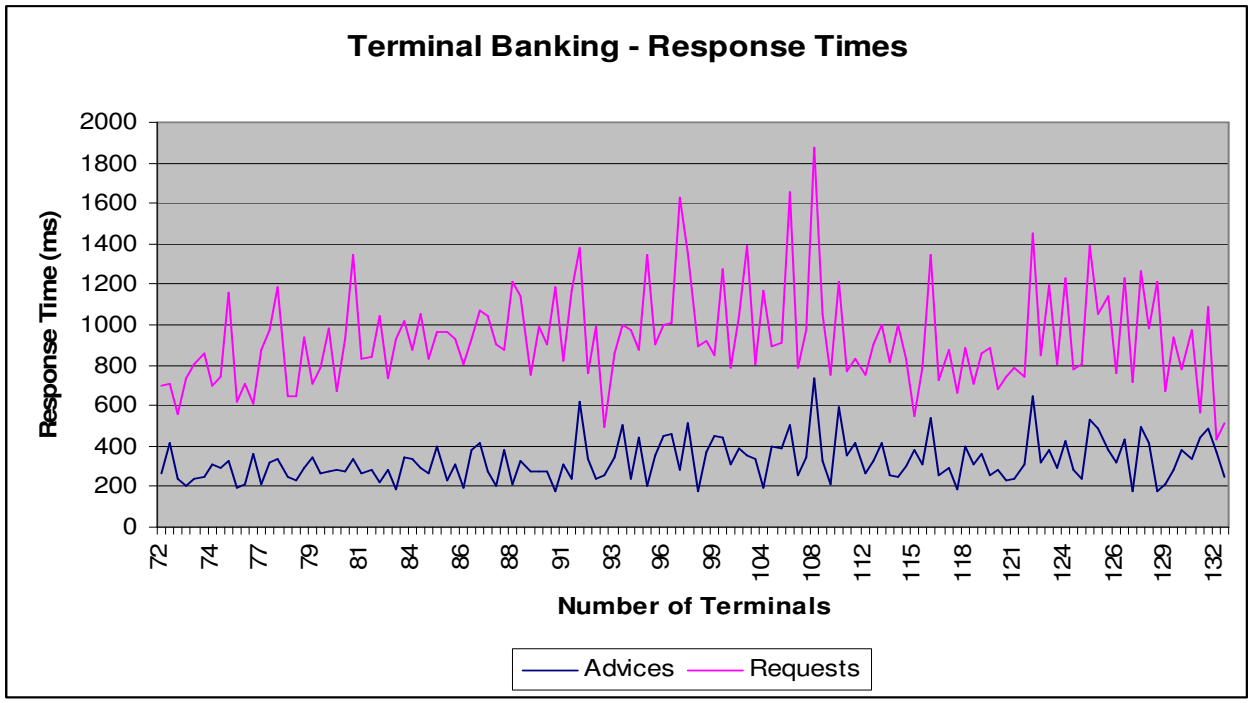


Figure 34 shows a small increase in response times as concurrency increases. This behaviour is expected. Request response times (which are passed on-line) show greater variation which is caused by varied response times from multiple authorizing systems.

Advice messages are handled as store-and-forward messages – the result is a more stable response time profile. An Advice is a message that is sent when a point-of-sale banks its transactions. An authorization request is an on-line authorization request from the merchant's point-of-sale (i.e. the transaction exceeds the merchant's floor limit).

5.3.2.2 Queue Processing vs. Terminal Banking Load

Postillion implements a queued processing model whereby events (e.g. "connect", "data message", "status update") are queued between modules and system participants. The following aspects of the queue processing are measured here:

- Queue depth – an increasing queue depth indicates that the system is not processing events as quickly as they are arriving – a backlog thus exists.
- Event processing time – a measure of how quickly events are being processed.
- Event queued time – a measure of how long (on average) events are queued before being processed.

Source Node Queue Processing

This section details the effect of terminal banking on the system's ability to handle incoming high banking concurrency. The next section will deal with the effect on Transaction Manager.

Figure 35: Source Node Queue Handling vs. Terminal Banking

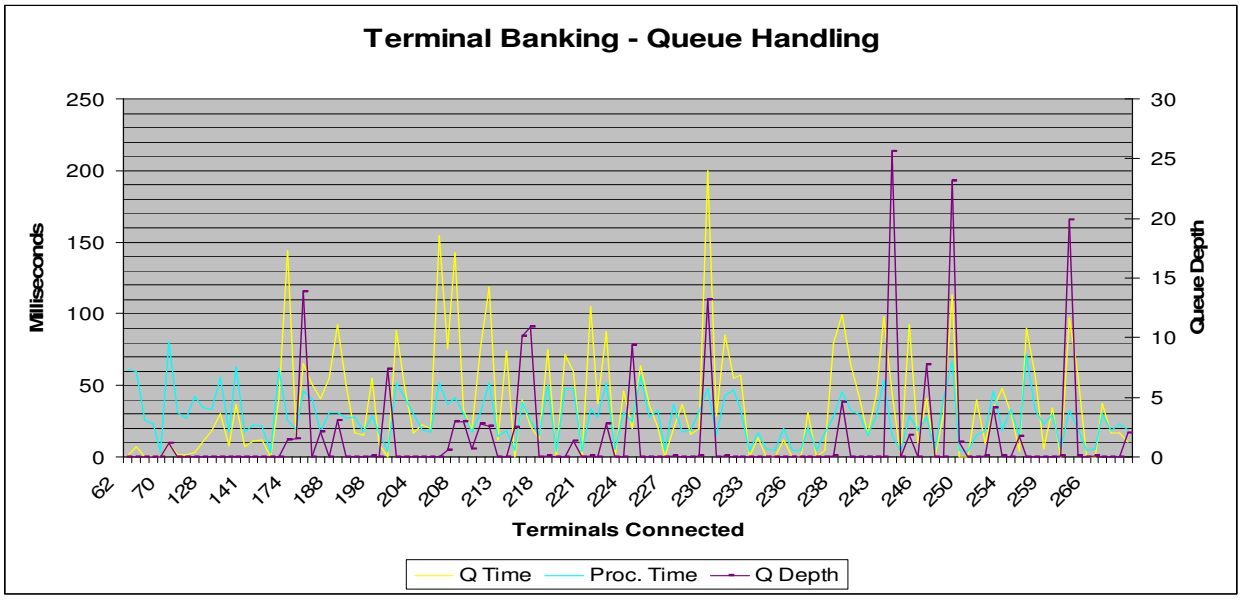


Figure 35 shows that throughout testing Terminal Application's queue handling experienced no problems whatsoever. Event handling was extremely fast (on average below 50ms) with source node event queue depth (on the secondary Y axis at right) at minimal levels. An increase event queued time was recorded as expected. The increase was negligible.

Transaction Manager Queue Processing

Transaction Manager forms the core of the Postillion transaction processing engine. A negative effect on its ability to process will have a knock-on effect for other transaction sources and destinations.

Figure 36: TM Queue Handling vs. Terminal Banking

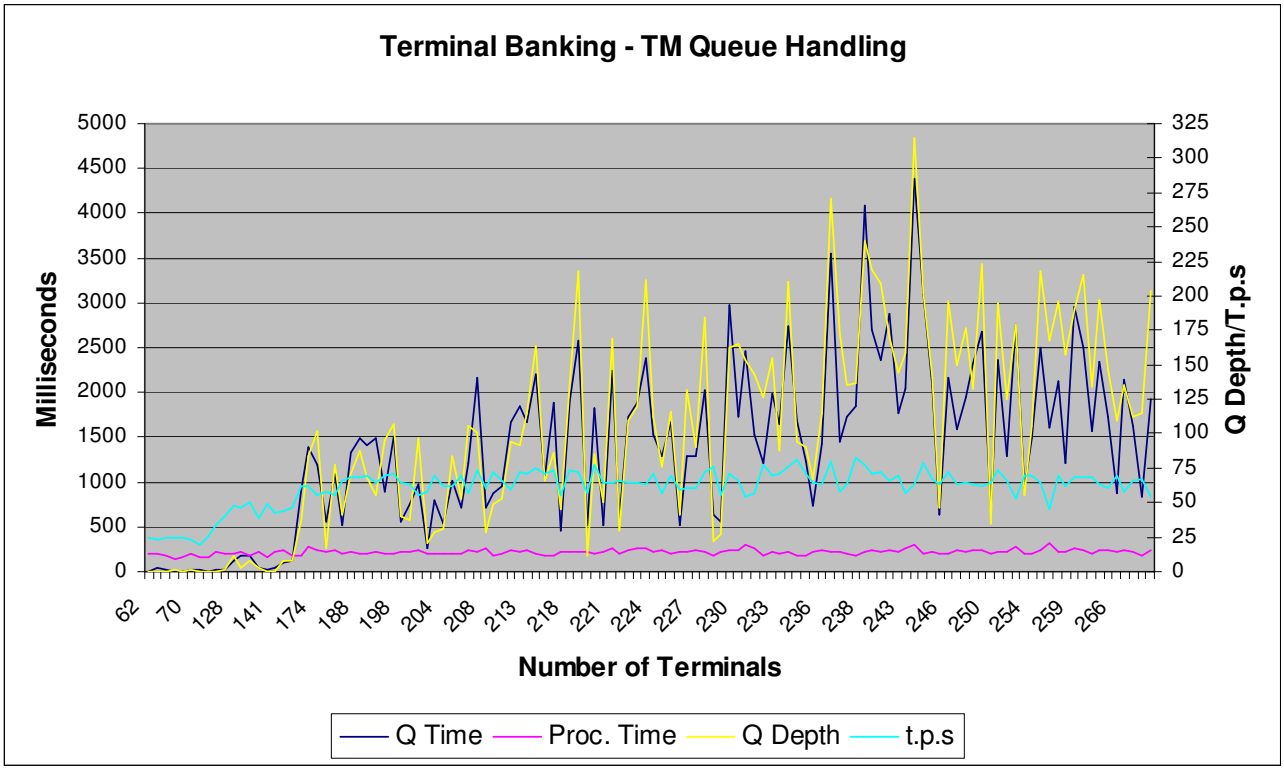


Figure 36 above shows the effect on Transaction Manager. There is a negligible increase in event processing time. The event queue length and event queued times increase as the number of transactions banked per second rises towards the transaction capacity threshold of approximately 65 TPS. Event processing time and queued time varies considerably from moment to moment. This is a relic of the batching process where a single batch message from the terminal is translated into multiple incoming

transactions with resultant bursts of transaction activity. This phenomenon also accounts for the intermittent spikes in internal queue depth (on the secondary Y axis at right).

From 240 devices onwards the average time an event spent in the queue regularly exceeded 2 seconds. This level of concurrency is equivalent to 9600 devices per hour which is approximately 4.5 times higher than the highest number of terminals banked in one hour in production. There is thus scope for higher concurrency before these levels are reached where the effect on processing queues is noticeable but does not result in loss of service.

5.4 Test 2 – Determine Online Transaction Capacity

This test sets out to determine the maximum sustained transaction rate that can be supported by the Postillion system. The simulated environment was configured to reflect the transaction profiles determined by *Appendix 3*.

5.4.1 Test 2 – Methodology

1. A background Terminal Application load was generated by simulating 15 terminals constantly performing a banking session (including parameters, hot card download etc.). This equates to approximately 620 banking sessions per hour.

2. The Terminal Application and other source node simulators injected transactions into the system at predetermined rates (per *Appendix 3*).

3. Additional terminals were added to the system in groups of 80 to perform online authorizations.

4. Non-Terminal Application source nodes slowly increase their rate of transaction injection in a stepped fashion.

5. The number of transactions was increased until the average CPU load on the system exceeded 90% and Postillion started showing signs of stress.

6. Once the break-point had been reached the transaction load was gradually reduced to test the system's ability to recover.

7. Tests ran from 13:50:47 to 15:09:48 (elapsed time 01:19:01).

8. Over 409000 transactions were executed during this period.

9. The highest average transaction rate over a 5 second period was 141 TPS.

10. The highest average transaction rate over 1 minute period was 106 TPS.

5.4.2 Test 2 – Results

1. There is sufficient memory capacity to perform well above the levels at which CPU capacity was reached.

2. The following significant boundaries were encountered:
    a. CPU reached 60% utilization at 70 TPS.
    b. Response times degraded significantly after 88 TPS.
    c. Terminal Application's internal event queue remained constant until 65 TPS.
    d. Transaction Manager's event queue remained constant until 65 TPS (at approximately 60% CPU utilization).

3. The system was able to recover from its over-stressed state without intervention. Service was restored to normal as soon volumes returned to sustainable levels.

The results show that the system has three performance 'zones':

- Comfort – Up to 65 TPS the system performs optimally with no degradation in service. The system is capable of easily absorbing transient spikes of over 100 TPS.

- Stressed – Up to 88 TPS where the system is performing under stress. Response times have degraded (by up to 200%) and reduced service is

being offered with some transactions being discarded as volumes grow towards 88 TPS. Transient volume spikes will temporarily decrease the grade of service further.

- Over-stressed – Over 88 TPS where performance is severely retarded. System behaviour is erratic with response times between 200% and 800% worse than those experienced at 65 TPS.

As of 9 November 2006 the busiest day in production was 28 October 2006 with 846,681 transactions during the day. 76,647 transactions were recorded during the peak lunch-time period of 13:00-14:00 on that day, for an average rate of 1277 per minute or 21 per second.

At 65 TPS (in the “Comfort Zone”) the system is capable of 3,900 transactions per minute or 234,000 per hour – approximately 3 times higher than the peak volumes thus far experienced in production.

A hardware upgrade (increase in available CPU capacity) will be required before transactions rates of more than 65 TPS can be sustained for periods exceeding a few minutes.

Resource Usage

The graph below reflects the key resource indicators for the duration of the test. The transaction rate is shown contrasted with CPU usage, available memory and context switches.

Figure 37: Test Indicators, Resource Overview

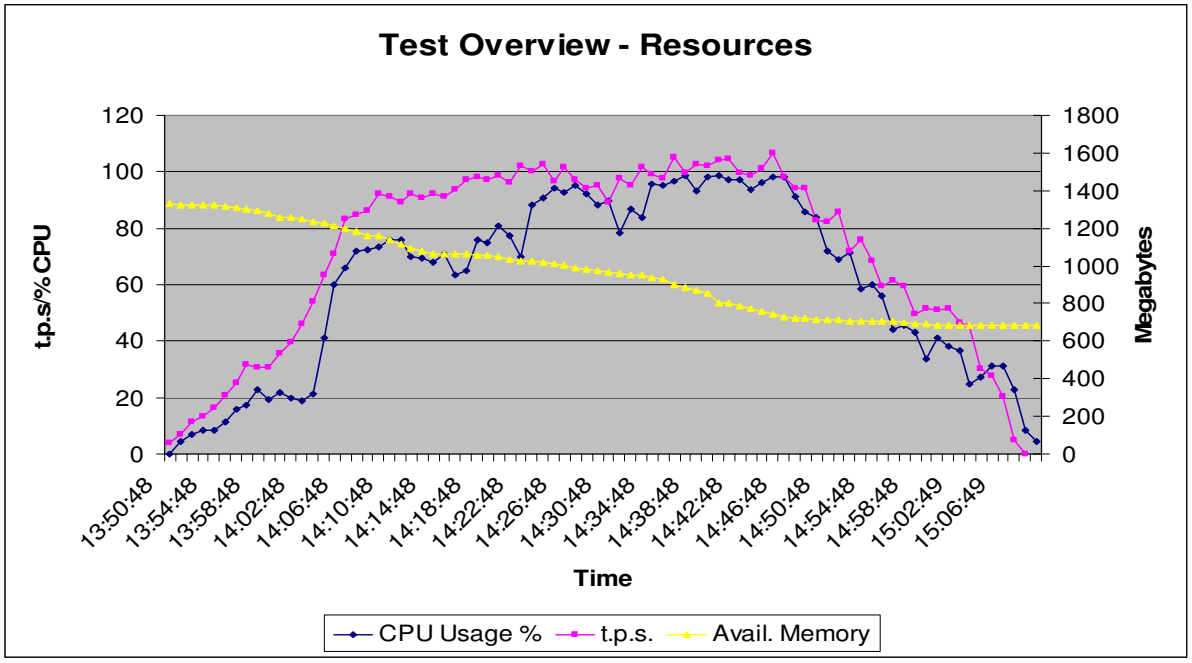


Figure 37 above reflects CPU usage and TPS rate on the on the primary Y-axis at left and available memory on the secondary Y-axis at right.

The following general comments may be made:

1. The system was unable to exceed an average sustained transaction rate past 106 TPS (although spikes well in excess of 106 TPS were noted at various stages).

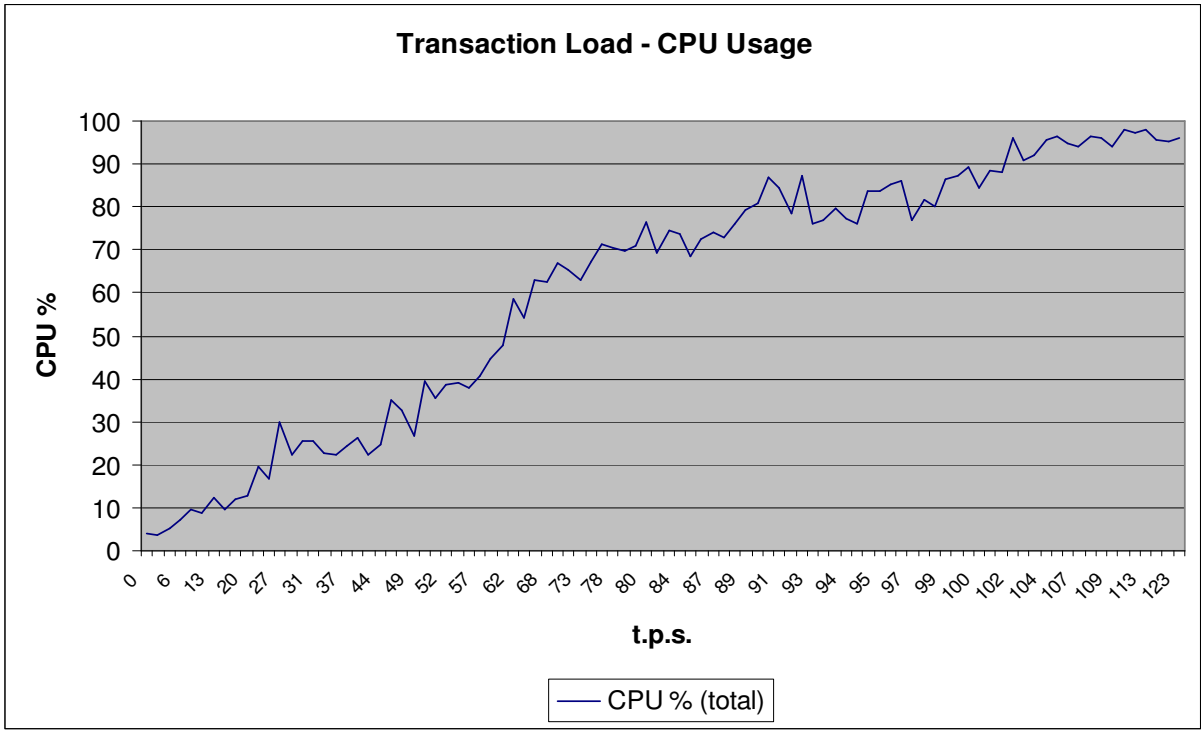
2. The primary constraint on the system is CPU capacity – CPU usage reached 60% when the average transaction rate (taken over 1 minute) exceeded 70 per second. At 89 transactions per second the CPU usage was 75%, and at 102 transactions per second CPU usage was 90%. The CPU processor queue depth started exceeding 8 (anything more than 2 per CPU indicates processor backlog) at approximately 66 TPS.

3. No memory problems were noted – available memory dropped from 1330MB to 688MB.

CPU Usage vs. Transaction Rate

Figure 38 shows the relationship between CPU utilization and the transaction rate. The CPU usage on the system increases as the transaction rate increases.

Figure 38: CPU Usage vs. Transaction Rate

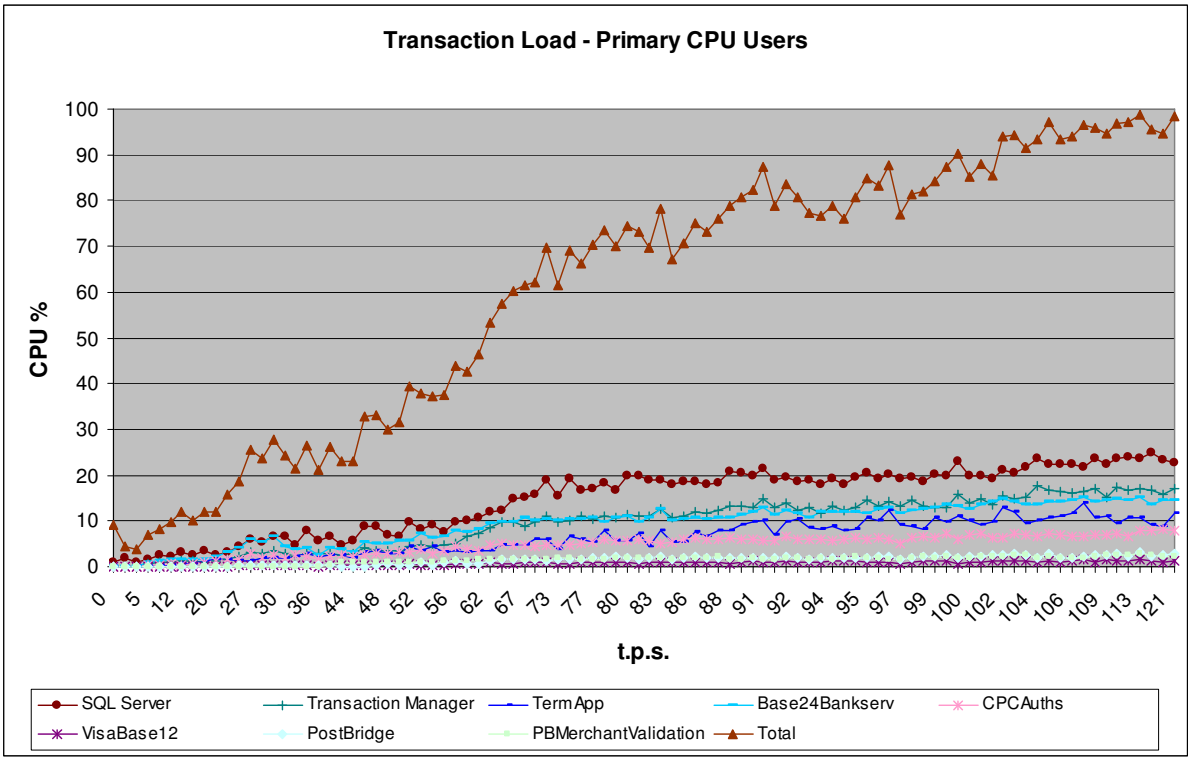


CPU utilization reached 50% at 62 TPS, 60% at 70 TPS, 70% at 80 TPS, 80% at 90 TPS and 90% at just over 102 TPS. If the upgrade threshold for CPU utilization is assumed to be 60% (midway between a conservative 50% and the traditional value of 70%) then the maximum transaction capacity of the Server 5600 is 70 TPS.

Primary CPU Consumers

Figure 39 below contrasts CPU usage by application against the transaction rate.

Figure 39: Primary CPU Users



As expected, the following are the top users:

1. SQL Server 2000 – the database accounts for the highest overhead since almost every transactional operation requires database access.
2. Transaction Manager –each transaction must pass through Transaction Manager.
3. Base24Bankserv – highest volume in terms of source and sink transactions (acquiring and issuing transactions).
4. Terminal Application – performs additional tasks and is responsible for the highest origination of transactions on the system.
5. CPCAuths – all on-us credit card authorizations are authorized via this node.

The host-to-host applications (PBMerchantValidation, PostBridge, and PostBridgeSBSA) and the Visa and MasterCard nodes do not add significant overhead.

Response Times vs. Transaction Rate

The response times reflected here are a measure of the level of service given by the system to the originator of a transaction. Since the response time includes the time taken

for an upstream entity to authorize a transaction (e.g. on average 610ms for Bankserv), the actual values are less important than the effect of increased banking load on the response times.

Figure 40: Response Times vs. Transaction Rate

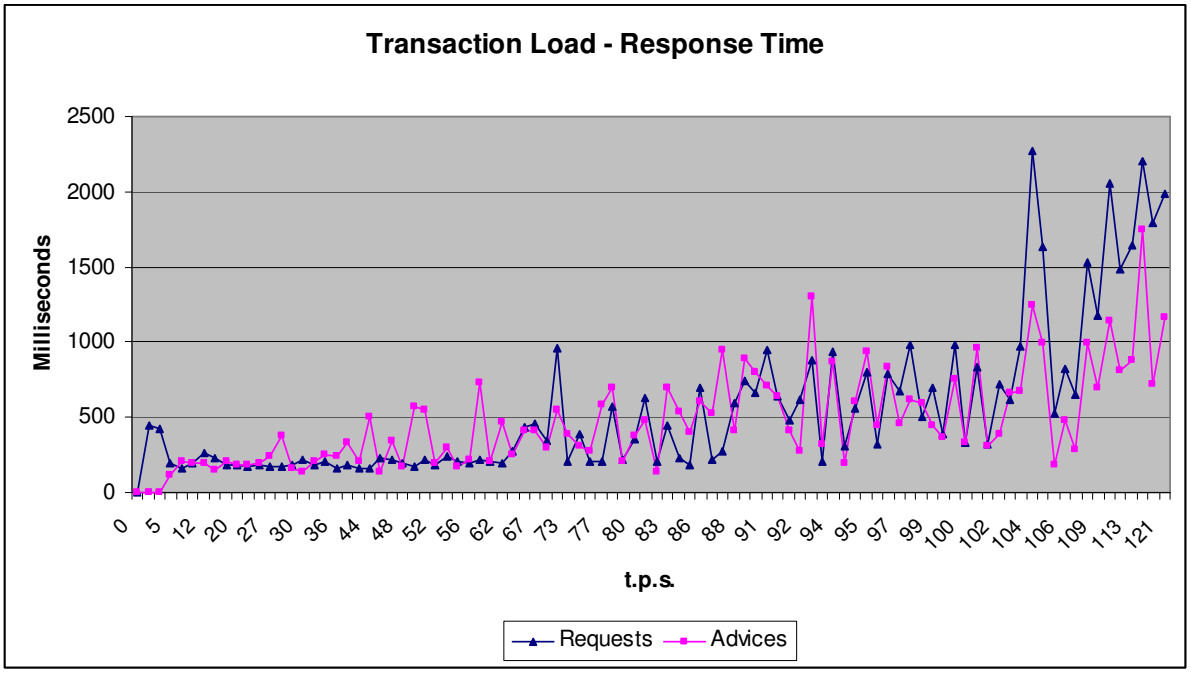


Figure 40 shows a clear upward trend in response times as the transaction load increases, especially for request transactions (these are on-line requests and have the greatest impact on customer service – advices are handled in store-and-forward queues and are typically system generated. Advices also have a lower delivery priority).

Response times were affected as follows:

1. An average of 250ms was sustained until the transaction rate reached 62 TPS.
2. For rates greater than 62 TPS response times became more erratic but remained within acceptable bounds of 250-500ms until the transaction rate reached 88 TPS.
3. For rates greater than 88 TPS response times were between 100% and 200% worse than at 62 TPS.
4. For rates in excess of 100TPS response times had degraded by approximately 640% and showed wild fluctuations.

It should be noted that the data reflects sustained transaction rates. Transient spikes in transaction activity above the thresholds of 62 and 88 TPS will be handled by the system without significant overall degradation

Queue Processing vs. Transaction Rate

Postillion implements a queued processing model whereby events (e.g. “connect”, “data message”, “status update”) are queued between modules. The following aspects of the queue processing are measured here:

- Queue depth – an increasing queue depth indicates that the system is not processing events as quickly as they are arriving – a backlog exists
- Event processing time – a measure of how quickly events are being processed
- Event queued time – a measure of how long (on average) events are queued before being processed

The only applications that experienced problems with their internal queues were Terminal Application and Transaction Manager. *Figure 41* below illustrates the relationship between increasing transaction volume and queue depth for these applications.

Overall Queue Processing

Figure 41: Event Queues vs. Transaction Rate

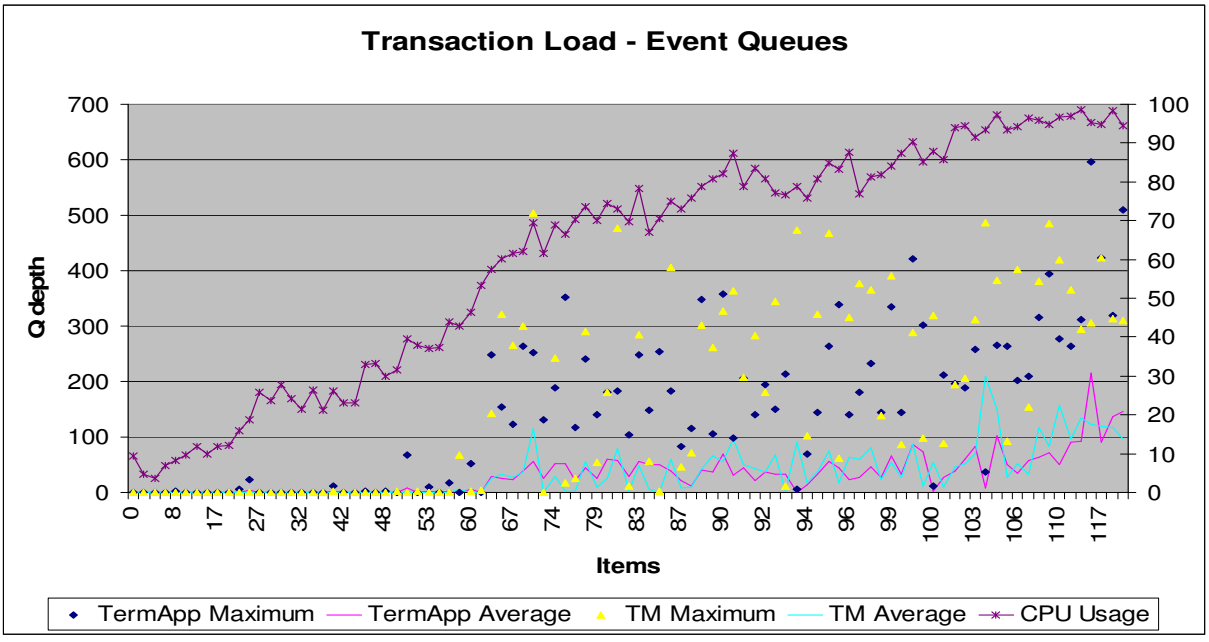


Figure 41 shows the queue depths for Terminal Application and Transaction Manager. Average queue depth (which reflects the overall state of the queue) is represented by solid lines and maximum queue depth (which reflects the momentary state of the queue) is represented by scatter points. The following is noted:

1. Terminal Application
    a. The internal queue shows intermittent spikes of up to 68 until the transaction rate reaches 65 TPS. These are attributable to terminal banking sessions and normal groupings of Terminal Application originated transactions which combine to cause a fleeting event spike
    b. For rates over 65 TPS the internal event queue manages to remain below 100 (with momentary spikes of up to 263) until the rate reaches 74 TPS
    c. For rates above 74 TPS the average queue depth fluctuates significantly with unacceptably high spikes exceeding 250 events

2. Transaction Manager
    a. The queue is stable (zero depth) until 58 TPS where the first transient spike is noted – this is not problematic
    b. Above 64 TPS the queue begins average more than zero with spikes to 322 events, and begins to fluctuate significantly
    c. Unacceptably high spikes (consistently 300 or above) are noted from 71 TPS onwards (with the worst value of 500 exactly occurring at 71 TPS)

CPU usage was approximately 60% when the queues experienced problems.

Transaction Manager Queue Processing

Transaction Manager forms the core of the Postillion transaction processing engine. A negative effect on its ability to process will have a knock-on effect for other transaction sources and destinations.

Figure 42: TM Queue Handling vs. Transaction Rate

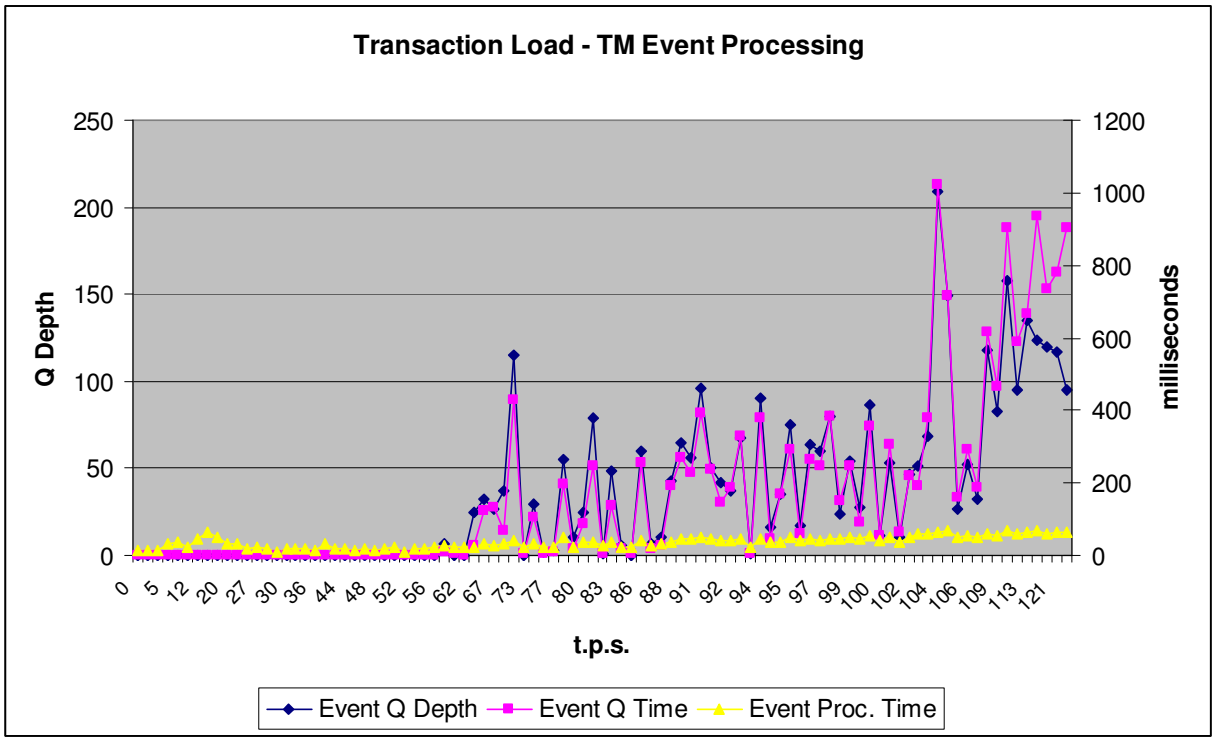


Figure 42 shows the effect on Transaction Manager.

1. As previously noted, TM's queue starts to exhibit unstable behaviour after 64 TPS
2. From 65 TPS onwards the average time spent in the queue by each element increases erratically but in lock-step with the event processing time
3. Event processing time begins to regularly exceed 100ms from 65 TPS

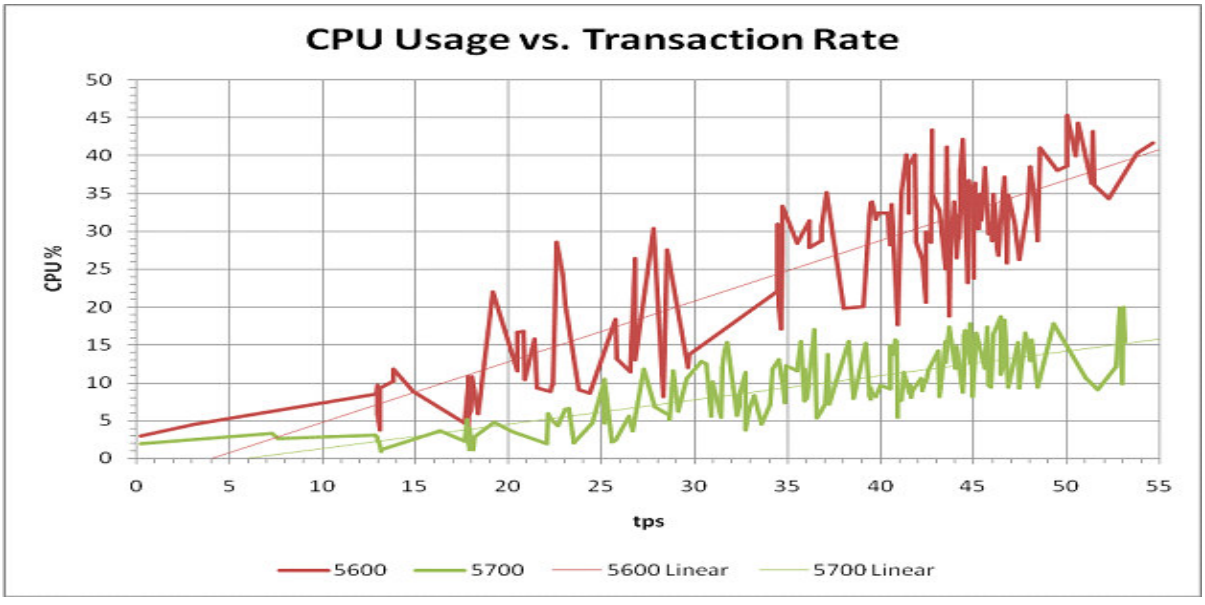
Interview

An interview was held with the Manager of Standard Bank's front-end processor and associated applications on the stress test performed by him with the commensurate results. The person being interviewed was Sean Baker (Baker, S, Manager IT Solutions Centre, 2007. Personal interview, 26 April 2007, 5 Simmonds Street, JHB). The following information was forthcoming based on the interview and the stress test results performed in May and June 2006.

Toward the end of 2006, the front-end processor had been upgraded and whereas it was dual processing with a comfort zone of 64 TPS, this figure can be mathematically doubled to 124 TPS as the front-end processor has been doubled in terms of its processing ability (quad processing).

The central processing unit and its processing speed is a key consideration in terms of front-end processing capability. Processing capability would be the most important systematic metric to propose a zero floor limit. The CPU ultimately determines the speed with which the transactions (authorizations are processed) and the load on memory consumption. The following diagram reflects the difference between the processing ability of the front-end processor's CPU prior to the upgrade (dual processing) and that after the upgrade (quad processing).

Figure 43: The difference between the CPU speeds before and after the front-end upgrade.



The red line (labeled 5600) reflects the front-end's CPU usage (as a percentage) versus the transactions per second processing *before the upgrade*. The green line (labeled 5700) reflects the front-end's CPU usage (as a percentage) versus the transactions per second processing *after the upgrade.* One can clearly see that the variability of the old CPU's processing is highly erratic when the transactions per second are increased. This variability is much less with the new CPU usage as more transactions are added to the processor. The Old CPU versus TPS linear slope is steeper than that of the upgraded CPU versus TPS slope. This reflects the ability of the new CPU to process more transactions faster and more efficient than the older CPU.

As part of the research, the researcher prepared the following questions:

1. Did the comfort zone of 62 TPS be reached in a production environment?
2. What was the busiest day on volume of transactions in 2006?
3. Can the upgraded comfort zone accommodate 99 TPS?

Mr. Baker's responses in relation to the questions asked are recorded below:

When Mr. Baker was asked whether the stress-tested comfort zone of 62 TPS (the old CPU processor) had been reached in a production environment, his answer was "*no*".
The busiest day in 2006 which was the historically highest volume of transactions processed was the 22nd December. The following table details the volume of transactions and the average transactions per minute (tpm) and average transactions per second (TPS):

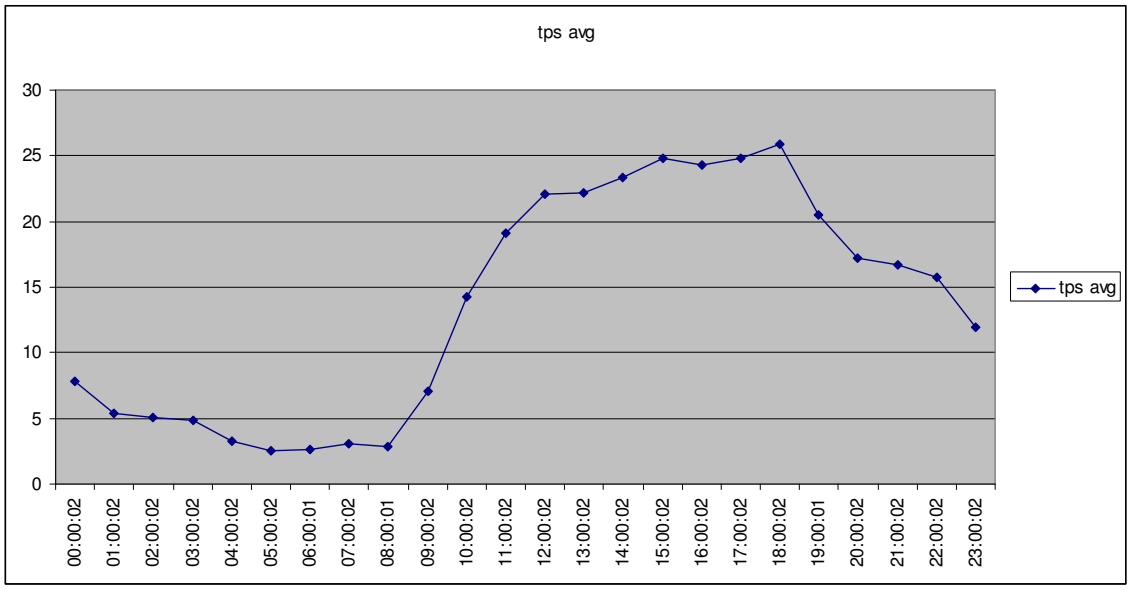
Table 15: The highest transactions ever recorded (December 2006)

Hour	Number of Transactions	TPM average	TPS average
00:00:02	28061	467.6833	7.794722
01:00:02	19358	322.6333	5.377222
02:00:02	18253	304.2167	5.070278
03:00:02	17569	292.8167	4.880278
04:00:02	11674	194.5667	3.242778
05:00:02	9252	154.2	2.57
06:00:01	9685	161.4167	2.690278
07:00:02	10911	181.85	3.030833

08:00:01	10430	173.8333	2.897222
09:00:02	25486	424.7667	7.079444
10:00:02	51517	858.6167	14.31028
11:00:02	69009	1150.15	19.16917
12:00:02	79584	1326.4	22.10667
13:00:02	79931	1332.183	22.20306
14:00:02	84071	1401.183	23.35306
15:00:02	89467	1491.117	24.85194
16:00:02	87293	1454.883	24.24806
17:00:02	89528	1492.133	24.86889
18:00:02	93142	1552.367	25.87278
19:00:01	73644	1227.4	20.45667
20:00:02	61831	1030.517	17.17528
21:00:02	60185	1003.083	16.71806
22:00:02	56583	943.05	15.7175
23:00:02	42943	715.7167	11.92861

The highest average TPS was at 18:00:02 at 26 TPS. The following run chart illustrates the volumes processed (average TPS):

Figure 44: The highest transactions ever recorded (December 2006)



Mr. Baker was asked whether the following mathematical assumption can be applied to ascertain the processing ability of the front-end processor after the upgrade:

- Highest TPS achieved in production: 25 (1500 transactions per minute)
- Comfort zone of old processor (TPS): 62 (3720 transactions per minute)

- Upgraded comfort zone (double the old processing speed) : 124 (7440 transactions per minute)
- Difference between the highest TPS achieved in production and the new processing capability :**99 (5940 transactions per minute)**

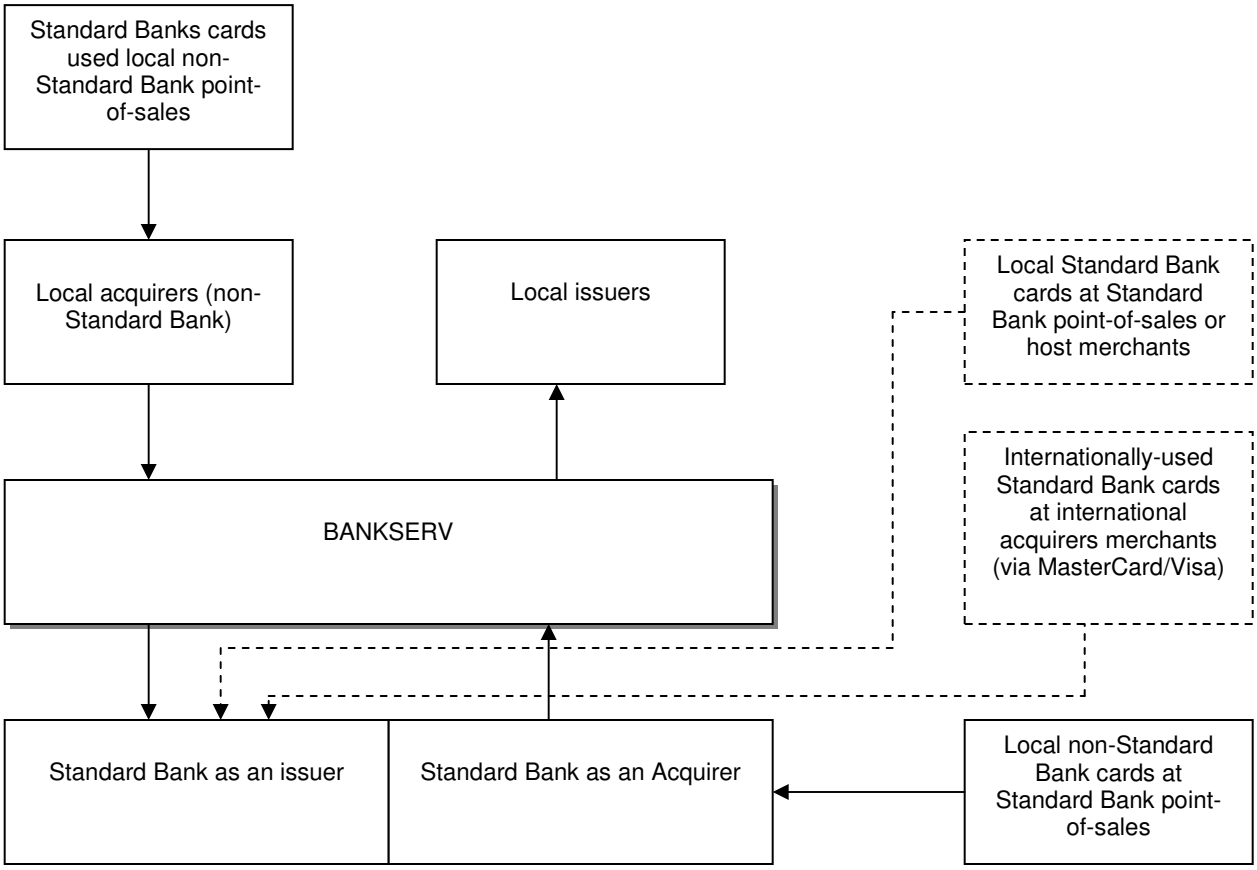
Mr. Baker responded that he supports the logic on a mathematical basis, however, the relationship between the CPU usage, the TPS and system memory consumption is *not linear* (as suggested by the calculations) and cannot be argued mathematically as done above. CPU consumption is positively correlated to memory use and TPS (as shown in the stress test results). Mr. Baker confirmed that the relationship is not linear but rather logarithmic and that no logarithmic scale is available to represent this relationship. He does however, believe that the logic is sound as represented above. In order to unequivocally prove whether the front-end processor can handle a zero floor limit, a stress test (Acid test) must be performed. As mentioned, a stress test (simulator) requires a project to be raised, prioritised and takes approximately 6 weeks of extensive testing. This was confirmed with the test manager within Standard Bank's Group IT. It is due to the considerable cost and time involved that an existing stress test (done in 2006) was used. To develop a simulator to test "what-if" scenarios would not be feasible due to the complexity and variability of the system architectural components and intermediaries. A simple simulation would not be sufficient to cater for all of these actors and concomitant variables and would not adequately prove the ability of Standard Bank's front end processor to handle zero or reduced floor limits.

5.6 Data Analysis – Bankserv

Bankserv is the largest operator (providing infrastructural components) in the South African payment and clearing system. A core function of this organization is the switching of electronic payments between banks (SASWITCH) and the clearing of South African payments systems (http://www.bis.org).

The following analysis was done by meeting with Bankserv and obtaining transactional volumes from them. Bankserv switch all local transactions for local issuers and acquirers based on the following macro-illustration:

Figure 45: Schematic representation of transaction flow



The following illustration positions the role of Bankserv. Bankserv only switch local transactions where the issuers cards used at the transactional channel are not synonymous with the selfsame acquirer. Let's say that a Standard Bank credit card is used at an ABSA merchant, the authorization and settlement will route via Bankserv. In the event that a Standard Bank credit card is used at a Standard Bank merchant, the authorization and settlement will *not* route via Bankserv as this routes directly to Standard Bank. This relationship is illustrated by the non-dashed stakeholders. All international transactions also route to the issuer and do not go through Bankserv. As mentioned previously, all international transactions have a zero floor limit and do not form part of the analysis regarding floor limits per the fourth hypothesis, viz:

Proposition 4:

The fourth Proposition is that local banks infrastructure and technology can accommodate an increase in authorisations as a result of a zero floor limit environment.

The analysis does however, incorporate Standard Bank credit cards used at a Standard Bank merchant. The following analysis needs to be done to incorporate the fourth Proposition which is the impact on authorizations as a result of a zero floor limit on the *industry* and as such needs to incorporate the Bankserv volumes.

The following data was extracted from Bankserv over December 2006 which is traditionally the busiest time of the year for transactional volumes and authorizations: The representative sample thus comprises transactions from 01st December 2006 to 31st December 2006.

Table 16: Bankserv volumes over December 2006

	ATM	DEBIT	CREDIT	TOTAL
DATE	VOLUMES	VOLUMES	VOLUMES	VOLUMES
1/12/2006	1132788	535065	471041	2138894
2/12/2006	843367	563538	547482	1954387
3/12/2006	558647	331876	335379	1225902
4/12/2006	723604	380161	386987	1490752
5/12/2006	608583	383894	401495	1393972
6/12/2006	542454	383883	427263	1353600
7/12/2006	561963	387219	456139	1405321
8/12/2006	736357	443012	496526	1675895
9/12/2006	629299	473825	556261	1659385
10/12/2006	446911	288791	339151	1074853
11/12/2006	492803	336278	399616	1228697
12/12/2006	469781	346904	426944	1243629
13/12/2006	633984	364564	456230	1454778
14/12/2006	579088	395975	476568	1451631
15/12/2006	1067306	628679	542949	2238934
16/12/2006	786545	619647	546654	1952846
17/12/2006	540480	381351	356579	1278410
18/12/2006	672687	500401	492263	1665351
19/12/2006	606174	510236	530060	1646470
20/12/2006	665486	561123	557115	1783724
21/12/2006	746799	600737	590166	1937702
22/12/2006	991703	773516	669577	2434796
23/12/2006	821722	728347	630734	2180803
24/12/2006	593704	517546	398257	1509507

25/12/2006	393687	79003	62055	534745
26/12/2006	475763	212116	178529	866408
27/12/2006	635038	433939	400552	1469529
28/12/2006	570460	412499	402701	1385660
29/12/2006	718713	499912	482451	1701076
30/12/2006	685492	479460	421958	1586910
31/12/2006	567724	322017	295958	1185699
	20499112	**13875514**	**13735640**	**48110266**
Daily average	661261.68	447597.23	443085.16	1551944.1

The highest authorization activity on cards for the month occurred on the 22nd December.

Table 17: CPU average use (%)

MAX TPS	BUSY TIME	CPU AVE %
71.9	**11:45 - 11:55**	**41.64**

Table 17 indicates the maximum TPS and CPU usage. Bankserv have confirmed that their maximum TPS threshold is 156 TPS for one site. Bankserv process authorizations via two separate sites (continuous processing) to balance the load and each site can maintain 156 TPS concurrently (reference: Bankserv). This results in a total TPS threshold of 312 TPS processing capability.

5.7 Data Analysis – Standard Bank

The following data was extracted from Standard Bank's Data Mart for 2006. The data represents all authorizations and postings (transactions that did not come up for authorization and were below the merchant's floor limit).

The posted transactions that did not come up for authorization (below the merchants floor limit) did not have a time stamp to determine the time of the transactions. The authorizations however, (transactions above the merchant's floor limit or transactions originating abroad that have a compulsory zero floor limit) did have the respective time stamp.

Based on these constraints, the following assumptions were made:

- Posted transactions follow a distribution similar to authorization data
- The maximum authorizations per second are equally distributed.

The data results are enclosed *in Appendix 4.*

The data in *Appendix 4* includes the following:

- Total authorization volumes over a representative week (day-on-day) within a month, on a month-on-month basis by hourly bands
- Total authorization percentages over a representative week (day-on-day) within a month, on a month-on-month basis by hourly bands
- Posted transaction volumes over a representative week (day-on-day) within a month, on a month-on-month basis
- Posted transaction percentages over a representative week (day-on-day) within a month, on a month-on-month basis
- Total posting volumes over a representative week (day-on-day) within a month, on a month-on-month basis by hourly bands based on the assumption that floor limits had been zero and postings follow the same distribution as authorizations.

Line charts reflecting the current authorization volumes per representative week, day-on-day per hour (labeled "As-Is") is depicted in the appendix. "What-if" line charts assuming zero floor limits (postings and authorizations) are depicted to ascertain the theoretical increase in authorizations and transactions per second.

With these assumptions, the following theoretical increases in transactions per second are evidenced:

Table 18: Standard Bank transaction increase month-on-month had a zero floor limit been adopted

Month	Increase (%)	Max Authorizations per Second
Jan-06	85%	61
Feb-06	77%	62
Mar-06	70%	62
Apr-06	69%	80
May-06	72%	66
Jun-06	67%	65
Jul-06	65%	77

Aug-06	70%	66
Sep-06	65%	86
Oct-06	70%	70
Nov-06	65%	69
Dec-06	59%	91

Highest theoretical TPS in the event that zero floor limits had been introduced in 2006: **91** (based on the December 2006 peak)

Upgraded comfort zone (double the old processing speed): **124** (7440 transactions per minute)

Difference between the highest TPS achieved in production and the new processing capability: **33 (1980 transactions per minute)**

The data thus theoretically illustrates that the 91TPS exceeds the comfort zone of 65TPS as evidenced in the stress test. At 65 TPS the system performs optimally with no degradation in service. The system is capable of absorbing transient spikes of over 100 TPS. When the system was stressed to 88 TPS, the system is performing under stress. Response times have degraded (by up to 200%) and reduced service is being offered with some transactions being discarded as volumes grow towards 88 TPS. Transient volume spikes will temporarily decrease the grade of service further. Over-stressed results (over 88 TPS) show that the performance is severely retarded. System behaviour is erratic with response times between 200% and 800% worse than those experienced at 65 TPS. The stress tests show that a hardware upgrade (increase in available CPU capacity) will be required before transactions rates of more than 65 TPS can be sustained for periods exceeding a few minutes.

5.8 Data Analysis – Card Industry Survey

The respondents to the questionnaire and focus sessions comprise a cross section of the card industry. The following companies and people are involved to a greater or lesser extent in credit card fraud, Merchant Services, telecommunications and system infrastructure. A brief overview of each company is presented below:

1. **FastNet**

   FastNet is an industry participant as it pertains to point-of-sale terminals and the radio communications service it provides to merchants throughout South Africa.

Their radio pad provides an efficient radio communication link between the card-swipe terminal and the banks' computers by replacing the telephone line.

2. X-Link

This company provides wireless data communications in the industry supplying a data communication interface to more than 10 000 merchants across South Africa. The company boasts the largest installed base of GPRS devices in the South African market.

3. ConnectNet

ConnectNet is a value added provider of wireless data communications and services for business-to-business and machine-to-machine applications. The ConnectNet boasts “A state of the art GPRS modem” Applications include Point-of-Sale (POS), ATMs, pre-paid airtime, healthcare verification, telemetry and security.

4. Retail Solutions

Retail Decisions (ReD) plc was founded in January 2000. ReD is a payment card issuer and a world leader in card fraud prevention and payment processing.

ReD's fraud prevention and payment processing operations located in Europe, South Africa and the US assists retailers, telecommunications companies, oil companies, e-commerce retailers and banks to prevent the fraudulent use of payment and credit cards in both card-present (CP) and card-not-present (CNP) payment environments.

5. Fair Isaac

Fair Isaac Corporation (NYSE: FIC) is the leading provider of decision management solutions powered by advanced analytics. Thousands of companies in more than 80 countries use Fair Isaac technology to acquire customers more efficiently, increase customer value and retention, reduce fraud and credit losses, lower operating costs and enter new markets more profitably.

Most leading banks and credit card issuers rely on Fair Isaac solutions, as do insurers, retailers, telecommunications providers, healthcare organizations and government agencies.

6. **CSC**

   Computer Software Consultants are a company that installs and maintains point-of-sale devices in the South African market. Most merchants acquired by Standard Bank utilize their services in the domestic arena.

7. **Standard Bank Front-End**

   The front-end staff maintains Standard Bank's front-end processor and ancillary systems, communications, hardware and software.

8. **Standard Bank Merchant Services**

   This business unit within Standard Bank engages in commercial agreements with merchants to process transactions thereby fulfilling a business partnership.

9. **MasterCard**

   MasterCard is a multinational corporation based in Purchase, NY in the United States. Throughout the world, its principal business is to process payments between the banks of merchants and the banks of purchasers that use its "Mastercard" branded debit- and credit cards to make purchases.

10. **Visa**

    Visa creates payment products, systems, services and standards on behalf of the banks that issue Visa cards and sign-up outlets to accept them. Visa also develops standards for global interoperability, security and new technologies.

5.8.1 School of Thought Survey

The sampling method used was that of non-probability sampling since the selection of the sampling elements was left to the researcher's discretion. The sampling method under the non-probability category was that of judgemental sampling in that the researcher used sample members based on his judgement of what constitutes a representative sample of the population of interest. The population of interest in this scenario comprises the stakeholders involved in the credit card market. The samples were taken from the following sample members:

Category 1: Fraud risk management staff in the local banking industry. This has been split between the banks (franchisees of MasterCard and Visa) and the franchisors (MasterCard and Visa).

Category 2: Telecommunications vendors or service providers.

Category 3: Merchant Services staff

The survey done with the fraud risk management staff comprised 13 respondents. The nature of the survey was to position the school of thoughts posited in Chapter 2.

The samples under each category comprise the following:

Fraud risk management staff	Number of respondents
Standard Bank	3
ABSA	2
First National Bank	2
Nedbank	2
Investec	1
Diners Club	2
Fair Isaac	1
MasterCard	1
Visa	1
	13

The Local bank fraud risk management staff comprised the following demographics:

Number of Respondents	Position	Average number of years in position
13	Managers, Investigators and Risk Analysts	8 years

The data was coded as follows:

Respondent	Respondent Classification
Standard Bank Fraud	1
ABSA Fraud	2
First National Bank Fraud	3
Nedbank Fraud	4
Investec Fraud	5
Mercantile Bank of Lisbon Fraud	6
MasterCard Fraud	7
Visa Fraud	8
Standard Bank Merchant Services	9
Retail Decisions	10
Fair, Isaac	11
Connectnet	12
Diners Club Fraud	13
CSC	14
MasterCard Operations	15
Standard Bank Front End	16

Likert Scale Category	Number
Strongly disagree	1
Disagree	2
Neither agree nor disagree	3
Agree	4
Strongly agree	5

The units of analysis were classified using the respondent classification table above. The variables comprise the questions in their numerical order. The data comprises the responses from each respondent (unit of analysis).

	Variables										
Units of Analysis	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
3	3	3	3	3	3	3	3	3	3	3	3
3	4	2	2	4	4	4	3	4	2	2	4
2	4	3	4	4	4	3	4	4	4	3	4
5	3	2	2	4	4	4	3	2	2	4	4
4	2	4	4	4	3	2	2	4	4	4	5
4	4	4	4	3	4	2	2	2	4	4	4
11	2	3	3	3	3	3	1	3	3	3	1
1	3	4	3	4	3	3	3	2	5	2	5
1	2	2	2	3	2	1	3	1	1	2	5
2	2	4	2	2	4	4	2	2	1	4	5
1	3	2	3	4	4	3	3	2	1	4	5
13	1	4	2	2	2	4	4	1	2	2	5
13	4	2	5	4	4	2	2	2	2	2	4
7	4	1	4	4	4	2	2	1	1	3	5

8	2	4	2	3	3	4	4	5	5	2	4
15											

Mode determination using the coded responses

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	1	1	0	0	0	1	1	3	4	0	1
2	5	5	6	2	2	4	5	6	4	6	0
3	4	3	4	5	5	5	6	2	2	4	1
4	5	6	4	8	8	5	3	3	3	5	6
5	0	0	1	0	0	0	0	1	2	0	7
Mode	**Bi**	**4**	**Bi**	**4**	**4**	**Bi**	**3**	**Bi**	**Bi**	**2**	**5**

As can be seen above, the responses to questions 1,3,6,8,9 are bimodal in terms of the relative frequencies of the responses.

Respondent answer distribution using the coded responses

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	7%	7%	0%	0%	0%	7%	7%	20%	27%	0%	7%
2	33%	33%	40%	13%	13%	27%	33%	40%	27%	40%	0%
3	27%	20%	27%	33%	33%	33%	40%	13%	13%	27%	7%
4	33%	40%	27%	53%	53%	33%	20%	20%	20%	33%	40%
5	0%	0%	7%	0%	0%	0%	0%	7%	13%	0%	47%

Using the abovementioned responses, a brief summation of the modal answers will be applied to the survey questions below:

Question 1

"The local telecommunications infrastructure (telephone, radio pad or GPRS) from the point of sale to the issuing bank during an authorization request has the ability to sustain a zero floor limit". The respondents were split between answering "Agreed" and "Disagreed". No insight can be obtained from these responses due to variability of the responses.

Question 2

"TELKOM is a reason for not adopting zero floor limits". Most of the respondents "Disagreed" which lends weight to the fraud school of thought posited by the researcher.

Question 3

"The reduction of floor limits will not have a negative impact on cardholders at the point of sale". The majority of the respondents disagreed which is an acknowledgement of the potential adverse impact a zero floor limit can have in terms of the slowness of service delivery.

Question 4

"Local issuers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests". The majority of the respondents agreed that the issuers in South Africa can handle the authorization capacity that would be evident by introducing a zero floor limit.

Question 5

"Local acquirers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests". The majority of the respondents agreed that the acquirers in South Africa can handle the authorization capacity that would be evident by introducing a zero floor limit.

Question 6

"An increase in authorization volumes attributable to a zero floor limit will adversely affect issuers in their ability to process the transactions." The responses had a bimodal distribution between "Agreed" and "Neither agree nor disagree". Evidence suggests that some respondents may affect issuing banks and their ability to process the authorizations traffic attributed to a zero floor limit. This answer goes against question 4 which suggests reliability measurement errors.

Question 7

"An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions." The majority of the responses were "Neither agree nor disagree".

Question 8

"Issuers and acquirers can wait for the full implementation of EMV (CHIP and PIN) as a solution to reducing fraud. An increase in authorization volumes attributable to a zero

floor limit will adversely affect acquirers in their ability to process the transactions." The majority of the responses were "Disagree". The respondents acknowledged in their comments that the roll-out of chip within the South African industry would be slow.

Question 9

"Below floor-limit credit card fraud is a cost of doing business on a credit card and is controllable by the issuing and acquiring bank." The majority of the responses were between "Disagree" and "Strongly disagree". This response lends weight to the problem that floor limits pose within the South African credit card industry.

Question 10

"Reduced floor limits will increase merchant's operational (telephony) costs as they have to now pay extra for the authorization request. This cost is greater for the merchant that the cost of charge-backs and voucher retrievals." The majority of the responses were "Disagree".

Question 11

"Floor limits should be incrementally decreased based on credit card fraud at certain merchant categories." It was overwhelmingly agreed that this approach should be used to implement a zero floor limit.

The survey done with the telecommunications service providers comprised 10 respondents. The nature of the survey was to position the school of thoughts posited in Chapter 2.

The samples under each category comprised the following:

Telecommunications staff	Number of respondents
Retail Decisions	1
Connectnet	3
CSC	1
Standard Bank Front-End Personnel	2
Fastnet	1
X-Link	2
	10

The respondents comprised the following demographics:

Number of Respondents	Position	Average number of years in position
10	Managers, Directors and Technical staff	7 years

The data was coded as follows:

Respondent	Respondent Classification
Standard Bank Fraud	1
ABSA Fraud	2
First National Bank Fraud	3
Nedbank Fraud	4
Investec Fraud	5
Mercantile Bank of Lisbon Fraud	6
MasterCard Fraud	7
Visa Fraud	8
Standard Bank Merchant Services	9
Retail Decisions	10
Fair, Isaac	11
Connectnet	12
Diners Club Fraud	13
CSC	14
MasterCard Operations	15
Standard Bank Front End	16

The units of analysis were classified using the respondent classification table above. The variables comprise the questions in their numerical order. The data comprises the responses from each respondent (unit of analysis).

	Variables										
Units of Analysis	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
10	4	1	5	4	4	2	2	1	1	1	5
12	5	5	5	4	4	2	2	3	2	1	2
12	4	5	4	4	3	3	2	2	2	2	3
12	5	5	5	4	4	2	2	2	2	4	2
14	4	3	3	4	4	2	2	3	3	2	2
16	4	4	2	3	3	4	4	2	3	4	4
16	4	4	5	4	4	2	2	1	4	3	2
17	4	4	2	2	2	4	4	2	4	2	3
18	5	2	1	4	2	3	2	2	2	4	5
18	4	5	5	4	3	3	3	2	3	1	4

Mode determination using the coded responses

	1	2	3	4	5	6	7	8	9	10	11
1	0	1	1	0	0	0	0	2	1	3	0
2	0	1	2	1	2	5	7	6	4	3	4
3	0	1	1	1	3	3	1	2	3	1	2
4	7	3	1	8	5	2	2	0	2	3	2
5	3	4	5	0	0	0	0	0	0	0	2
Mode	**4**	**Bi**	**Bi**	**Bi**	**4**	**2**	**2**	**Bi**	**2**	**Bi**	**Bi**

As can be seen above, the responses to questions 2, 3,4,8,10,11 are bimodal in terms of the relative frequencies of the responses.

Respondent answer distribution using the coded responses

	1	2	3	4	5	6	7	8	9	10	11
1	0%	10%	10%	0%	0%	0%	0%	20%	10%	30%	0%
2	0%	10%	20%	10%	20%	50%	70%	60%	40%	30%	40%
3	0%	10%	10%	10%	30%	30%	10%	20%	30%	10%	20%
4	70%	30%	10%	80%	50%	20%	20%	0%	20%	30%	20%
5	30%	40%	50%	0%	0%	0%	0%	0%	0%	0%	20%

Using the abovementioned responses, a brief summation of the modal answers will be applied to the survey questions below:

Question 1

“The local telecommunications infrastructure (telephone, radio pad or GPRS) from the point of sale to the issuing bank during an authorization request has the ability to sustain a zero floor limit”. The respondents answered “Agreed” and “Strongly Agreed”. This lends weight to the fact that the telecommunications infrastructure and technology in South Africa can sustain a zero floor limit environment.

Question 2

“TELKOM is a reason for not adopting zero floor limits”. Most of the respondents “Agreed” and “Strongly Agreed”. This result was not expected and would need to be researched further.

Question 3

"The reduction of floor limits will not have a negative impact on cardholders at the point of sale". The majority of the respondents "Strongly Agreed". This lends evidence to the fact that the telecommunications respondents have confidence in the infrastructure and technology to support a zero floor limit environment.

Question 4

"Local issuers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests". The majority of the respondents agreed that the issuers in South Africa can handle the authorization capacity that would be evident by introducing a zero floor limit.

Question 5

"Local acquirers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests". The majority of the respondents agreed that the acquirers in South Africa can handle the authorization capacity that would be evident by introducing a zero floor limit.

Question 6

"An increase in authorization volumes attributable to a zero floor limit will adversely affect issuers in their ability to process the transactions." The majority of the responses were "Disagree" which provides an insight into the confidence these respondents have on the ability of the bank to handle the volume of authorization requests.

Question 7

"An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions." The majority of the responses were "Disagree" which provides an insight into the confidence these respondents have on the ability of the bank to handle the volume of authorization requests

Question 8

"Issuers and acquirers can wait for the full implementation of EMV (CHIP and PIN) as a solution to reducing fraud." The majority of the responses were "Disagree". The

respondents acknowledged in their comments that the roll-out of chip within the South African industry would be slow.

Question 9

"Below floor-limit credit card fraud is a cost of doing business on a credit card and is controllable by the issuing and acquiring bank." The majority of the responses were "Disagree".

Question 10

"Reduced floor limits will increase merchant's operational (telephony) costs as they have to now pay extra for the authorization request. This cost is greater for the merchant that the cost of charge-backs and voucher retrievals." The majority of the responses were "Disagree" and "Strongly Disagree".

Question 11

"Floor limits should be incrementally decreased based on credit card fraud at certain merchant categories." Most of the respondents "Disagreed".

The survey done with the merchant service providers comprised 6 respondents. The nature of the survey was to position the school of thoughts posited in Chapter 2.

Merchant Services Personnel	Number of respondents
Retail Decisions	6
	6

The merchant services personnel comprised the following demographics:

Number of Respondents	Position	Average number of years in position
6	Managers and Merchant Services staff	5 years

The data was coded as follows:

Respondent	Respondent Classification
Standard Bank Fraud	1
ABSA Fraud	2
First National Bank Fraud	3
Nedbank Fraud	4
Investec Fraud	5
Mercantile Bank of Lisbon Fraud	6
MasterCard Fraud	7
Visa Fraud	8
Standard Bank Merchant Services	9
Retail Decisions	10
Fair, Isaac	11
Connectnet	12
Diners Club Fraud	13
CSC	14
MasterCard Operations	15
Standard Bank Front End	16

The units of analysis were classified using the respondent classification table above. The variables comprise the questions in their numerical order. The data comprises the responses from each respondent (unit of analysis).

	Variables										
Units of Analysis	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
9	4	3	3	4	3	3	4	2	2	4	4
9	2	4	2	2	2	4	4	4	4	4	5
9	4	5	4	3	4	4	3	3	3	2	4
9	4	3	2	4	4	2	2	4	4	2	5
9	4	5	4	3	1	3	4	2	2	4	4
9	4	5	4	3	1	3	4	2	2	4	4

Mode determination using the coded responses

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	0	0	0	0	2	0	0	0	0	0	0
2	1	0	2	1	1	1	1	3	3	2	0
3	0	2	1	3	1	3	1	1	1	0	0
4	5	1	3	2	2	2	4	2	2	4	4
5	0	3	0	0	0	0	0	0	0	0	2
Mode	**4**	**5**	**4**	**3**	**Bi**	**3**	**Bi**	**2**	**2**	**4**	**4**

As can be seen above, the responses to questions 5 and 7 are bimodal in terms of the relative frequencies of the responses.

Respondent answer distribution using the coded responses

	1	2	3	4	5	6	7	8	9	10	11
1	0%	0%	0%	0%	33%	0%	0%	0%	0%	0%	0%
2	17%	0%	33%	17%	17%	17%	17%	50%	50%	33%	0%
3	0%	33%	17%	50%	17%	50%	17%	17%	17%	0%	0%
4	83%	17%	50%	33%	33%	33%	67%	33%	33%	67%	67%
5	0%	50%	0%	0%	0%	0%	0%	0%	0%	0%	33%

Using the abovementioned responses, a brief summation of the modal answers will be applied to the survey questions below:

Question 1

"The local telecommunications infrastructure (telephone, radio pad or GPRS) from the point of sale to the issuing bank during an authorization request has the ability to sustain a zero floor limit". The respondents answered "Agreed". This lends weight to the fact that the telecommunications infrastructure and technology in South Africa can sustain a zero floor limit environment.

Question 2

"TELKOM is a reason for not adopting zero floor limits". Most of the respondents "Agreed" and "Strongly Agreed". This result was not expected and would need to be researched further.

Question 3

"The reduction of floor limits will not have a negative impact on cardholders at the point of sale". The majority of the respondents "Agreed". This lends evidence to the fact that the telecommunications respondents have confidence in the infrastructure and technology to support a zero floor limit environment.

Question 4

"Local issuers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests". The majority of the respondents neither agreed nor disagreed that the issuers in South Africa can handle the authorization capacity that would be evident by introducing a zero floor limit.

Question 5

"Local acquirers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests". The majority of the respondents disagreed that the acquirers in South Africa can handle the authorization capacity that would be evident by introducing a zero floor limit.

Question 6

"An increase in authorization volumes attributable to a zero floor limit will adversely affect issuers in their ability to process the transactions." The majority of the responses neither agreed nor disagreed.

Question 7

"An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions." The majority of the responses were "Agree".

Question 8

"Issuers and acquirers can wait for the full implementation of EMV (CHIP and PIN) as a solution to reducing fraud". The majority of the responses were "Disagree". The respondents acknowledged in their comments that the roll-out of chip within the South African industry would be slow.

Question 9

"Below floor-limit credit card fraud is a cost of doing business on a credit card and is controllable by the issuing and acquiring bank." The majority of the responses were "Disagree".

Question 10

"Reduced floor limits will increase merchant's operational (telephony) costs as they have to now pay extra for the authorization request. This cost is greater for the merchant that the cost of charge-backs and voucher retrievals." The majority of the responses were "Agree".

Question 11

"Floor limits should be incrementally decreased based on credit card fraud at certain merchant categories." Most of the respondents "Agreed".

5.9 Data Analysis – Standard Bank Credit Card Fraud 2006

The credit card fraud perpetrated on Standard Bank products for 2006 is discussed below. The transactions have been extracted from Standard Bank's enterprise resource planning system. The products have been categorized according to families of products. The families of products have been segmented according to the following the assigned generic floor limits that they enjoy. The family of product classification is enclosed in *Appendix 1*. Cards that enjoy a generic floor limit of R300.00 at "face-to-face" channels comprise:

- Blue (classified as S)
- Company (classified as B)

Cards that enjoy a generic floor limit of R500.00 at "face-to-face" channels comprise:

- Garage (classified as S)

Cards that enjoy a generic floor limit of R600.00 at "face-to-face" channels comprise:

- Gold (classified as G)
- Platinum (Classified as P)

The transactions only comprise the domestic fraud and exclude Standard Bank-issued credit card fraud perpetrated abroad (as this is a delimitation for the research report).

Standard Bank comprised an average market share of 25% (based on credit card debt). The transactional market share and credit card market share was not available at the time of this research report. The fraud analysis can thus be reasonably determined from the market share based on credit card debit balances as reflected in *figure 46*. Albeit that the credit limits assigned to the respective products by the issuing banks may differ as well as the diversification of the products, the overall market share is a good barometer when applying the Standard Bank fraud analysis as an indication of the market losses.

The information was extracted from the DI900 (Deposit-Taking Institution) which is reported to the South African Reserve Bank (Standard Bank Card Division, 2007).

Figure 46: Market share year-on-year between the major credit card issuers in South Africa

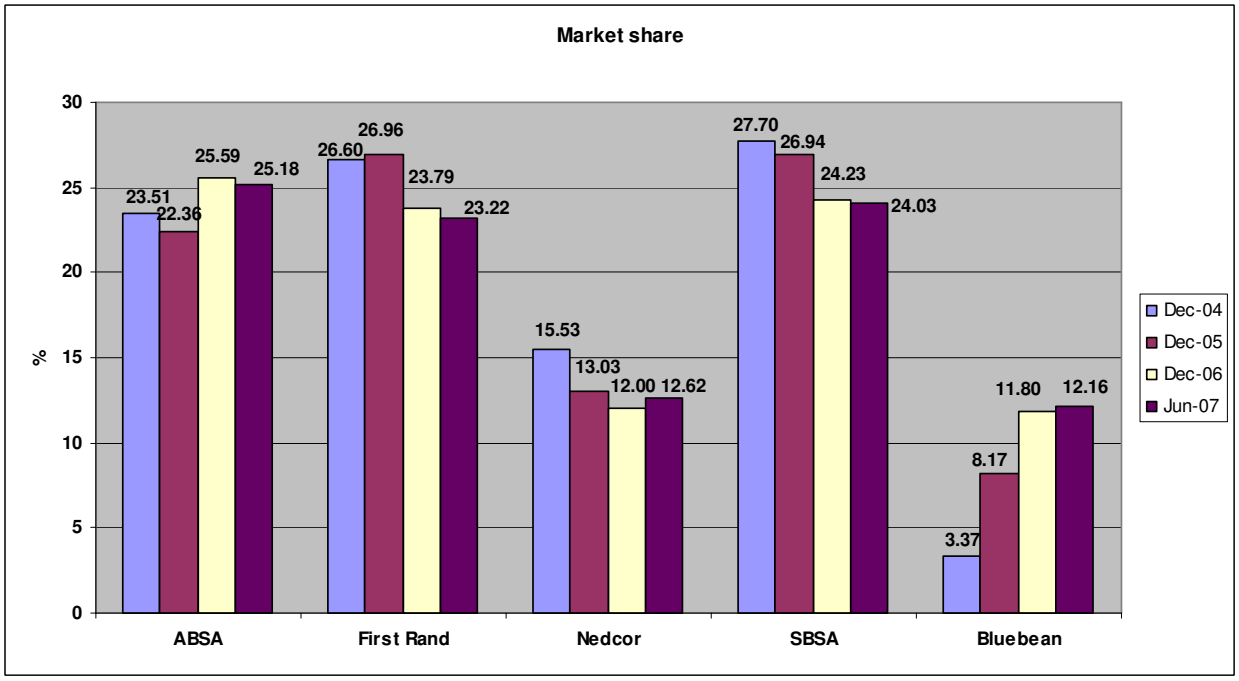


Figure 47: Issuer share of monthly gross market balances (percentage)

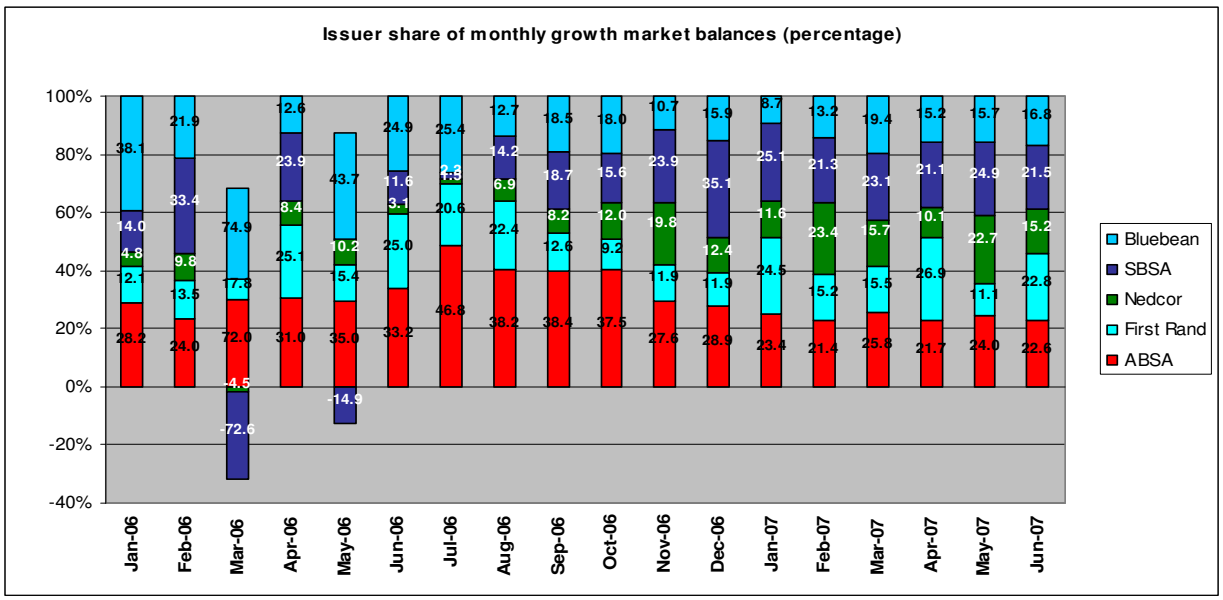


Table 19: Below and above floor limit fraud on a blue family of products

Blue - Local >= 300			
Year	BIN	Amount	Count
2006		R 9,799,029.51	6804
	286235	R 40,326.70	11
	454858	R 510,198.20	226
	510432	R 15,268.03	21
	510433	R 114,257.60	101
	512055	R 1,550,027.81	1024
	512056	R 13,368.66	12
	522100	R 5,939,707.42	3961
	522262	R 921,837.29	699
	527466	R 694,037.80	749
Grand Total		R 9,799,029.51	6804

Blue - Local < 300			
Year	BIN	Amount	Count
2006		R 9,402,789.74	76229
	286235	R 871.00	5
	454858	R 90,029.66	663
	510432	R 25,388.03	139
	510433	R 18,076.27	595
	512055	R 1,451,814.51	13261
	512056	R 21,787.41	142
	522100	R 5,128,015.72	41304
	522262	R 1,778,937.75	13228
	527466	R 887,869.39	6892
Grand Total		R 9,402,789.74	76229

This family of products comprises 51% of transactions above the merchant's floor limit on the transaction amounts as a Rand value. 49% of the domestic fraud is perpetrated below the merchants floor limit. If one considers the transactions as a number of transactions conducted below and above the floor limit, the differentiation is 8% above the merchant's floor limit as opposed to 92% below the floor limit.

Table 20: Below and above floor limit fraud on corporate family of products

Corporate - Local >= 300			
Year	BIN	Amount	Count
2006		R 1,932,971.17	1107
	522118	R 1,932,971.17	1107
Grand Total		R 1,932,971.17	1107

Corporate - Local < 300			
Year	BIN	Amount	Count
2006		R 488,823.46	3828
	522118	R 488,823.46	3828
Grand Total		R 488,823.46	3828

This family of products comprises 80% of transactions above the merchant's floor limit on the transaction amounts as a Rand value. 20% of the domestic fraud is perpetrated below the merchants floor limit. If one considers the transactions as a number of transactions conducted below and above the floor limit, the differentiation is 22% above the merchant's floor limit as opposed to 78% below the floor limit.

Table 21: Below and above floor limit fraud on a Garage family of products

Garage - Local >= 500			
Year	BIN	Amount	Count
2006		R 313,454.75	268
	201010	R 49,063.86	35
	225050	R 178,910.98	172
	603951	R 85,479.91	61
Grand Total		R 313,454.75	268

Garage - Local < 500			
Year	BIN	Amount	Count
2006		R 7,004,504.75	34640
	201010	R 989,287.85	4604
	225050	R 3,729,879.78	18639
	603951	R 2,285,337.12	11397
Grand Total		R 7,004,504.75	34640

This family of products comprises 4% of transactions above the merchant's floor limit on the transaction amounts as a Rand value. 96% of the domestic fraud is perpetrated below the merchants floor limit. If one considers the transactions as a number of transactions conducted below and above the floor limit, the differentiation is 1% above the merchant's floor limit as opposed to 99% below the floor limit.

Table 22: Below and above floor limit fraud on a gold family of products

Gold - Local >= 600			
Year	BIN	Amount	Count
2006		R 15,535,389.40	5752
	406928	R 649.90	1
	512057	R 1,005,999.86	478
	512058	R 7,540.99	4
	522126	R 11,364,139.06	4080
	522134	R 1,134,277.06	395
	522175	R 907,195.24	333
	522250	R 1,007,024.10	405
	522263	R 5,647.80	2
	526397	R 28,902.56	15
	603951	R 74,012.83	39
Grand Total		R 15,535,389.40	5752

Gold- Local < 600			
Year	BIN	Amount	Count
2006		R 17,546,477.10	75721
	406928	R 560.40	3
	512057	R 1,876,917.56	9361
	512058	R 51,019.13	202
	522126	R 9,857,677.92	41003
	522134	R 1,993,558.02	7107
	522175	R 157,024.15	707
	522250	R 1,291,968.53	5818
	522263	R 1,404.79	7
	526397	R 19,542.40	94
	603951	R 2,296,804.20	11419
Grand Total		R 17,546,477.10	75721

This family of products comprises 47% of transactions above the merchant's floor limit on the transaction amounts as a Rand value. 53% of the domestic fraud is perpetrated below the merchants floor limit. If one considers the transactions as a number of transactions conducted below and above the floor limit, the differentiation is 7% above the merchant's floor limit as opposed to 93% below the floor limit.

Table 23: Below and above floor limit fraud on a platinum family of products

Platinum - Local >= 600			
Year	BIN	Amount	Count
2006		R 5,138,113.56	1,779
	454858	R 487,771.74	175
	523958	R 100,219.07	73
	552057	R 3,562,113.78	1,204
	552065	R 988,008.97	327
Grand Total		R 5,138,113.56	1,779

Platinum- Local < 600			
Year	BIN	Amount	Count
2006		R 1,100,221.20	5,904
	454858	R 112,456.12	714
	523958	R 7,510.47	53
	552057	R 635,849.27	3,545
	552065	R 344,405.34	1,592
Grand Total		R 1,100,221.20	5,904

This family of products comprises 82% of transactions above the merchant's floor limit on the transaction amounts as a Rand value. 18% of the domestic fraud is perpetrated below the merchants floor limit. If one considers the transactions as a number of transactions conducted below and above the floor limit, the differentiation is 23% above the merchant's floor limit as opposed to 77% below the floor limit.

The major contributors to fraud under the product families comprise:

Table 24: Below and above floor limit fraud on a all families of products as an amount (R's)

	Above		%	Below		%
Blue	R	9,799,029.51	30%	R	9,402,789.74	26%
Corporate	R	1,932,971.17	6%	R	488,823.46	1%
Garage	R	313,454.75	1%	R	7,004,504.75	20%
Gold	R	15,535,389.40	47%	R	17,546,477.10	49%
Platinum	R	5,138,113.56	16%	R	1,100,221.20	3%
Total	**R**	**32,718,958.39**		**R**	**35,542,816.24**	

Table 25: Below and above floor limit fraud on a all families of products as a count of transactions

	Above	%	Below	%
Blue	6,804.00	43%	76,229.00	39%
Corporate	1,107.00	7%	3,828.00	2%
Garage	268.00	2%	34,640.00	18%
Gold	5,752.00	37%	75,721.00	39%
Platinum	1,779.00	11%	5,904.00	3%
Total	**15,710.00**		**196,322.00**	

Table 26: Below and above floor limit fraud on a all families of products as a cumulative amount (R's)

Above Floor Limit	Below Floor Limit
R 32,718,958.00	R 35,542,816.00

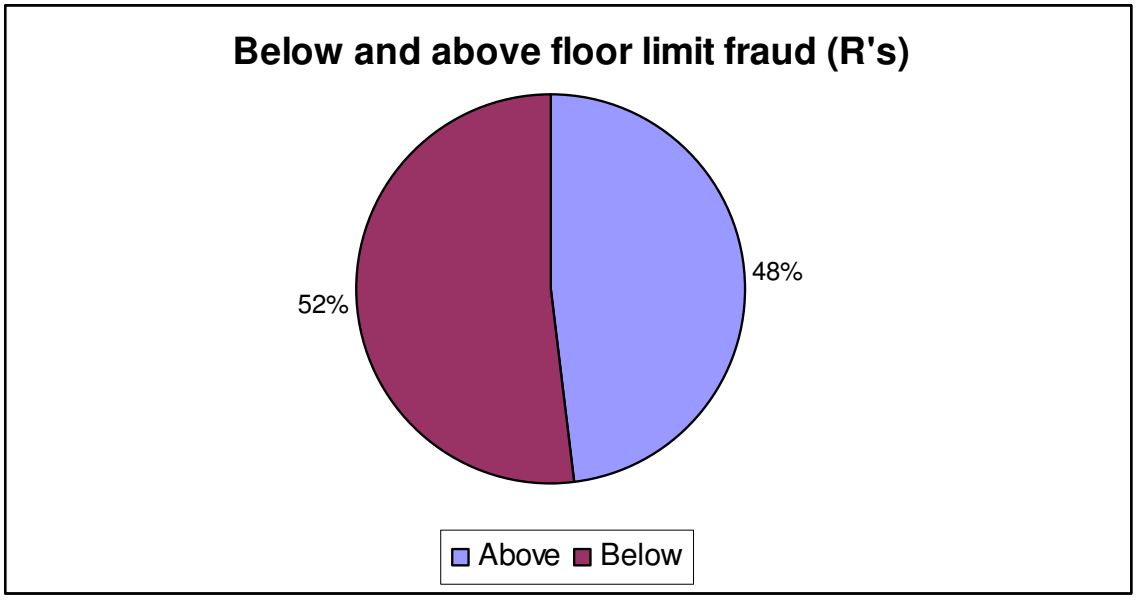


Table 27: Below and above floor limit fraud on a all families of products as a cumulative count

Above Floor Limit	Below Floor Limit
15,710	196,322

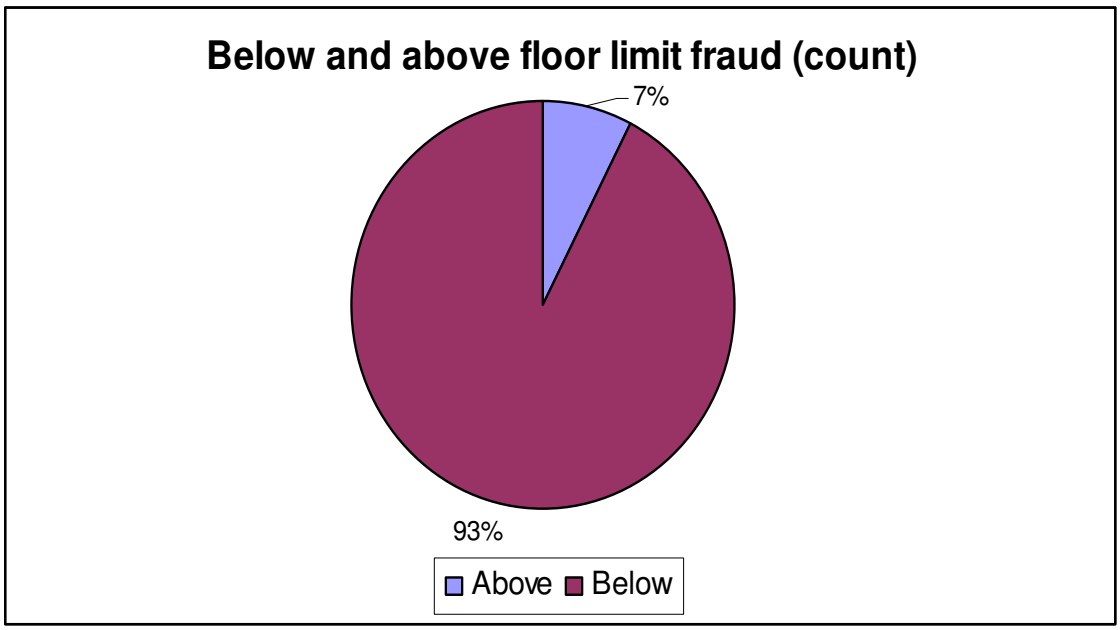


Table 28: Below floor limit fraud at the top 10 products (BIN) and top 5 merchant category codes

Merchant Category	Card BIN	Amount (R's)	Count of transactions
Grocery stores and supermarkets	**Total**	**10,194,717**	**777**
	512055	818,853	80
	512057	757,580	80
	522100	1,982,931	82
	522126	4,006,555	82
	522134	626,095	76
	522250	343,973	79
	522262	614,239	77
	527466	428,883	81
	552057	395,977	77
	552065	219,631	63
Service stations (petrol)	**Total**	**14,131,561**	**644**
	201010	1,231,169	68
	225050	9,528,064	140
	512055	39,624	58
	512057	45,385	58
	522100	89,527	62
	522126	100,009	60
	522134	15,701	39
	522262	34,493	49
	527466	20,689	41
	603951	3,026,899	69
Men's and boy's clothing	**Total**	**4,046,735**	**541**
	512055	259,722	62
	512057	311,676	57
	522100	646,414	70
	522126	1,745,291	80
	522134	289,881	51
	522250	265,560	53
	522262	216,719	52
	527466	130,417	49
	552057	110,557	39
	552065	70,497	28
Family Clothing Stores	**Total**	**5,649,465**	**642**
	512055	413,682	67
	512057	262,449	68
	522100	965,509	76
	522126	2,538,725	75
	522134	391,849	66
	522250	327,420	58
	522262	263,259	64
	527466	235,579	71
	552057	140,509	53
	552065	110,485	44
Restaurants	**Total**	**4,122,533**	**790**
	512055	363,466	80
	512057	395,092	79
	522100	890,727	80
	522118	158,562	80
	522126	1,294,863	80

	522134	151,517	77
	522250	234,492	80
	522262	254,560	77
	527466	244,728	79
	552057	134,525	78
Grand Total		**38,145,012**	**3,394**

As can be seen from the analysis above, below floor limit fraud in South Africa comprises 52% of transactions as a Rand value (R35,542,816) and 93% as a count of transactions (196,322). This in turn represents an average ticket value of R181.00. If Standard Bank represents 25% of the market share (based on market balances), the calculations above represent a quarter of the fraud perpetrated below the merchant's floor limit in South Africa. It is not prudent to multiply the calculations by 75% to determine the overall impact of below floor limit fraud for the industry as there are many dependent variables notwithstanding:

- The type of products issued by the issuing bank
- The acquiring market share (as the acquirer can set zero floor limits for merchants acquired by them)
- The issuer's lending propensity (credit limit allocated to cardholders)
- The product's floor limit that is personalized to the point of sale machines (the issuing bank sends this to the acquiring bank)
- The number of cards in issue by the issuing bank and the number of active accounts

If one took the view that the calculations quoted represent a quarter of the below floor limit problem and applied the 75% calculation, the following would result:
Below floor limit fraud by amount (R's): R62, 200,000.00
Below floor limit as a count of transactions: 344,000.00

It must be mentioned that this relates to credit card fraud only and discounts the credit losses from a collections perspective as this falls outside the ambit of this research report (a delimitation). The credit losses due to over limit, delinquent, arrear, revoked and legal accounts will far exceed the fraud losses. If one considers the merchant categories where fraud is prevalent from an industry perspective as mentioned in chapter 1 and supported by the Standard Bank data above, it becomes apparent that it is the large retailers that generate the largest volume of transactions where below floor limit

fraud occurs. This is not surprising as the fraudsters generally shop at these establishments as:

- Their anonymity is preserved due to the multiple till and purchase points
- The selection of merchandise is substantial
- The resale value of the merchandise is lucrative
- The possibility of fraud detection by the merchant or merchant employee is minimal.

The majority of the fraud losses perpetrated below the merchant's floor limit are ascribed to the following fraud types:

Table 29: Fraud contribution by fraud type below the merchant's floor limit.

Fraud Type	% Below floor limit
Lost and stolen	88.00%
Counterfeit	6.00%
NRI	3.00%
Fraudulent Application	3.00%
Account Take Over	0.00%
Card Number Used	0.00%
	100.00%

As can be seen from above, lost and stolen fraud comprises the majority of the fraud perpetrated below the merchant's floor limit.

If one considers the analysis results done in the chapter, the following becomes apparent:

- Fraudsters generally frequent the large retailers which comprise the bulk of the transactional volume.
- A large portion of the fraud occurs below the merchant's floor limit.
- Lost and stolen fraud comprises the majority of the fraud losses.
- The fraud is perpetrated in large metropolitan areas.
- If a zero floor limit is introduced at all merchant categories, in all geographic areas, the ability of Standard Bank to service these transactions is questionable based on the anticipated increase in TPS.

- The telecommunication service providers agree that the telecommunications infrastructure (especially GPRS) can handle the anticipated increase in transactional volumes.
- The majority of the telecommunications service providers consider issuers and acquirers to have the capacity to handle an increase in authorization volumes attributable to a zero floor limit.
- The majority of the respondents acknowledged the Proposition that chip and PIN (EMV) would not stem the fraud losses as the roll-out of this technology would be slow.
- Fraud losses are generally not considered to be a cost of doing business and should be curtailed.

CHAPTER 6

6. Discussion, Conclusions and Recommendations

6.1 Introduction

It is pertinent to recap on the Propositions and the data collected from the various populations mentioned in chapter 4 and 5. The Propositions are:

Proposition 1:

The first Proposition is that merchant floor limits in South Africa have an adverse impact on bank-issued credit card fraud.

Proposition 2:

The second Proposition is that South African telecommunications can sustain a zero floor limit.

Proposition 3:

The third Proposition is that the cost of introducing a zero floor limit in South Africa is negligible in relation to the fraud which floor limits sustain.

Proposition 4:

The fourth Proposition is that local banks infrastructure and technology can accommodate an increase in authorisations as a result of a zero floor limit environment.

The sample data collected from the various populations comprised the following:

1. Data collected from SABRIC on credit card fraud in South Africa
2. Issuing data contained within Standard Bank's data mart on all authorizations and postings from January 2006 to December 2006.
3. Data results from a stress test performed from May to June 2006.
4. Data from Bankserv over the period January 2006 to December 2006.
5. Samples from a survey to determine attitudes and opinions relating to floor limits and telecommunications.

The data has been collected and analyzed to support the Propositions from a quantitative and qualitative perspective. Many interviews and discussions were had with various stakeholders in the credit card industry.

6.2 Inherent weaknesses of this study

The study has inherent weaknesses which need to be contextualized in relation to the scope and complexity of the research report and its concomitant objectives. The weaknesses are listed below:

6.2.1 The complexity of the credit card architecture from the point-of-sale to the issuing or acquiring bank. There are a host of system intermediaries (data switches) and interfaces (notwithstanding the complexity of the Standard Bank internal architecture) that are not synonymous and depend on the nature of the technology deployed by the merchant. In order to build a simulator to do an end-to-end stress test taking each scenario into consideration would be too cumbersome and time-consuming for this research report. An end-to-end volume and stress test would be ideal to truly simulate a production environment. The volume test performed pertains to generic simulated transactions and is geared to Standard Bank's front-end processor solely. The vagaries of a production environment coupled to the multiple system intermediaries and "what-if" scenarios are not utterly represented by the volume test.

6.2.2 A second weakness is the issuing data stored by Standard Bank (being representative of the domestic credit card market by applied market share). The data was extracted over a representative period of 2006 to test the distribution of authorizations against batched transactions (transactions conducted below the merchant's floor limit). A **"goodness-of-fit"** test would have been used to compare the extent to which the observed (i.e. empirical) frequencies "fit" the expected (i.e. theoretical) frequencies. The anticipated increase in authorization volumes due to a zero floor limit environment would have been compared with the ability of Standard Bank's front-end processor (Postillion) to handle the volume of transactions (measured by its transaction per second processing

capability). The distributions being tested are those of authorizations (which have a time stamp) in conjunction with postings (transactions conducted below the merchant's floor limit) which *do not have a time stamp* for this test. The time stamp is not stored for issuing transactions conducted below the merchant's floor limit by Standard Bank. A large sample of data (transactions below the merchant's floor limit) is available from the Group's data mart but no time is stored. This makes the use of the chi-square test irrelevant for testing the assumption that posted transactions follow the same distribution as the authorized transactions.

6.2.3 A third weakness of the study is that the issuer and acquirer's ability to handle an increase in authorizations has been limited to Standard Bank's system architecture. The fourth Proposition is that the local banking infrastructure and technology can accommodate an increase in authorisations as a result of a zero floor limit environment. The supposed ability of the industry to fulfil this requirement vests in the analysis done on Standard Bank's systems. Albeit that Standard Bank has a substantial market share in domestic credit cards, the other local agent banks have different systems and system architectures. To perform stress (volume) tests on these entities is not viable due to the time constraints and the competitiveness of the domestic banks.

6.2.4 A fourth weakness of the study has been the ability to completely and accurately differentiate between below floor limit and above floor limit fraud. Certain products have different floor limits associated with them. The product differentiation from an industry perspective has been taken into account during this research report however, certain merchants have been placed on a zero floor limit by the acquiring bank due to excessive fraud perpetrated at these establishments. The zero floor limits does not apply indefinitely at these merchants and to accurately assess the fraud perpetrated below the floor limit, the timing of the zero floor limit placement would be a key consideration. The industry fraud data was analysed in terms of generic floor limits and Standard Bank's fraud segmentation (as a representative sample using applied market share) was used to cross-check the floor limit fraud spend.

6.2.5 A fifth weakness is the inability to calculate the true costs pertaining to reducing floor limits as the costs entail not only direct costs but also indirect costs in terms of potential revenue leakage. The costs associated with the zero floor limit debate are discussed under Proposition 3 in the next section.

6.2.6 A sixth weakness of the study is that the anticipated increase in authorization volumes in a zero floor limit environment from a local industry perspective has not been determined. This is due to the sensitivity of the data amongst the local competitors and the differentiation between transactions that are switched by the domestic switch (Bankserv) and transactions that go directly to the issuer bypassing the domestic switch altogether. This differentiation is difficult to determine as it would also need to be seen in light of the following:

- The merchant's location
- The cardholder's location
- The particular channel used
- The merchant's patrons and their propensity to purchase with a credit card
- The nature of the merchant's merchandise
- The seasonality of the merchant's sales.

Figure 45 in chapter 5 illustrates this complexity by differentiating between transactions that go directly to the issuing bank and those that are switched by Bankserv. Albeit that Standard Bank was used in the depiction, it applies to the local industry issuers and acquirers as well.

6.2.7 A seventh weakness of the study is that the stress test performed was done in order to test the capability of the front-end processor. As a component of the test objectives, the aim was to determine online (authorisation) capacity. The tests did not however, take a full zero floor limit into consideration (as an issuing and acquiring institution). The tests were run for a small passage of time (1.2 hours) and aimed at putting the front-end processor (Postillion) under as much stress as possible. Over 409,000 transactions were executed during this period with the highest average transaction rate over a 5 second period being 141 TPS and the highest average transaction rate over 1 minute period was 106 TPS. It would

have been preferable to stress test the anticipated number of authorizations that would be routed to the Postillion in a zero floor limit environment to test whether these thresholds were exceeded or not. Another consideration would be the transient spikes within a day (depending on when customers are at their most active in shopping). These scenarios would need to be stress tested as well. The data obtained and analyzed for 2006 (authorizations and postings) represents averages (TPS) only and may not accurately represent transient spikes in a production environment. As the relationship between TPS processing capability and authorization requests is not linear (it is more logarithmic), the ability to ascertain the actual impact of zero floor limits is difficult. The CPU processing ability and queue lengths and waiting times for the authorizations are further considerations that need to be tested.

6.2.8 The eighth weakness is that relationship between the CPU usage, the TPS and system memory consumption is *not linear* and cannot be argued mathematically. CPU consumption is positively correlated to memory use and TPS (as shown in the stress test results). No logarithmic scale is available at Standard Bank to represent this relationship. In order to unequivocally prove whether the front-end processor can handle a zero floor limit, a stress test (acid test) must be performed where a zero floor limit based on production volumes is used.

6.2.9 The ninth weakness is that the upgraded CPU processor introduced late in 2006 has not been stress tested. The stress test was performed on the older hardware configurations. Assumptions have been made in terms of the double-processing capability of the replicated hardware.

6.3 Discussion

The analysis and research done to date on the formulated Proposition are discussed under this heading.

6.3.1 Proposition 1: The first Proposition is that merchant floor limits in South Africa have an adverse impact on bank-issued credit card fraud. This can be seen in chapter 1 that positions the infrastructural components of the credit card process in South Africa that contribute to the fraud life cycle. The two major contributing factors are:

- The settlement delay between the acquiring bank and the issuing bank,
- The delay in closing the POS channel where the issuing bank and the acquiring bank are not synonymous.

As already mentioned, fraudsters are aware of the window of opportunity available to them due to the infrastructural architecture. The fraudsters purposely purchase at merchants that are acquired by acquirers that are not the issuing bank with which the fraudster transacts (i.e. the credit card used by the fraudster is issued by an issuing bank that is not the same as the transaction acquiring institution). The data obtained from SABRIC in chapter 1 as well as the data obtained from Standard Bank's data warehouse supports this statement. Domestic fraud in 2006 comprised R179M of which R62M is expected to represent the below floor limit component as calculated in chapter 5. This represents 35% of the transactions as a Rand value. If one had to consider the number of transactions (as a transaction count) as a percentage to the total fraud transaction count, a figure of 80 – 85% is apparent. The transaction counts were not available from SABRIC. Standard Bank's fraud as a transaction count for 2006 comprised 93%. The linear growth in fraud year-on-year from an industry perspective presents a concern to the domestic banking industry. The roll-out of chip and PIN is expected to take up to two years. This technology will reduce the number of lost and stolen transactions (as well as counterfeit and NRI) as the PIN and card must be present at the time of the sale. Card parameters personalised to the chip by the issuing bank will allow a certain amount of off-line transactions. In the event that the fraudster disables the chip (e.g. by placing adhesive tape over it or micro waving it), the transaction will default to the magnetic stripe which will automatically come on-line for

authorisation. The key drivers for the anticipated increase in authorisation traffic will be the following:

- The card parameters personalised to the chip
- The point-of-sale parameters personalised to the point of sale
- The number of default to magnetic stripe transactions
- The number of "face-to-face" transactions conducted via the physical channels
- The number of chip cards in the market
- The EMV roll-out strategy of the issuing and acquiring banks
- The card and merchant base growth and the propensity to use and accept credit cards in the domestic market.

Chip and PIN (EMV) may inadvertently contribute to increased authorisation volumes that are currently not experienced in production. In most instances the issuer cannot write-back to the chip to change the chip parameters initially personalised to the card. The only way to mitigate the increased authorisations where the issuing and/or acquiring bank are experiencing service degradation (due to system constraints) would be to:

- Recall the plastic from the customer and reissue cards with a higher offline transaction capability *and/or*
- Scale up the systems to accommodate the increase in authorisations.

A further exacerbation is that the fraud funding contained within the card interchange is insufficient to cater for the fraud losses incurred on the credit card products. As floor limits contribute substantially to the fraud losses, the profitability of the issuing bank is reduced due to the floor limit infrastructure. The fraud funding in the interchange in relation to the fraud losses experienced is not discussed in this research report due to the competitive nature of the calculations and the complexity of the various interchange rates and fees per product type. This is excluded in the delimitations section of this research report.

6.3.2 The second Proposition is that South African telecommunications can sustain a zero floor limit. The research done has provided evidence that the technology exists in the market to support and sustain a zero floor limit. The survey done with

the telecommunications and technology service providers and vendors in the market has afforded confirmation to this end. If one considers the questions asked in the survey and the concomitant responses, it is apparent that this is indeed the case. The following questions answered in the survey by the telecommunications service providers lend weight to this:

"The local telecommunications infrastructure (telephone, radio pad or GPRS) from the point of sale to the issuing bank during an authorization request has the ability to sustain a zero floor limit". The telecommunication and technology respondents answered "Agreed" and "Strongly Agreed". The mode for the decoded responses was "4" with the entire distribution of the responses under the "Agreed" and "Strongly Agreed" categories of the applied Likert scale. The technology is currently deployed in the domestic credit card market. The merchant decides on the respective technology that it will use to fulfill credit card processing. The acquirer gives advice to the merchant on the most efficient and cost-effective solution to accomplish the processing. The acquirer does not own nor maintain this network as it is not part of the core business of the acquiring bank. The merchant is responsible for signing up with a chosen service provider as it is the merchant that is accountable for the operational costs and overheads to that particular service provider. GPRS technology is the most cost effective and contemporary technology that can be used to meet the requirements of a zero floor limit. It is an "always-on" technology, as a user can remain connected for long periods without transmitting any data. GPRS has several unique factors such as the speed. The maximum speed of a GPRS connection is around 171.2 kbps when using all 8 of the GPRS timeslots at the same time. This is around three times as fast as the usual data transmission speeds over today's fixed telecom networks and ten times faster than the CSD or circuit switched data on the GSM Networks. GPRS works by allowing all the information to be transmitted more quickly, immediately and efficiently across the mobile network. GPRS is also less costly to send data than SMS and Circuit Switched Data. GPRS connects instantly so information can be sent and received immediately as and when the need comes up – depending on radio coverage. Connectnet commented that *"A zero floor limit is easily attainable when using GPRS, because transactions take less than 10 seconds to be processed. It will also not increase the customers cost*

per transaction, because monthly call charges are fixed on GPRS". Fastnet commented on authorizations and floor limits by stating *"Unlike the rest of the world (which doesn't use them as far as we know), floor limits exist because of two fundamental issues:*

- *The slower speed of online transactions via telephone causing queuing issues at retailers.*
- *The increased volumes of online authorizations causing server load on the Bank's server.*

We believe that approximately 80% of Standard Bank's authorizations are below the floor limit. Making all authorizations go online therefore implies a five-fold increased in load (100%/20%) to the authorization servers. Since these servers already run at high loads during peak periods, this is a problem".

The comment on floor limits being introduced in order to mitigate the load that the volumes would have on the issuing and acquiring bank's hardware and software is supported by the research. The adoption of floor limits was a technological constraint when credit cards were initially introduced into the market in the latter half of the twentieth century. Technology has developed with the microprocessor being the culmination of the explosive growth in telecommunications and technology. This technology has enabled the growth of high-power, low cost computing which allow the microprocessor to encode, transmit and decode the vast amounts of information along electronic highways. The cost of microprocessors continues to fall while their power increases (a phenomenon known as Moore's Law, which predicts that the power of the microprocessor technology doubles and its cost of production falls in half every 18 months). As this happens, the costs of global communications are plummeting.

The GPRS may be a viable solution but it has its constraints as well. Interviews had with technology experts within Standard Bank (D, Els, N, Jansen, Network Architects – Infrastructure Solutions Design, 2007 Personal Interview, 06 August 2007, 5 Simmonds Street, JHB) have warned about the time slots and coverage of GPRS services. The resource is neither infinite nor infallible. The 8 time slots are not dedicated to data transmission only. The time slots are shared with voice

(caller conversations) transmission. The prioritization of the time slots and the concomitant load balancing, depending on the GPRS coverage, are key considerations to fulfilling a zero floor limit. To rely solely on GPRS for a zero floor limit may be counterproductive. Should a particular merchant trade in an area that has a high density of human traffic that are using their cellular telephones for voice transmission, the occupancy of the 8 time slots for data transmission pertaining to credit cards is not dedicated. This also needs to be seen in the context of the merchant's location in relation to the coverage afforded by the GSM base stations. Further constraints may include infrastructural restrictions in terms of the coverage barriers (e.g. high density concrete). Because service delivery and fulfillment to the merchant and the customer transacting with a credit card are vitally important, it is not prudent to rely solely on GPRS technology in light of the constraints mentioned above.

"The reduction of floor limits will not have a negative impact on cardholders at the point of sale". The majority of the respondents "Strongly Agreed" (the mode was "5"). This lends evidence to the fact that the telecommunications respondents have confidence in the infrastructure and technology to support a zero floor limit environment. This response is understandable due to the telecommunications technology available to the credit card industry. What is debatable is the issuer and acquirer's ability to handle the increase in authorization traffic as well as the data switches that route the authorization requests to the issuing bank. This is discussed under the fourth Proposition. The respondents' answer to this question is congruent to their answers *to "An increase in authorization volumes attributable to a zero floor limit will adversely affect issuers in their ability to process the transactions"* and *"An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions."* The majority of the responses were "Disagree" which provides an insight into the confidence these respondents have on the ability of the bank to handle the volume of authorization requests. One needs to consider the position of the acquiring bank in handling the authorization volumes. If a transaction is conducted on a credit card where the acquiring bank is not the issuing bank, it will need to receive the transactions from the merchant and route the authorization to the issuing bank. The concomitant authorization response would then be re-routed back to the

acquirer from the issuing bank. The acquirer's ability to handle the authorization requests and responses is as important as the issuer's ability to process the authorization request.

The Merchant Services personnel that service the merchant base from a sales and support perspective answered differently to the questions. Their answer *to "Local acquirers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests"* was "Disagree". This response was harmonious to their answer to *"An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions"* which was "Agree". The Merchant Services personnel do not get involved in the technical installation of the point-of-sale device nor the telecommunications services and support. It is their perceptions that are important in considering the technology school of thought as posited in chapter 2.

The stress test performed on Standard Bank's front-end processor (Postillion) suggests that the optimal metric for system performance is 65 TPS (prior to the upgrade after the stress test where the front-end processor has now doubled the processing capability as mentioned earlier). The data obtained from Standard Bank's data warehouse implies that had zero floor limits been introduced in 2006 under the old processing capability (assuming that postings followed the same distribution as authorizations), an increase in TPS ranged from 61 TPS to 91 TPS. This range exceeded the comfort zone on more than one occasion. At 65 TPS the system performs optimally with no degradation in service. The system is capable of absorbing transient spikes of over 100 TPS. When the system was stressed to 88 TPS, the system was performing under stress. Response times had degraded (by up to 200%) and reduced service was being offered with some transactions being discarded as volumes grew towards 88 TPS. Transient volume spikes will temporarily decrease the grade of service further. Over-stressed results (over 88 TPS) showed that the performance is severely retarded. System behaviour was erratic with response times between 200% and 800% worse than those experienced at 65 TPS. The stress tests show that a hardware upgrade (increase in available CPU capacity) would be required before transactions rates of more than 65 TPS could be sustained for periods exceeding a few minutes. This

upgrade took place but has not been stress tested yet. The calculated expansion in TPS as a result of a theoretical zero floor limit (up to 91 TPS), does not take into consideration the growth in the card base over time which will increase sales and concomitant TPS. This further suggests that service degradation could occur in terms of responding to authorization requests in a timely manner. An upgrade to the front-end system infrastructure would need to be done to accommodate the full zero floor limit environment. As Standard Bank may encounter system constraints as an issuer in processing the authorization requests (and adversely affect its cardholders), it will also encounter constraints as an acquirer (and adversely affect its merchants and issuers' cards used at the merchants). The 65 TPS threshold mentioned even all transactions including those acquired by Standard Bank. *Figure 48* illustrates this scenario:

Figure 48: Standard Bank's distinction between issuing and acquiring authorisations

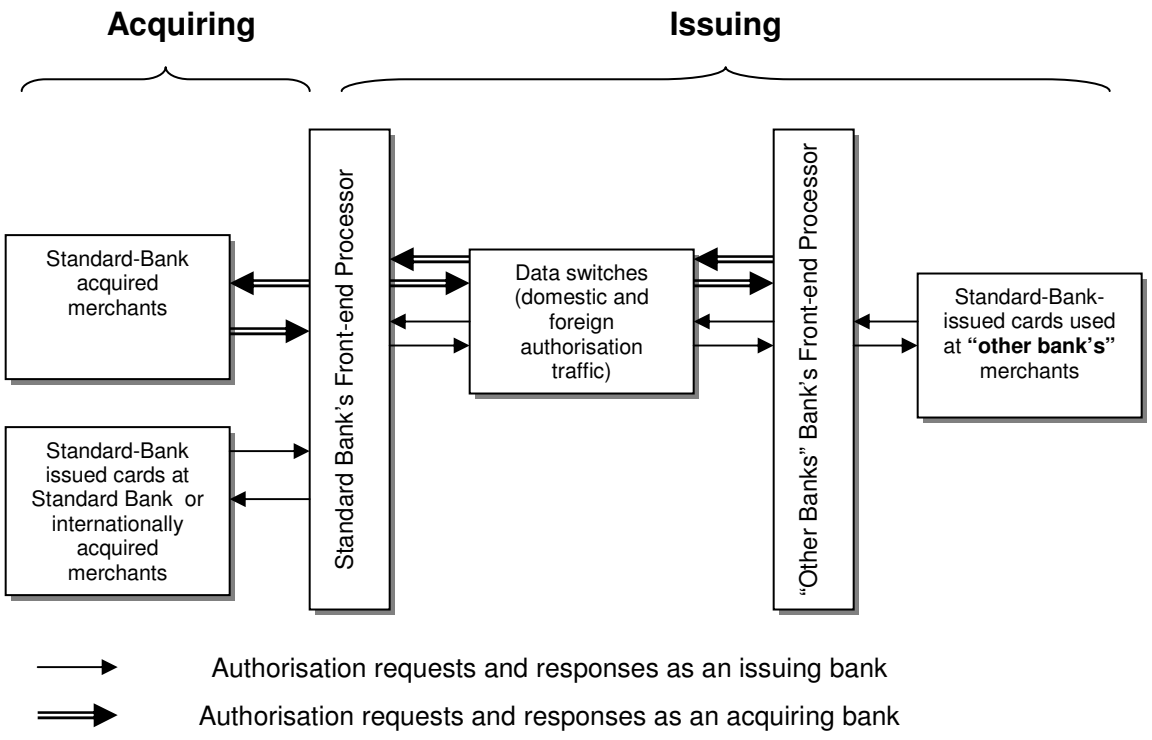


Figure 48 illustrates the role that Standard Bank's front-end processor plays in authorizing transactions. Standard Bank will authorize cards issued by it as well as route transactions where other card issuers' cardholders transacted at Standard Bank merchants (the acquiring segment illustrated in the figure). The service degradation due to not being able to service the increase in TPS, will affect other role-players in the domestic market notwithstanding the following:

- Domestic agent banks (as card issuers),
- Standard Bank-issued cards and their cardholders,
- Standard Bank acquired merchants,
- International banks whose cardholders use their cards at Standard Bank merchants,
- Transactions switch (Bankserv).

The technology and telecommunication respondents' response to *"Issuers and acquirers can wait for the full implementation of EMV (CHIP and PIN) as a solution to reducing fraud"* was "Disagree". The respondents acknowledged in their comments that the roll-out of chip within the South African industry would be slow. This is further supported by the Merchant Services and Fraud Risk Management personnel. The implementation of EMV is expected to curtail fraud losses due to the on-board chip parameters personalized to the card and the merchant's point-of-sale device. This, coupled to the fact that a PIN is used to authenticate the cardholder other than signature, is a further risk mitigation expectation. PIN is more secure than signature as a cardholder authentication mechanism. The doubt expressed by the respondents is related to the lethargic roll-out of chip (EMV). As most magnetic-stripe credit cards enjoy two year expiration dates (whereupon a renewal card is sent to the customer), it is expected that the chip roll-out to the entire card issuing base could take up to two years. A further risk mitigation is that should the on-board chip be damaged, the transaction will automatically revert to the magnetic stripe which will by design be subject to a zero floor limit. This operational functionality must be taken into consideration as it may further exacerbate the ability of the issuing and acquiring bank to handle the authorization volumes. The dependency on when an EMV transaction goes for authorization is dependent on:

- The EMV parameters personalized to the chip
- The EMV parameters personalized to the point-of-sale device
- The functioning of the chip at the time of sale

In the event that the issuing and acquiring bank do not do the respective research in setting the chip and point-of-sale parameters, coupled to the chip functionality (whether the card is used at an EMV-enabled point-of-sale device or fallback to magnetic stripe), the authorization volumes may prove to be onerous for the issuing bank.

6.3.3 The third Proposition is that the cost of introducing a zero floor limit in South Africa is negligible in relation to the fraud which floor limits sustain. It has already been mentioned that the domestic fraud within the South African credit card market in 2006 was R179M of a total of R257M. This comprised 70% of the South African bank-issued credit card fraud that was perpetrated in South Africa. Of this figure, a further anticipated 35% was perpetrated below the merchants designated floor limit (based on the calculations done in chapter 5). The costs of the various technologies are listed below:

Telephone Line

Service	**Tariff**
Business installation	R342.30
Monthly Rental	R132.75
Local calls (0-50km) – peak rates	
Minimum charge for the first unit of 89 seconds	R0.59
Long distance calls (> 50km) – peak rates (per minute)	R0.72
Outgoing calls to mobile network (1 minute)	R1.89
International calls to the United States – peak rates (per minute)	R1.20

Source: Telkom South Africa, BMI-T, 2006 (387)

GPRS

	Lite	Standard	Express
Monthly charges (ex VAT)	R 175.00	R 195.00	R 295.00
Nº. of Transactions per month	600	1800	3000
Data Cap per month	0 - 1.5MB	1.5-2.5mb	2.5-10mb

Source: www.xlink.co.za

Fastnet Radio Pad Tariffs

Purchased Radio PAD (becomes the property of the customer)

Option	Connection Fee (Once-Off)	Monthly Maintenance Fee	Call Charges (Peak Hours)	Call Charges (Off-Peak Hours)
Radical	R75.30	R30.75	11.5 Cents	11.5 Cents

Rented Radio PAD (Remains the property of FastNet)

Option	Connection Fee (Once-Off)	Monthly Maintenance Fee	Call Charges (Peak Hours)	Call Charges (Off-Peak Hours)
Benefit	R75.30	R80.50	43.5 Cents	18.0 Cents
Merit	R75.30	R126.40	31.5 Cents	18.0 Cents
Value	R75.30	R178.50	18.0 Cents	18.0 Cents

Source: www.fastnet.co.za

If one considers the costs mentioned above, it becomes apparent that from a merchant's perspective, the cheaper telecommunications option for authorising transactions is GPRS. A break down of the costs shows the following:

Telephone fixed cost range (excluding installation): R132.75 per month
Telephone variable cost range: R0.59 to R1.89 per call

GPRS fixed cost range (excluding installation): R175,00 to R275,00 per month
GPRS variable cost range: **Nil**

Radio Pad fixed cost range (excluding installation): R30.75 to R178.50 per month

Radio Pad variable cost range: R0.115 to R0.435

To work out a generic telecommunications cost for a merchant would not be viable as their credit card volumes are dependent on many factors notwithstanding:

- The merchant's location
- The merchant's patrons and their propensity to purchase with a credit card
- The nature of the merchant's merchandise
- The seasonality of the merchant's sales.

In considering the costs associated with the telecommunications deployed, one must also consider the speed and efficiency and reliability of the service. In obtaining the comments from the telecommunications service providers survey, XLINK mentioned *that "Yes, the merchant's telephone costs will increase substantially if they dial up through Telkom. Merchants using GPRS bill might increase slightly as this is dependent on X.25 and if they go over the packaged number of transactions".* A further interesting statement made by X-Link that supports the mentioned disintermediation of X.25 mentioned in chapter 3 is "*X.25 is another point of failure – acquiring banks should consider moving to IP (internet protocol)"*. Connectnet mentioned in their survey *"A zero floor limit is easily attainable when using GPRS, because transactions take less than 10 seconds to be processed. It will also not increase the customers cost per transaction, because monthly and call charges are fixed on GPRS".* Both of these statements support the research done on the speed and efficiency of GPRS. It is clear that GPRS is the better technology to adopt if one is considering speed, cost and efficiency. The questionable component of GPRS technology as mentioned above is the dedication and reliability of the service due to the occupancy rates of the 8 time slots for data and concomitant infrastructural considerations. Fastnet commented on telephone telecommunications as a data conduit from point-of-sale by stating *"telephone dialup authorizations take 40 to 60 seconds to connect and complete (versus 10 to 15 seconds on Radio PAD and GPRS), which causes queues to form at retailers during peak periods".*

The costs of introducing a zero floor limit are not only restricted to the telecommunications from a point-of-sale perspective as positioned above. One needs to consider the following costs as well:

- The cost for the issuing bank and acquiring bank to scale up their hardware and software to deal with an increase in authorization volumes.
- The cost to the merchant in terms of the increase in their operational costs to fulfill a zero floor limit environment (principally telecommunications costs).
- The cost to the merchant in the event that the telecommunications selected to support a zero floor limit environment loses sales due to the "timing-out" of the authorization request
- The cost to the acquiring bank of losing market share due to merchants moving to competitive acquirers which may still offer floor limits as negotiated with the issuing banks.
- The potential loss of interchange revenue by the issuing bank and reduced commission revenue by the acquiring bank. The merchants may argue that the risk associated with the credit card transactions does not warrant the interchange rate paid on these transactions due to the lesser risk associated with the authorized transaction. As already mentioned in this research report, acquirers pay issuers interchange to cover the issuer's cost of funds (in funding the credit), fraud and credit risk and other operational costs the issuer may incur. The acquirer recovers this fee from the merchant by charging a commission on every transaction.

Almost every merchant in South Africa has electronic point-of-sale devices (stand alone or integrated solutions). This requirement is a prerequisite to facilitate card transactions. The most feasible telecommunications solution purely from a cost perspective would be GPRS.

6.3.4 The fourth Proposition is that the local banking infrastructure and technology can accommodate an increase in authorisations as a result of a zero floor limit environment. The analysis done on the ability of the domestic switch (Bankserv) and Standard Bank (as an issuer and as an acquirer) to handle the authorisation traffic attributable to a zero floor limit environment was discussed in chapter 5. It

appears that the domestic switch has the ability to handle the anticipated increase in Standard Bank authorisation traffic. As mentioned, the highest authorization activity on cards for the month occurred on the 22nd December, peaking at 71.9 TPS. Bankserv have confirmed that their maximum TPS threshold is 156 TPS for one site. Bankserv process authorizations via two separate sites (continuous processing) to balance the load and each site can maintain 156 TPS concurrently (reference: Bankserv). This results in a total TPS threshold of 312 TPS processing capability. The anticipated increase in authorization volumes in a zero floor limit environment from a local industry perspective has not been determined. This is due to the sensitivity of the data amongst the local competitors and the differentiation between transactions that are switched by the domestic switch and transactions that go directly to the issuer bypassing the domestic switch altogether. The analysis done with Standard Bank's data for 2006 presents the following theoretical increase in authorization traffic had zero floor limits been introduced in 2006:

Table 30: Anticipated increase in authorisations had a zero floor limit been introduced

Month	Increase (%)	Max Authorizations per Second
Jan-06	85%	61
Feb-06	77%	62
Mar-06	70%	62
Apr-06	69%	80
May-06	72%	66
Jun-06	67%	65
Jul-06	65%	77
Aug-06	70%	66
Sep-06	65%	86
Oct-06	70%	70
Nov-06	65%	69
Dec-06	59%	91

The anticipated increase in authorisation traffic had zero floor limits been introduced in 2006 is reflected in the table above. The combination of authorisations and postings (batched transactions – i.e. transactions conducted below the merchant's floor limit) comprises the increase in authorisation traffic above. The maximum TPS that occurred was in December 2006 at 91 TPS.

Albeit that Standard Bank had scaled-up its front-end processor (Postillion) where it originally had a comfort zone of 62 TPS to double the capacity (from a comfort zone perspective) to a theoretical 124 TPS, it cannot be alluded that the spare capacity is 33 (the difference between the 124 TPS and 91TPS). The logic may be sound on a mathematical basis, however, the relationship between the CPU usage, the TPS and system memory consumption is *not linear* (as suggested by the calculations) and cannot be argued mathematically as done above. CPU consumption is positively correlated to memory use and TPS (as shown in the stress test results). No logarithmic scale is available at Standard Bank to represent this relationship. In order to unequivocally prove whether the front-end processor can handle a zero floor limit, a stress test (acid test) must be performed where a zero floor limit based on production volumes is used. This stress test will differ from the original stress test performed in that its primary objective is to test zero floor limits (as opposed to stress test the Postillion by injecting multiple transactions). The two stress tests are not dissimilar from each other in that they both put the front-end processor and ancillary systems under stress (volume testing). The key differentiator however, is that zero floor limits are tested which will give us a clear indication of the processing ability, queue lengths, queue waiting times, CPU usage and response times of the front-end processor and peripheral systems. This stress test must consider the increase in volumes as an issuing bank and as an acquiring bank as illustrated in *figure 48*. If the domestic industry follows suite in terms of introducing zero floor limits, the multiplier effect on Standard Bank's front-end processor as well as the domestic agent banks (as issuers and acquirers) and local switches would need to be determined. The research done has been on Standard Bank's ability to process transactions in a zero floor limit environment. With the exception of the stress test performed, Standard Bank–issuing volumes have been considered only (Standard Bank cards are used in the domestic credit card market at all acquiring bank's merchants). The acquiring portion of Standard Bank in terms of routing authorization requests to other issuing banks have not been taken into consideration (other than in the stress test). In the event that merchants which are acquired by Standard Bank are placed on a zero floor limit, the multiplier effect would be substantial. The reason for not incorporating the acquiring volume is that this has not been readily available at the time of this research report. Card and sales growth (including

merchant sales and banking growth) would need to be tested as well to determine the anticipated growth in the number of transactions over time.

Based on the initial stress tests performed on Standard Bank's front-end processor as well as Bankserv's ability to theoretically handle an increase in Standard Bank's authorization traffic provides a theoretical baseline to suggest that Standard Bank cannot sustain a zero floor limit environment. This however is not a complete synopsis of the entire industry as the selfsame studies need to be performed by the domestic banks with due consideration on Bankserv as the domestic switch on their concomitant volumes.

6.4 Conclusions

Below floor limit fraud is a worrisome concern for domestic issuers and acquirers. The advent of chip and PIN is expected to reduce the below floor limit fraud initially. The migration to other fraud types is expected notwithstanding false application and card number used fraud. In a recent press release (M, Keegan, *CNP Growth in the United Kingdom*, Bankserv, 2007) confirmed this by stating *"CNP fraud has shot up by 22 per cent in the past 12 months alone. This is largely because the advent of `chip and PIN' makes it far more difficult for criminals to get away with using stolen credit cards in the shops."* A further article by APACS (www.apacs.org.uk, 2007. "*Transactions with your chip and PIN terminal"* Available from http://www.apacs.org.uk [Accessed 12 September 2007], state that *"The first chip and PIN transaction in the UK took place in Northampton in May 2003. Today, just four years on, more than 900,000 shop tills (98 per cent of all shop tills in the UK) have upgraded to chip and PIN with over 185 chip and PIN transactions taking place every second. This new way to pay has been a positive step forward for card security in the UK and, as a result, card fraud losses on the high street have fallen 67 per cent since 2004".*

Albeit that issuers and acquirers adopt chip and PIN in the South African market and follow the rest of the world in adopting this technology, the magnetic stripe is expected to be part of the credit card transactability in the next 5 years at least. The reason for this is that many merchants and acquirers in the world are lagging behind the investment in chip and PIN. Many merchants' point-of-sales will only accept the magnetic stripe technology and in order not to lose potential sales, the issuing bank will still issue cards

to its cardholders with this technology. The impact that chip and PIN will have on the domestic issuer's ability to process an anticipated increase in online transactions is not completely known. Standard Bank is theoretically able to handle the anticipated increase in authorization traffic assuming a zero floor limit, but this statement is based on the stress test performed on injected transactions and not an assumed zero floor limit scenario. The processing ability of the upgraded front-end processor (doubling the old processing speed (124TPS of assumed comfort zone)) was not stress tested. The stress test volumes over the tested period suggest that production volumes will not reach the thresholds reached during the stress test. This however, excluded the assumed increase in authorization volumes for a tacit zero floor limit. The stress test performed 409,000 transactions over one-hour and twenty minutes which suggests an average TPS of 85. If one considers the anticipated increase in authorization volumes had a zero floor limit been introduced (from an issuing perspective only) in 2006 *(Appendix 4)*, it becomes theoretically apparent that this average will be met in production. The stress test goal was to increase the injected transactions to put the hardware and software under stress. The increase in injected transactions amplified the average TPS before the system returned to normal processing.

The multiple data systems and intermediaries (and their concomitant systems and processing capability) in the credit card model are key dependencies to ensure that the transactions is sent to the issuer and acquirer and processed within reasonable time frames. If one takes the theoretical production volume spike in December 2006 (an estimated 91 TPS) and compares this to the processing capability of the front-end processor and peripheral front-end systems (124 TPS), this represents a capacity cushion of 33 TPS (or 1980 transactions per minute). This was discussed in the previous chapter. This may not be contingency enough to cater for a zero floor limit environment. The data obtained and analyzed represents averages (TPS) only and may not accurately represent transient spikes in a production environment (peak purchasing times or seasonal credit card spend). As the relationship between TPS processing capability and authorization requests is not linear (it is more logarithmic), the ability to ascertain the actual impact of zero floor limits is difficult. The CPU processing ability, and queue lengths and waiting times for the authorizations are further considerations that need to be tested.

The convenience and speed of use of the card product at point-of-sale and other physical channels from a customer's perspective is integral to the value proposition. This is coupled to the customer's expectations of security in using the product. The disintermediation of the X.25 network In Standard Bank (as discussed in Chapter 2) would assist in the speedier transportability of the transaction. It was confirmed that the X.25 protocol is archaic and outdated. Standard Bank would be better positioned to service its merchants and their customers by using GPRS and receiving the transactions directly into its infrastructure and avoiding the X.25 protocol. GPRS is a potential solution to reducing the merchant's costs in deploying a technology that would facilitate quicker authorization requests and responses (again dependent on the issuer's and acquirer's ability to process transactions). The reliability of the service is questionable due to the time slots and channels afforded to data and voice and the coverage that the base stations afford. To rely solely on this technology where the load balancing and capacity planning by the service providers may be dependent on the above factors is too risky for acquirers The risks and associated costs are mentioned below. A further consideration is the merchant categories where fraudsters generally spend. The majority of the fraud takes place at supermarkets, grocery stores and department stores. These merchants generate the greater part of the retail volume. These large retailers see the customer as one of their patrons and invest large sums of money in increasing their patronage and prompting repeat purchases. If their clients are continually negatively impacted by delays in purchasing with a credit card attributable to the technology adopted (slow telecommunications and issuer/acquirer response rates), they may lobby against the domestic issuers and acquirers. The issuing banks' brand integrity and that of the associations (MasterCard and Visa) is at risk as well as that of the retailers themselves. The large retailers have a substantial market of customers that take-up their in-store credit cards. This is currently a competitive value proposition to credit cards issued by domestic banks. The competition in this arena may increase and result in bank-issued credit card patronage attrition to the competitor products.

The commercial engagement with merchants necessitates a responsible approach by acquirers. To negotiate a single technology in the form of GPRS and rely on the service providers to fulfill the data requirements in terms of increased authorization traffic may cause the merchants to lobby for reduced commission fees. The reduced risk (fraud and credit risk for the issuing bank) of sending authorizations online for issuers to process

may further exacerbate the lobby issue. As fraud funding is inherent in the interchange (which is part of the merchant commission that is paid to the acquirer), merchants may argue that risk is reduced and hence interchange should be adjusted accordingly. As interchange on an entire card base (where this fee is applicable) is a key revenue stream for issuing banks, the costs of reduced interchange in relation to the fraud savings (on a small portion of the card base) may present an interesting analysis. If acquirers promote GPRS to its merchants and transactions are not fulfilled due to technological capacity constraints (as already mentioned), the following may occur:

- Slower response times from issuing banks. This may cause the cardholder to question the product in fulfilling the cardholder's needs of speed, convenience and ease of use. This may also cause the cardholder to question the merchant's ability to fulfill the selfsame needs.

- The merchant's operational costs will increase as the authorization request may "time-out" resulting in the merchant telephoning the acquiring or issuing bank for authorization. This not only results in increased telephony costs but delays the sale and causes queues to swell at the purchase point which may lead to loss of sales on the part of the merchant.

- The loss of revenue for the merchant may result in them seeking recourse from the acquirer.

In order to implement a zero or reduced floor limit policy, it has to be introduced by the domestic issuing and acquiring banks collectively. The timing of the implementation is an important consideration. In the event that an issuer or acquirer defers the respective implementation, it would trade-off its fraud losses for increased market share. Merchants and/or cardholders may migrate to the late adopter of this initiative as the costs and convenience from a merchant or cardholder perspective would be better fulfilled by the laggard. The regulation of this adoption is currently under the ambit of MasterCard in their publication. The 2005 MasterCard International published mandate (Appendix 5) states that "Effective 8 April 2006, MasterCard will require a card acceptor *(acquirer)* to obtain an authorization from the issuer for:

- All non face-to-face transactions, regardless of the transaction amount,

- All face-to-face transactions, card-read or key-entered, occurring at a location with a point-of-sale (POS) device that has both online and magnetic stripe-read capability, regardless of the transaction amount"

Table 31 holistically summarizes the dependencies and issues in adopting zero floor limits in the domestic industry.

Table 31: Issues, dependencies and comments in adopting zero floor limits

Technology		
Issue	**Dependency**	**Comments**
Chip and PIN	Chip and PIN is dependent on the issuing and acquiring bank's roll-out to cardholders and merchants and all physical transaction channels such as point-of-sale and ATM.	Magnetic stripe technology is expected to be in the South African market for the next 5 years. It may take issuers up to 2 years to roll-out chip and PIN to their card base. Some products may not be converted to this technology. The cost of the chip versus the fraud savings is a further consideration.
Zero floor limits	GPRS at point-of sale.	GPRS affords a quicker and a more cost-effective solution to merchants to adopt a zero floor limit.
GPRS	The ability of the service providers (cellular telephone companies) to ensure that the infrastructure (radio coverage) is sufficient to support all areas. The load balancing of the 8 time slots and the dedication given to data in these time slots is a further dependency.	The 8 time slots are not dedicated to data transmission only. The time slots are shared with voice (caller conversations) transmission. The prioritization of the time slots and the concomitant load balancing, depending on the GPRS coverage, are key considerations to fulfilling a zero floor limit. To rely solely on GPRS for a zero floor limit may be counterproductive.
Data intermediaries	Data intermediaries' dependency in terms of zero floor limits is their hardware,	Bankserv have the theoretical infrastructure to handle a zero floor limit in terms of their hardware and software.

	software and telecommunications protocols.	This has not been stress (volume) tested. The disintermediation of the X.25 protocol by issuing banks and the conversion and processing of the TCP/IP protocol may expedite the authorization requests and responses.
Issuer and acquirer infrastructure	Issuer and acquirer's ability to process increased authorization volumes is dependent on system hardware, software and communication protocols.	Standard Bank have the theoretical capacity to handle reduced or zeroed floor limits. This however is subject to a stress (volume test) that tests for zero floor limits in particular
Standard Bank's front-end processor and peripheral systems	The CPU processing ability and queue lengths and waiting times for the authorizations.	The data obtained and analyzed represents averages (TPS) only and may not accurately represent transient spikes in a production environment. As the relationship between TPS processing capability and authorization requests is not linear (it is more logarithmic), the ability to ascertain the actual impact of zero floor limits is difficult.

Pricing and Associated Costs		
Issue	**Dependency**	**Comments**
Merchant commission	The merchant commission that is paid to the acquirer contains an interchange rate on most credit card transactions. The reduction of floor limits may depend on the negotiation of reduced interchange rates and hence merchant commission.	Acquirers argue that the commission paid to acquirers comprises an interchange fee that has an inherent fraud loss funding mechanism and that by reducing or zeroing floor limits, the merchant is prejudiced in that their operational costs will increase (due to the additional authorization traffic which

	The loss of revenue in reduced interchange may not support the fraud losses experienced as a result of reducing or zeroing merchant floor limits. The revenue earned by acquirers may be reduced.	will increase the communication costs) whilst the fraud funding in the interchange model remains the same. They argue that the merchant would need to be compensated in the form of a reduced interchange (which the acquirer recovers from the merchant and pays the issuing bank) to cater for the increased operational costs.
Interchange rate	Acquirers pay issuers interchange in South Africa as inherent within the credit card model. The dependency on implementing zero floor limits may be reduced interchange to the issuing bank (with a concomitant reduction in revenue).	The risk-funding is inherent within the interchange that the acquirer pays the issuing bank for every sale. Interchange is generally set to 1.71% of the sale. There are two main categories of risk in this funding, namely credit risk and fraud risk. Fraud risk funding in the interchange (1.71%) is roughly 0.12%.
Merchant overhead	The merchant's overheads are dependent on the technology deployed to support a zero floor limit environment.	Should the technology not enable quick and speedy responses to authorization requests, the merchants will have to telephone for authorization which will delay processing sales and increase queues at point-of-sale and may also result in a loss of sales.

Competition and Customer Fulfillment		
Issue	**Dependency**	**Comments**
Large retail categories representing the largest volumes of	The dependency is on the ability of issuers and acquirers to fulfill the service expectations of the large retailers (supermarkets, grocery stores,	The large retailers have a substantial market of customers that take-up their in-store credit cards. This is currently a competitive value proposition to credit cards issued by domestic banks. The

transactions	department stores) and their customers.	competition in this arena may increase and result in bank-issued credit card patronage attrition to the competitor products.
Issuers and acquirers to collectively adopt zero floor limits	The dependency of adopting reduced or zero floor limits is on the industry timing the implementation together.	Should a domestic acquiring bank refrain from implementing a reduced or zero floor limit, it could steal market share from other acquirers.
Cardholder fulfillment	The dependency is on the technological infrastructure to support a reduced or zero floor limit environment.	The speed, efficiency, convenience and security of the credit card are integral to the customer value proposition. To maintain this value-add service it is important to reduce the inconvenience the customer may have at the point-of-sale.

6.5 Recommendations

The following recommendations emanate from the research and represent the most feasible solutions in adopting reduced or zero floor limits. Each recommendation is interdependent of the others and comprises a holistic solution for the domestic industry.

6.5.1 Incrementally reduce floor limits based on high risk methodologies

To implement a zero floor limit across all merchant categories may not be feasible in light of the technological constraints involved. A more prudent approach may be reducing floor limits incrementally based on a collective methodology. It is proposed that the high risk merchant categories and their respective geographies be determined first. The roll-out of the zero floor limits must be aimed at these establishments. The high risk establishments as determined by SABRIC in chapter 1 comprise:

Merchant Category	Amount	% Contribution to total
Grocery Stores and Supermarkets	R 17,749,223.63	21%
Department Stores	R 13,550,846.39	16%
Service Stations	R 13,450,314.50	16%
Family Clothing	R 8,215,591.31	10%
Men's and Boy's Clothing and Accessories Stores	R 5,761,266.15	7%
Package Stores Beer, Wine, and Liquor	R 5,748,439.43	7%
Eating Places and Restaurants	R 4,936,593.36	6%
Betting	R 4,756,085.21	6%
Financial Institutions (Manual Cash Disbursements)	R 4,447,530.63	5%
Financial Institutions (Automated Cash Disbursements)	R 4,133,097.30	5%
Total	R 82,748,987.91	100%

The high risk merchant categories as determined by Standard Bank comprise:

Merchant Category	Amount	% Contribution to total
Service Stations	R 14,182,599.58	28%
Grocery Stores, Supermarkets	R 10,895,993.57	22%
Clothing and Furnishings Stores	R 5,964,783.85	12%
Restaurants	R 4,302,810.67	9%
Clothing and Furnishings Stores	R 4,214,518.50	8%
Liquor Stores	R 3,043,746.39	6%
Department Stores	R 2,172,876.75	4%
Fast Food Restaurants	R 1,964,399.33	4%
Drug Stores & Pharmacies	R 1,558,427.93	3%
Home Furnishing Specialty Shops	R 1,506,709.28	3%
Total	R 49,806,865.85	100%

The top merchant geographies comprise:

City	Amount	% Contribution to total
JOHANNESBURG	R 28,239,690.56	31%
PRETORIA	R 11,979,679.19	13%
SANDTON	R 11,234,818.99	12%
DURBAN	R 10,780,031.78	12%
CAPE TOWN	R 8,097,703.04	9%
RANDBURG	R 5,321,512.76	6%
ROODEPOORT	R 5,078,364.66	6%
BOKSBURG	R 3,516,826.07	4%
KEMPTON PARK	R 3,268,735.36	4%
CENTURION	R 2,531,799.77	3%
Total	R 90,049,162.18	100%

The roll-out must take into consideration the nature of the merchant's average ticket value which is based on the merchandise that the merchant sells. Those merchants that generate the majority of the authorization volumes due to the

nature of their merchandise are also a key consideration. The large retailers that have the technological infrastructure to host an industry negative card file must be differentiated from the smaller merchants that use a conventional point-of-sale machine.

Once these segmentations have been performed, it is possible to implement a strategy to reduce or zero floor limits. The incremental roll-out approach is supported by the respondents in the survey done. This roll-out is envisaged to include high risk merchant category codes in high risk geographical areas. The following high-risk merchant category codes namely, service stations, restaurants and liquor stores in the greater Johannesburg area can be placed on a zero or reduced floor limit by the domestic banking industry as an initial pilot. These merchants generally have a stand-alone point-of-sale device (and the INCF file is not a current solution for these establishments). This solution is, in itself, a proactive step toward reducing below-floor limit fraud. The problem, however, is that the fraud is expected to migrate to other merchant categories in the same area or the same merchant categories in other geographical areas.

6.5.2 The industry negative cards file roll-out to large retailers.

Many large retailers currently subscribe to the industry card file as provided by Retail Decisions. Not all large retailers however, receive the full negative card file and may only receive subsets which list the most recent compromised cards. This solution has reduced post-statussed fraud (by the issuing bank) at the subscribed establishments. Post-statussed fraud is fraud that takes place after the card has been statussed lost, stolen or fraud by the issuing bank. The post-status nature of the fraud is as a result of the four-day fraud life cycle as detailed in this research report. The problem with this type of solution is the following:

- Pre-statussed fraud (by the issuing bank),
- Reliance on the merchant's hardware and software infrastructure,
- The segmentation of merchants receiving a full file as opposed to a subset file,
- The reliance on merchants to invest in upgrading their infrastructure to accommodate an industry negative card file,
- The reliance on acquirers to incentive merchants to adopt this solution,

- The migration of fraud to non-subscribed merchants and other channels,
- The service only confirms whether a card is on the restricted list and does not cater for generating exceptions based on abnormal usage or deviations from the cardholder's spending profile.

The service provider is merely an intermediary in the provision of these services and relies on merchants, issuers and acquirers to provide the solution for its services. The decentralization of the issuer's exception file (compromised cards and cards abused by cardholders) is the best option in an environment that supports a floor limit. It would be better to disintermediate this service provider by allowing all transactions to go to the issuing bank for authorization as the issuers are able to detect questionable cardholder activity. This is due to the fact that the cardholder's transaction history and other information are contained at the issuing bank. To centralize the solution (i.e. all transactions go online to the issuer for authorization) is too risky as an initial adoption (due to the envisaged technological constraints that may prevent this from happening). This assumption is based on the analysis done on Standard Bank's front-end processor (and in the absence of a stress test centered on zero floor limits alone as already discussed).

In order to leverage the decentralized model (and mitigate the technological issues from an issuer's perspective), it would be prudent to adopt the recommendation set out in section 6.5.1 *and* investigate the possibilities of:

- Providing incentives to merchants to upgrade their infrastructure or
- Networking shopping malls and similar retail configurations
- Adopt GPRS as an initial telecommunications technology with a secondary technology to cater for GPRS "time-outs"
- Provide telecommunications hardware and software using existing telecommunications networks

6.5.3 Network shopping centers

A possible solution to mitigate the constraints with the decentralized restricted card file concept (the industry negative card file) is to create a local or wide area network within shopping malls. The constraints mentioned in 6.5.2 can be

mitigated if the industry negative card file resides within large shopping malls and all merchant's point-of-sales communicates with a centralized server. The maintenance of the local area network can be outsourced to the current (or other) service provider. The issuing bank will transmit their exception cards to the service provider who in turn will ensure that the cards are placed on the server. The issuer currently trickle feeds statussed cards on a 15 minute basis to the service provider. This methodology can still be adopted in the decentralized model. Those retailers that have their own integrated solutions (a client-server in store as opposed to a stand-alone point-of-sale) can be networked with the respective shopping mall server. Those merchants that have a stand-alone point-of-sale device can be configured to communicate with the server using telephone line, radio pad or GPRS. This will cut down on the telecommunications costs associated with connecting with the acquiring or issuing bank from a remote site.

6.5.4 Adopt GPRS as the first dial-up with a secondary technology for contingency purposes

The merchants can be prompted to use GPRS technology as opposed to radio pad and telephone. Most merchants have a landline for telephone calls. A hybrid point-of-sale can be configured to first attempt to use GPRS and if there is a telecommunications failure, to automatically divert to telephone for dial-up. Technology exists in the market whereby the point-of-sale can be connected to telephone line and GPRS. As already discussed, there is no guarantee that the 8 time slots used in GPRS can be dedicated to data (as opposed to voice). Albeit that the fixed costs for merchants may be doubled (GPRS and telephone line), the costs associated with GPRS are negligible for those merchants that do a substantial amount of credit card transactions. The GPRS monthly rental can be subsidized to an extent by the issuing and acquiring banks.

6.5.5 Chip and PIN

The deployment of chip and PIN is an integral part of the floor limit solution. An off-line chip transaction where a PIN is keyed-in by the cardholder and the chip parameters mitigate fraud risk is a solution for lost, stolen, NRI and counterfeit

fraud. Should the chip be rendered inoperable by a fraudster and the transaction defaults to the magnetic stripe, it will automatically be subject to a zero floor limit. The chip parameters allow the customer to spend offline subject to limits (accumulative transaction counts and amounts) before the chip recommends to the point-of-sale device to go online for authorization. The limits comprise lower cumulative counts and amounts and upper cumulative counts and amounts. If the lower cumulative counts or amounts are reached, the point of sale will attempt to go online for authorization. In the event that the authorization attempt is unsuccessful, the transaction can still be performed offline (subject to PIN authentication). In the event that the upper cumulative counts and amounts are met, the transaction must go for authorization. In the event that this attempt is unsuccessful, the chip will not allow and further transactions to take place. In authorizing the transaction, the issuer sends a script back to the chip to reset the accumulated counters on the chip.

The ability to change the personalized chip parameters during an authorization is key to ensure that the load in terms of authorization traffic is reduced. At the moment, the chip parameters (upper and lower cumulative counts and amounts) are set on the chip and cannot be changed during an authorization request.

6.5.6 Service codes.

Contained within the magnetic stripe is a 3-digit numeric value (service code) that communicates with the point-of-sale on the nature of the product and where it can be used. The service code advises the point-of-sale whether the card is subject to a magnetic stripe transaction or alternative technology (i.e. chip), whether PIN must be keyed-in by the customer (or the transaction is signature-based), whether the transaction must come online for authorization, where the card can be used (domestically only or domestic and international) and the type of devices where the card can be used (point-of-sale devices, self service devices, etc). The issuing bank sets the service code for the product. For high risk products, the issuer can personalize the service code to force all transactions online or be subject to PIN (in which case all transactions must come online). Petrol cards and service stations represent a large portion of fraud as represented in section 6.5.1 above.

As petrol is regulated in the South African market by the government, the economics in terms of commission and interchange is different. No interchange is charged on petrol transactions and the issuing bank pays the acquiring bank a transaction fee for every sale. As petrol prices are subject to fluctuation and more often than not increase on a regular basis (fuelling inflation), the floor limits increase as the petrol price increases. The floor limit increase is based on collaboration amongst issuing and acquiring banks. In lieu of the growth in fraud perpetrated on these cards, it is not feasible to continue increasing the floor limits. It is questionable whether the pricing caters adequately for the growth in fraud losses and it is necessary to reduce floor limits at garages or change the service code of these products.

6.5.7 Bankserv

The domestic switch (Bankserv) can be used to deploy a restricted card file. As all online transactions conducted at merchants where the acquirer and issuer are not synonymous must be switched by this entity, it makes good sense to host the industry negative card file here. Bankserv's core competence is in the data switching realm and they invest to this end. To mitigate potential issuer and acquirer processing delays, all transactions can be sent online to Bankserv. Point-of-sale devices are personalized with "network user addresses (NUA)" that comprise the numbers or addresses the point-of-sale devices must connect to for authorization. There is more than one address personalized to the point-of-sale that allows the device to switch to different NUA's depending on the response time from the host machine (acquirer). For those merchants that do not switch via Bankserv (the acquirer and the issuer are synonymous), one NUA can be captured to send transactions to Bankserv for reference against the industry negative card file. Bankserv can potentially host the industry negative card file for all merchants that have a zero floor limit.

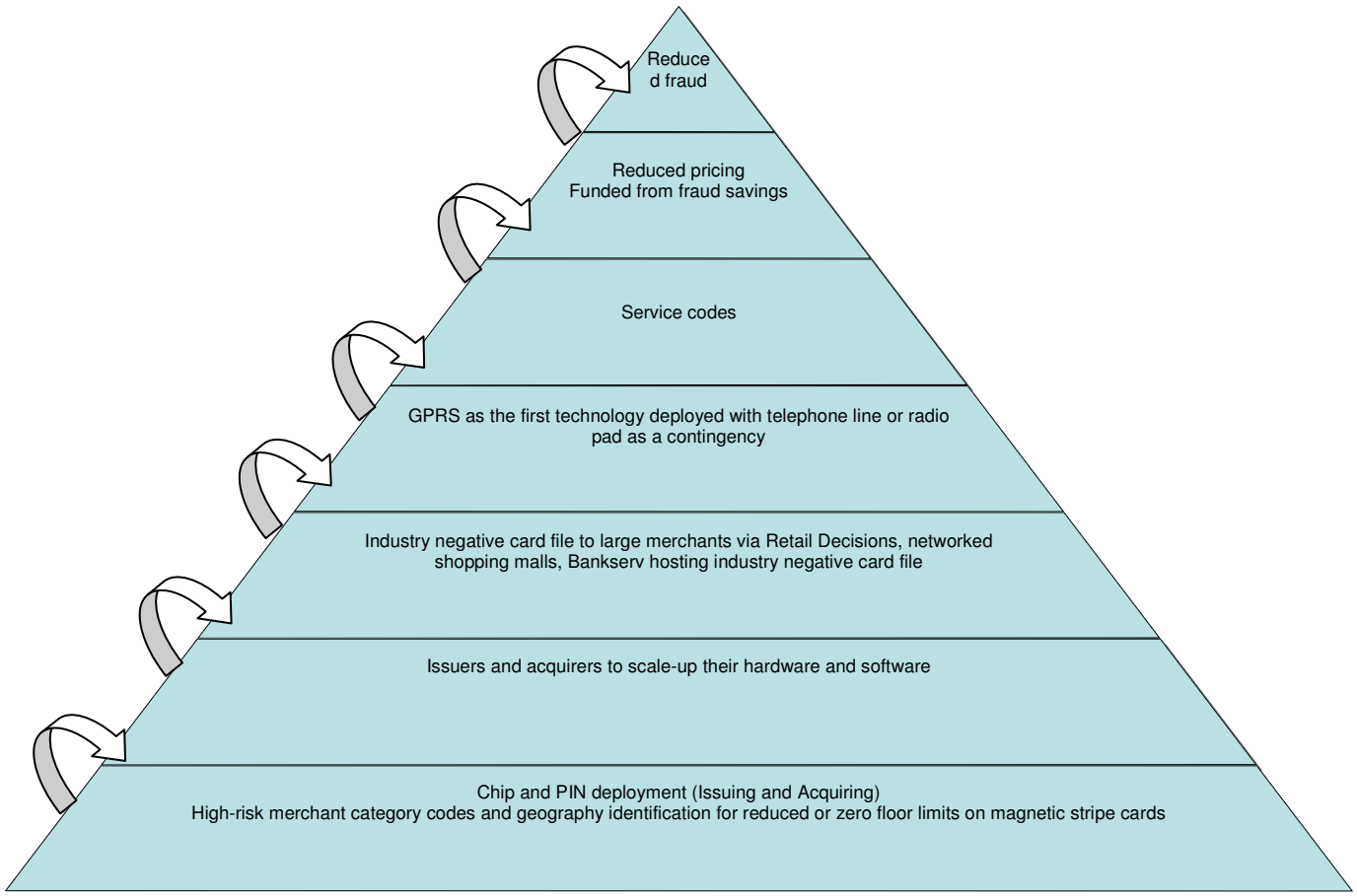
6.5.8 Issuer and acquirer scaling-up.

The issuing and acquiring bank can scale up their front-end processors and ancillary devices to handle a zero floor limit.

6.5.9 Pricing

Issuers and acquirers can reduce the interchange and commission fees to promote a zero floor limit environment. The reduction in fees can be used to subsidize the merchants operational costs and the fees themselves can be subsidized from the fraud savings. The issuers can reduce their interchange rates and the acquirers can pass this discount to the merchants by reducing their commission fees.

Figure 49: The interdependent solution



The above schematic represents the interdependent solutions one could take in reducing or zeroing floor limits. It is proposed that the solutions are interdependent of each other and combinations between the proposals can be adopted.

6.6 Recommendations for further research

The research done does not calculate the true costs pertaining to reducing floor limits as the costs entail not only direct costs but also indirect costs in terms of potential revenue leakage.

An interesting analysis would be the costs of fraud losses in relation to the interchange charged on credit card products. The competitiveness of the domestic interchange rate is a further consideration. The study did not include the bad debt losses on credit cards as this study was only restricted to fraud losses within the domestic banking industry. This study did not compare the interchange revenue with the fraud and bad debt costs to the issuing bank. The interchange rate has inherent bad debt and fraud funding and the differential between the funding, the actual losses accrued and the revenue earned would be an interesting analysis.

A further recommendation would be the costs of introducing chip and PIN in relation to the fraud losses curtailed. The roll-out of chip and PIN is considerably more than the fraud losses incurred on credit cards. If one calculates the investment that acquirers need to make in order to ensure that the point-of-sale and ATM infrastructure is chip and PIN compliant, and the costs the issuing banks incur in purchasing microchips and ensuring that the infrastructure is chip and PIN enabled, it could be argued that these are substantially greater than the fraud prevented (and concomitant savings). This analysis in line with the interchange rates and commissions charged would by an interesting economic debate.

CHAPTER 7

7. Article for Publication

Introduction

Credit card fraud perpetrated below merchant's designated floor limits within South Africa has been increasing alarmingly over the last two years. In 2006, card fraud perpetrated in South Africa alone exceeded R179M (Source: SABRIC, 2006) of which a substantial portion was attributed to below floor limit spending by miscreants. Discussion and collaboration with local bank credit card issuers at industry forums has identified the need to move to a zero-floor limit environment. The main quoted stumbling blocks to achieve this objective are the following:

- The inability of the local telecommunications infrastructure to sustain a zero floor limit due to the envisaged increase in authorization traffic,
- The inability of the issuing bank to process the anticipated volume of authorizations which would be the case in a zero-floor limit environment,
- The potential negative impact to cardholders due to longer queues and delays at the point-of-sale,
- The high operational costs that merchants will incur as telephony is an overhead that they pay for in fulfilling an authorization request.

South African-issued credit cards are fraudulently used mostly below the merchants floor limit in South Africa. This operating model perpetuates the fraud life cycle as the issuing bank only sees this transaction after an average of 2 days once the settlement process has occurred (this applies to cases where the issuing bank and the acquiring bank are not the same institution). As a result of this operating model, "hot" card files are stored on the merchant's point-of-sale which place the issuing bank's cards at the merchant location. Size constraints of these files and the delay of loading these exception cards further perpetuate the fraud life cycle.

The objective of the study was to analyse the effects that merchant floor limits have on bank-issued credit card fraud in the South African credit card industry and compare this to the ability of telecommunications to sustain a zero-floor limit environment. The objectives included the telecommunications capacity-handling from the point-of-sale to the issuing bank as well as the issuing bank's capability to process the transactions

emanating from a zero floor limit. In fulfilling these objectives, the researcher would be able to propose a case for reducing or zeroing floor limits with an end in view of lessening credit card fraud perpetrated below the merchant's floor limit. The researcher also acknowledged that fraud will migrate to other channels.

The problem statement was that floor limits assigned to merchants in South Africa for credit card products issued by South African banks continues the fraud life cycle as the point-of-sale channel cannot be effectively closed for credit card use.

The benefits of this study would be in the research to obtain the relevant facts to entertain a viable business case to move to a zero floor limit credit card infrastructure. This in turn should reduce recurrent fraud losses on credit card products and enable issuing banks to detect questionable cardholder behaviour earlier as they will now "see" all the transactions. The quoted stumbling blocks and Propositions would also be tested via a survey to choice industry participants

Credit card fraud has been prevalent since the inception of credit cards as a transactional product. According to Akers et al, the present day credit card industry originated in the nineteenth century. In the early 1800's merchants and financial intermediaries provided credit for agricultural and durable goods. In the late 1950's, the Bank of America began the first general purpose credit card program.
Miscreants have used various techniques and technologies to defraud issuing and acquiring banks and their respective customers. The credit card product has evolved not only in terms of its conventional value proposition and customer-oriented design, but also in terms of its aesthetic and technological features in an effort to thwart fraudsters. Bank-issued credit cards in the South African industry are either individually-branded by the issuing bank (proprietary cards) or co-branded under the auspices of international Associations (MasterCard International, Visa, Diners Club International or American Express). Should a credit card be dually-branded by the Association and issuing bank, the respective product would need to conform to the franchise regulations pertaining to the card features, technology and acceptance criteria. In research performed by Akers et al, Visa and MasterCard together held about 70 percent of the market share of the general-purpose card market.

An inherent limitation of South African bank-issued credit cards is that they have a magnetic stripe which is easily compromised by fraudsters. Contained within the magnetic stripe is sensitive card and cardholder data notwithstanding card numbers, card expiration dates and unique card identifiers. This information can be readily retrieved by miscreants and used to perpetrate fraud. Most credit card products within South Africa are signature-based. The signature on the reverse of the credit card is compared to the cardholder-signed sales voucher by the merchant. Apart from the cosmetic security features built-into the credit card (holograms and unique security characters/features), the merchant's only reliance that the presenter of the card is the lawful cardholder is the signature verification which takes place during the sale. This verification is open to substantial subjectivity and does very little to ensure that the presenter is *bona fide*. According to Ward S. 2007, in her guide to small businesses under the topic of credit card fraud, states that a questionable behavior on the part of a card presenter is one where they "ask what the floor limit is – and then either make purchases to just fall under the floor limit or ask to have items processed separately, so their credit card purchase doesn't exceed the floor limit".

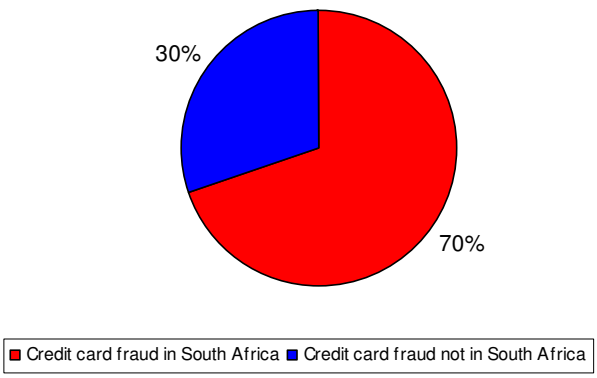
Coupled to the product limitations in reducing risk exposure, it operates in an environment where floor limits are assigned to select transaction types or merchants (or categories of merchants) which participate in the franchise arrangement and are signed-up by the acquiring bank to accept the products. Transactions conducted below the merchant's assigned floor limit do not go to the issuing bank for authorization and are only acknowledged by the issuing bank on average 1 to 2 days later during settlement. This is the first time that the issuing bank is able to detect questionable transaction behavior and take preventative steps to curtail further fraud. Albeit that issuing and acquiring banks have invested in chip and PIN technology, the roll-out has been lethargic and magnetic-stripe technology is expected to be a feature of the card until all card acceptance channels have been converted to accept this technology.

Fraud Statistics

Credit card fraud has increased alarmingly on South African bank-issued credit cards. The total fraud in 2006 which is the respective representative sample of this research totaled R257M over this period (Source: SABRIC, 2006). The researcher has further

differentiated between credit card fraud perpetrated within South Africa and compared this to fraud perpetrated abroad on South African bank-issued credit cards. The following pie chart reflects this differentiation:

Figure 1: South African-issued credit card fraud differentiated between local and cross-border.



Credit card fraud in South Africa	R 179,341,309.06
Credit card fraud on S.A bank-issued cards abroad	R 77,536,387.60

The pie chart illustrates that 70% of the South African bank-issued credit card fraud was perpetrated in South Africa. The large retail infrastructure in South Africa coupled to the fact that floor limits are in use and the product is magnetic stripe technology with signature as a cardholder authentication mechanism makes South Africa a lucrative country for fraudsters to apply their trade.

Credit card fraud in South Africa had increased at a burgeoning rate in 2006. *Figure 2* illustrates this growth year-on-year since 2005. This data was extracted on 20 February 2007 and illustrates a substantial growth in credit card fraud between 2005 and 2006. This worrisome trend is expected to continue in 2007. (Source: SABRIC, 2006).

Figure 2: South African credit card fraud year-on-year growth (in R's)

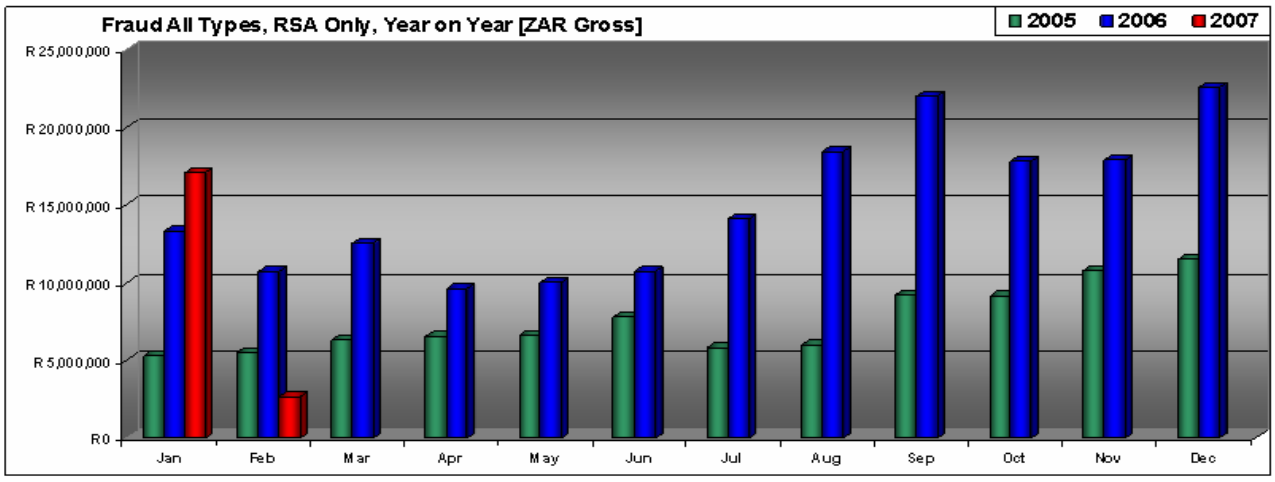


Table 1: Top 10 fraud merchant categories in South Africa

Description	Total
Grocery Stores and Supermarkets	R 17,749,223.63
Department Stores	R 13,550,846.39
Service Stations	R 13,450,314.50
Family Clothing	R 8,215,591.31
Men's and Boy's Clothing and Accessories Stores	R 5,761,266.15
Package Stores Beer, Wine, and Liquor	R 5,748,439.43
Eating Places and Restaurants	R 4,936,593.36
Betting, including Lottery Tickets, Casino Gaming Chips	R 4,756,085.21
Financial Institutions (Manual Cash Disbursements)	R 4,447,530.63
Financial Institutions (Automated Cash Disbursements)	R 4,133,097.30
TOTAL	**R 82,748,987.91**

Table 1 categorizes the credit card fraud per the top 10 merchant categories in 2006. These merchant categories may move up or down the fraud-risk hierarchy from time to time but generally predominate year-on-year.

Figure 3: Credit card fraud in South Africa by fraud type

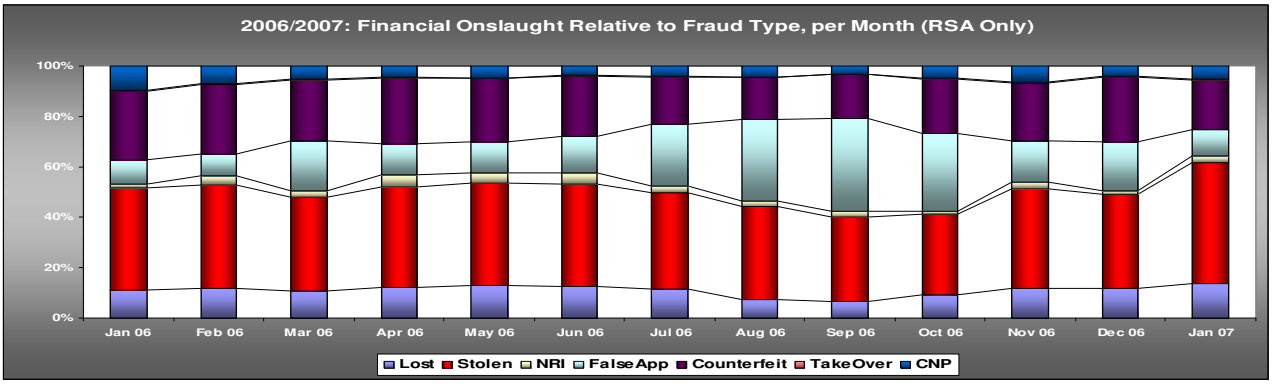


Figure 3 illustrates the different types of fraud perpetrated with credit cards in South Africa over the period January 2006 to January 2007 as a rand value per fraud type (Source: SABRIC, 2006). This analysis is pertinent as certain fraud type *modus operandi* is perpetrated below merchant's assigned floor limits. The fraud categories are a broader classification based on the following factors:

- How the card plastic, cardholder authentication (Personal Identification Number) and/or card data was obtained,
- The method used by the miscreants to perpetrate the fraud via the various financial channels (point-of-sale, internet, automated teller machines (ATM), mail order, telephone order, cash disbursement within the banks points of representation (branches))

Certain transactional channels enjoy floor limits whereas others have a mandatory zero floor limit as mandated by Visa, MasterCard or local banking industry rules (governed by the local banking industry). The transactional channels which do not have an assigned floor limit (i.e. zero floor limit) are those where:

- The card and/or cardholder are not present at the time of the transaction. These transactions are deemed "card-not-present" or "non face-to-face" transactions. The respective transactional channels where these transactions originate are:
  - Internet purchases
  - Mail order transactions
  - Telephone order transactions
- Transactions which involve cash disbursements, namely:
  - Cash disbursed via automated teller machines
  - Cash disbursed "over the counter" within financial points of representation (branches)

Floor limits are assigned to "face-to-face" transaction channels (where the card and cardholder are present). This excludes transactions which involve cash disbursements as mentioned above. The traditional "face-to-face" channels are points of sale.

Floor limits are generally assigned to merchant categories (with points of sale) based on the nature of the product they sell (the average ticket values of the goods or service) and the risk propensity of the business. The issuing bank determines the floor limit based on the merchant category and the current industry standards as governed by the local Association of Bank Card Issuers in South Africa (Source: MasterCard). The issuing bank funds the risk on the product they issue. The risk-funding is inherent within the interchange that the acquirer pays the issuing bank for every sale (detailed later in this document). Interchange is generally set to 1.71% of the sale. There are two main categories of risk in this funding, namely credit risk and fraud risk. Fraud risk funding in the interchange (1.71%) is roughly 0.12%.

The following analysis was done on credit card fraud perpetrated in South Africa from a banking industry perspective. The information was extracted and collated from Nedbank, First National Bank, Standard Bank, ABSA, Investec and Mercantile Bank (Source SABRIC 2007). The first chart represents fraud as a transaction cumulative amount within value bands. Lost and stolen fraud comprises the majority of fraud as a cumulative total. Most of the lost and stolen fraud is transactions which are perpetrated below the merchant's designated floor limit. Merchant floor limits are assigned on the basis of the nature of the merchant and their respective merchandise. The issuing bank also determines the floor limit with regard to the nature of the product. Credit card products that are at the lower end of the market segment enjoy a generic floor limit of between R200.00 to R300.00 which is in line with the merchant's assigned floor limit. Products at the higher end of the market segment (i.e. Gold and Platinum cards) have a floor limit which is double that of the conventional products. This implies a floor limit of between R400.00 and R600.00 (Source SACFF, 2007).

Figure 4: Fraud types per Rand value band over December 2006 to February 2007:

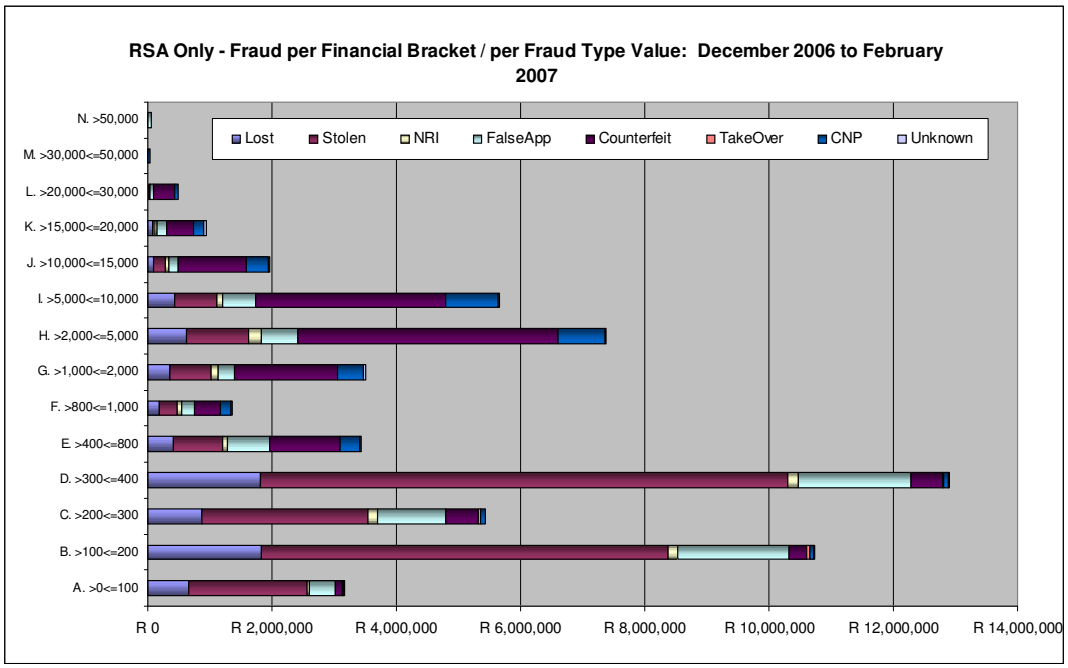


Figure 4 illustrates that most of the fraud as a cumulative total is within these floor limits on lost, stolen and false application fraud.

Figure 5: Fraud types as a count of transactions per value band over December 2006 to February 2007:

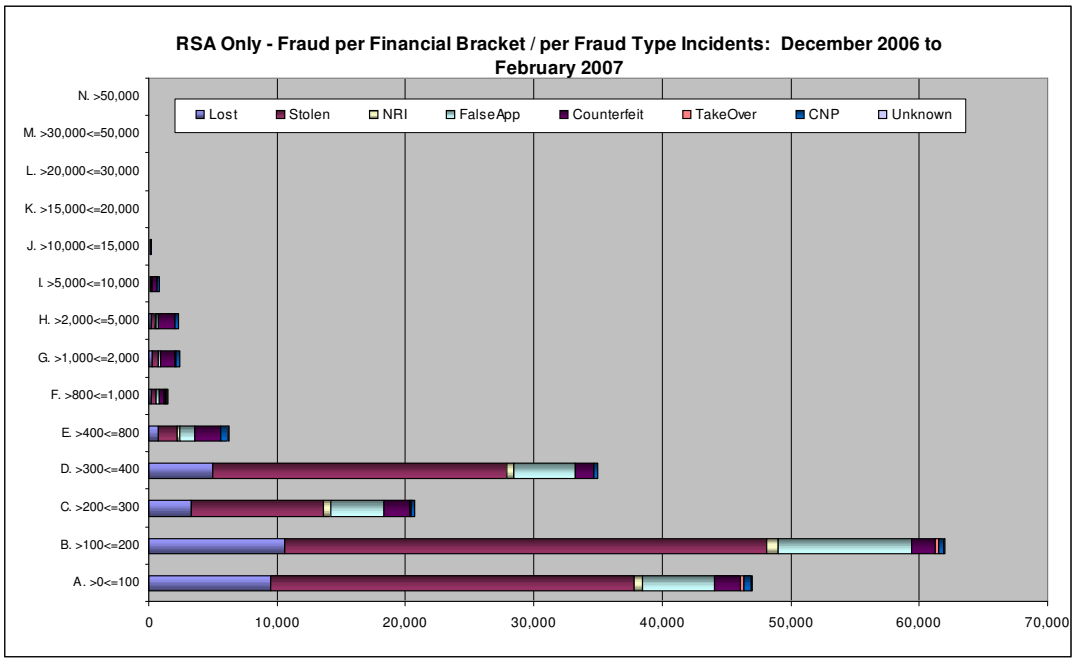


Figure 5 illustrates that the number of fraud incidents within the selfsame value bands also concentrates within the R200.00 to R600.00 category. This lends further weight to the argument that most fraud is perpetrated below the merchant's designated floor limit.

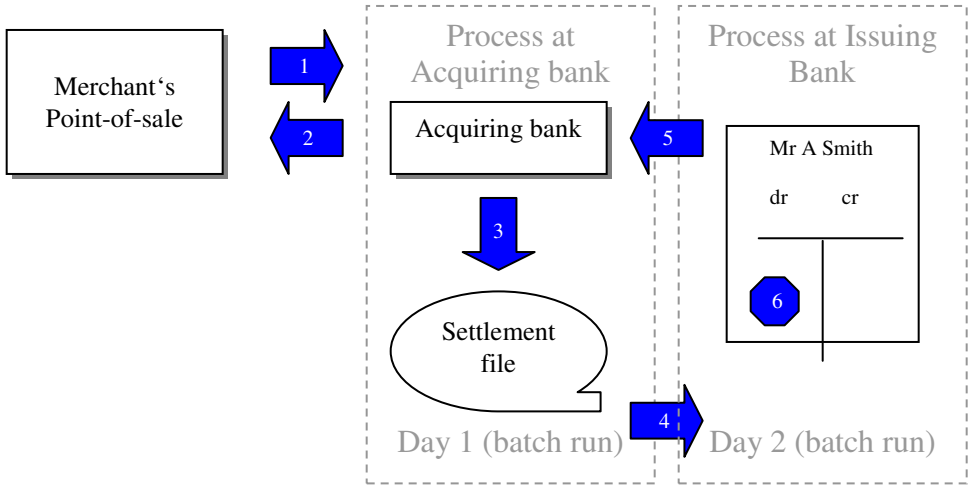
Settlement delay contributing to the "below floor-limit" fraud problem

Acquirers engage in a commercial relationship with merchants to accept credit cards and depending on the nature of the merchant and the infrastructure and technology the merchant has available, the acquirer may give the merchant credit card facilities. The acquirer or an agent acting on their behalf (third-party processor) will then process the transactions on behalf of the merchant. The merchant's point-of-sale facility (in the case of a "face-to-face" merchant) is programmed to dial-up to the acquirer to bank the credit card proceeds during a predetermined schedule. The merchant may also elect to do this manually. The acquirer will then credit the merchant for the sales (subject to cleared effects) and send settlement files to the issuing banks (whose cardholders transacted at the merchant) who in turn will financially reimburse the acquirer and financially account to their respective cardholder's accounts. The process is schematically represented in *figure 6*. The arrows depict the sequence of events as follows:

Step 1: The point of sale transmits the transactional data to the acquiring bank for processing during a predetermined scheduled which is programmed in the device's software.
Step 2: The acquiring bank financially reimburses the merchant for the transactions as part of their commercial engagement (subject to cleared effects).
Step 3: The acquiring bank then identifies all the issuing bank's transactional data and compiles a settlement tape.
Step 4: The settlement tape is then sent to the issuing bank so that it can financially account to the cardholder's account.
Step 5: The issuing bank financially reimburses the acquiring bank for the transactions its cardholders concluded.
Step 6: The issuing bank then credits the cardholder's account (in the case of a refund) or debits the cardholder's account (in the case of a sale).

The entire process takes on average two days in the case of the acquiring bank and the issuing bank being separate institutions. The delay is attributed to two separate batch runs, one batch run for the acquiring bank to obtain its merchant's sales and create a settlement file for the issuing bank, and one batch run for the issuing bank to financially adjust their cardholder's accounts. Batch runs do not take place during normal office hours. If the issuing bank and the acquiring bank are the same institution, this process generally takes one day.

Figure 6: The settlement delay when the issuing and acquiring bank are separate entities



As most acquiring banks brand their merchant's point of sale devices, fraudsters are able to easily differentiate between acquiring banks. Fraudsters are aware of the two day settlement delay between an acquirer and issuer (in the case where they are two separate institutions) and thus use compromised cards at these establishments below the merchant's assigned floor limit. The issuing bank will only acknowledge the sale after the transactions has been processed to the cardholder's account two days later. No amount of investment in fraud detection and prevention software from an issuing banks' perspective will be able to prevent or identify questionable card activity before the transaction is settled. Fraudsters are able to thus use the account's funds in excess of the card's allocated credit limit. This not only poses a fraud risk but also a credit risk in that the settlement delay can invariably create "additional" credit which is not catered for by the issuing bank. The settlement delay and the concomitant fraud/credit risk life cycle are depicted below:

Figure 7: The fraud/credit risk life cycle where the issuing and acquiring bank are separate entities

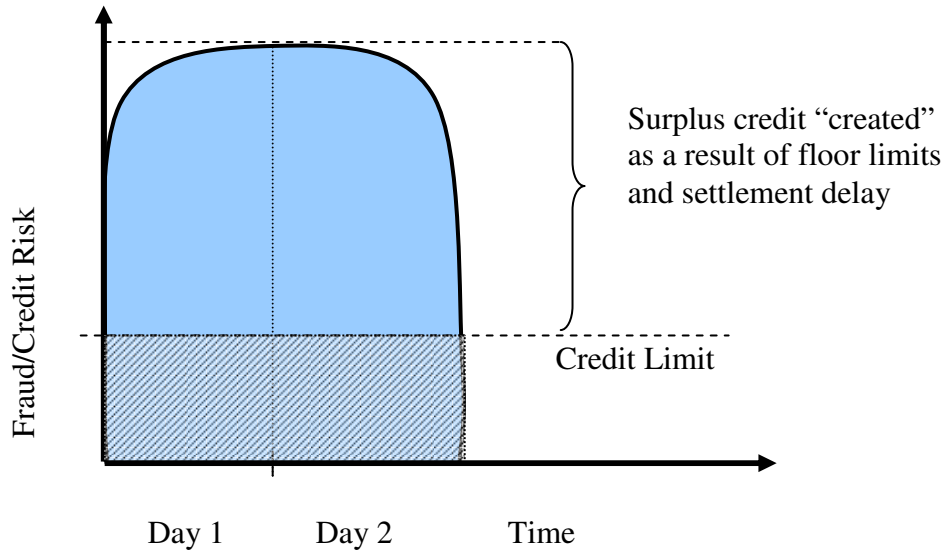


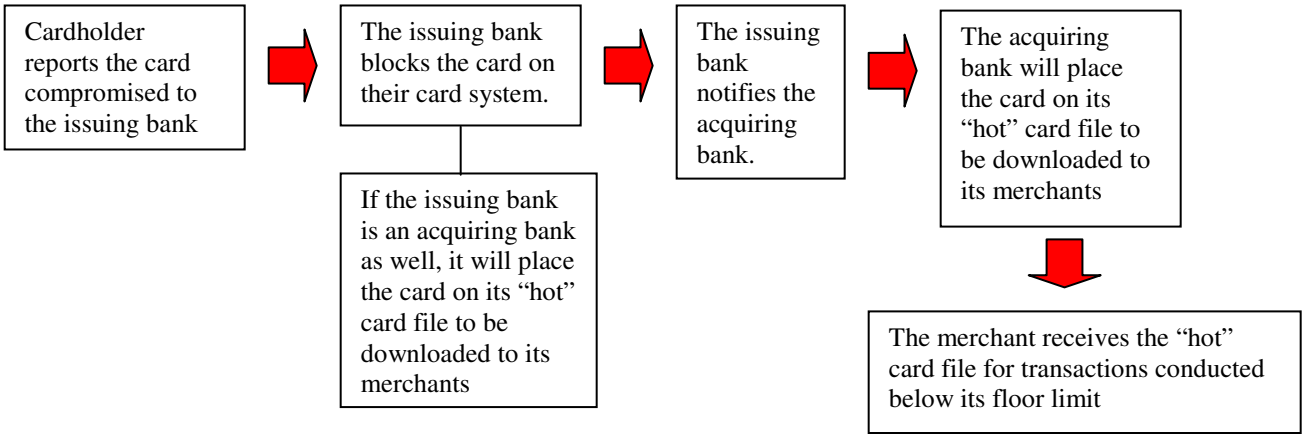
Figure 7 above illustrates the two-day fraud life cycle. The area below the shaded area represents the credit limit assigned to the cardholder based on their qualifying criteria on card application. The area above the shaded region is the surplus credit "created" and abused as a result of the merchant's floor limits and the settlement delay. This scenario holds true in instances where the issuing bank and the acquiring bank are not synonymous.

"Hot" card files

As credit cards can be used fraudulently below a merchant's designated floor limit, the issuing banks are at risk as they do not see or acknowledge the transaction(s) until they are settled up to two days later. In an effort to control the risk, "hot" card files have been created by terminal vendors of point-of-sale machines which enable a predetermined amount of compromised cards to be stored within the point-of-sale software. Issuing banks communicate the compromised cards to acquiring banks which in turn transmit this data to the merchant's point-of-sale during batch run when the device dials the acquiring bank's front-end processor to do its banking. The storage capacity of the point-of-sale for "hot" or compromised cards is limited. The acquiring bank and issuing bank

enter into an arrangement as to what the issuing bank's allocation is for "hot" cards. The acquiring bank has an obligation to its merchant to safeguard it against potential fraud and as such obtains issuing bank's compromised cards from all over the world. Due to the point-of-sale's storage limitations, cards are systematically purged from the "hot" card files after a passage of time. The purge is based on an aging process (generally first-in, first-out) or is done so by the issuing bank. Guerin, D, 2003 confirms that issuing banks only list the "most current and high-risk, hot-listed cards before being sent for authorisation, so that stolen cards may be rejected even if the transaction is below floor limit". In South Africa, compromised cards can be loaded on merchant's point-of-sale devices for up to 60 days where after they automatically purge. The hot card file process is depicted in *figure 8* below:

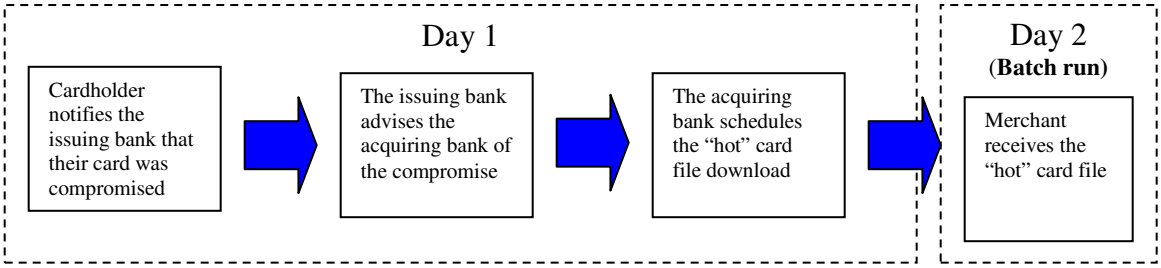
Figure 8: "Hot" card file process



The "hot" card file is somewhat different for merchant's who do not have a conventional point-of-sale and who use their own integrated solution which is linked to an inventory control system. These merchants typically get an extended "hot" or exception file from the acquiring bank as they have the hardware and software to accommodate more exception card numbers.

It can take the issuing bank up to two days to close the point-of-sale channel for compromised card numbers. If the issuing bank and the acquiring bank are the same institution, the compromised card can be stopped from being used at point-of-sale the next day. In the event that the issuing bank and the acquiring bank are not synonymous, it takes up to two days (or longer) for the acquiring bank's merchants to receive the compromised card(s). The delay is depicted below:

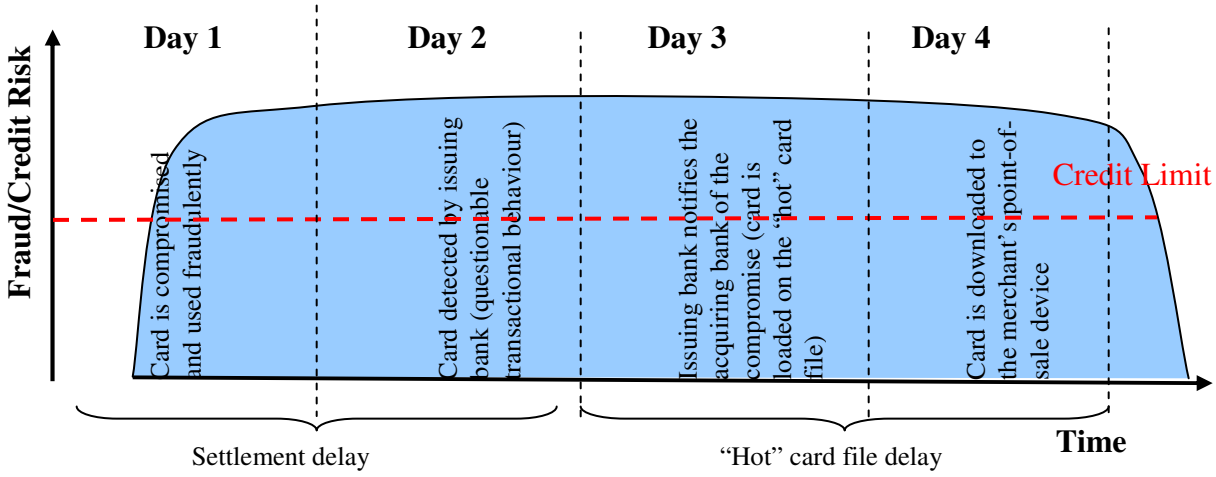
Figure 9: “hot” card file delay



The issuing bank has to prioritize the listing of its hot cards. All issuing banks in South Africa have more compromised cards that the “hot” card allocation which acquirer’s allow them on their merchants’ point-of-sale devices. Compromised cards may not necessarily be South African – issued cards but might include foreign cards as well.

The two-day delay of ensuring that the issuing bank’s compromised card is loaded on the “hot” card file increases the fraud life cycle as illustrated in *figure 10*. If one combines the settlement delay with the delay in sending the hot card file to the acquirer’s merchant’s point-of-sale (assuming the two institutions are not synonymous), the following life cycle is apparent:

Figure 10: Extended fraud life cycle

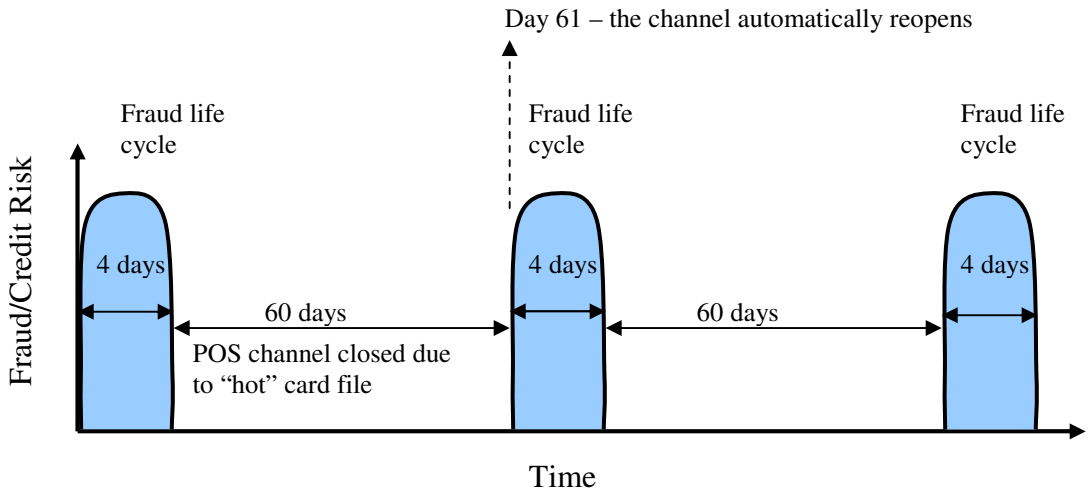


The illustration above depicts the extended fraud life cycle as a result of the settlement and the “hot” card file delays. It is through these delays that fraud perpetrated below the merchant’s floor limit can exceed the credit funding on the account and result in substantial fraud losses to the issuing bank. There are also associated costs of managing this “hot” card file which includes staff costs, operational costs and costs to the acquirer via charge backs which are discussed under the next heading. The 4-day fraud life cycle may be extended in instances where the issuing bank’s fraud detection systems or operational constraints do not detect the questionable transaction behavior on day 2 (during settlement). The longer the issuing bank takes to authenticate the questionable behavior with its customers, the longer the fraud life cycle can be extended. Albeit that the “hot” card file can forewarn merchants that the credit card has been compromised and in so doing avert any further potential losses to the issuing bank, the aging of the credit card from the point-of-sale due to capacity constraints further exacerbates the losses. This can be illustrated in *figure 8* below.

The card can only be loaded on South African merchant’s “hot” card files for a period of up to 60 days where after it purges. This means that the point-of-sale channel cannot be permanently closed and automatically reopens after 60 days. Fraudsters are currently aware of this constraint and use the card for its 4-day life cycle until it is loaded on each merchant’s point-of-sale. The miscreants then retain the card until it has purged from the “hot” card file (day 61) and then reuse it, perpetuating the fraud life cycle.
An article published by Levi, M et al (1991) confirm this in the following statement “Patterns of fraudulent use reveal that after initial use within the first day of theft, some fraudsters wait months until they expect that the card has been removed from the “hot file” and then reuse it”

According to Smith, R.G, 1997, it has been suggested that floor limits which apply to cards be reduced in order for transactions other than those involving very small amounts. Smith advocates that one of the main strategies used to prevent point-of-sale fraud has been to lower floor limits. This means that many more transactions will now require bank’s approval.

Figure 11: perpetuating fraud life cycle



Guerin, D, 2003 states in his publication on Fraud in Electronic Payments that fraudsters generally make as many purchases as possible within a window of time until the card is reported stolen by the customer to the issuing bank who in turn blocks the card. In some instances, the cardholder may not be aware that the card is missing (which is especially the case for *Lost and stolen fraud*) which in turn provides more time for the fraudster to transact. Guerin, D, 2003 goes on to state "Authorisation floor limits are amount thresholds used in dual-message environments below which purchases do not have to be authorised by the merchant, introduced to reduce the cost of merchant phone calls. In some European countries, knowledgeable fraudsters will specifically target stores with a transaction amount that is just below the merchant's authorisation floor limit to maximise the usage of the card even when it is blocked by the card issuer". This underscores the life cycle presented and discussed above. He goes on to state further that "Eventually, such cards may be sold abroad for use in countries with **poor telecommunications networks**".

South Africa currently deploys a service known locally as the INCF (Industry Negative Card File). The service is hosted by Retail Decisions, a leading card-based transaction services business providing fraud prevention to the finance, telecommunications, and retail and e-commerce sectors. An article by www.finextra.com contextualizes this service by stating "card transactions are screened against the Industry Negative Card File (INCF), a national database of lost, stolen and delinquent cards. Retail Decisions will collate and update the INCF for the banks and retailers using information gleaned from

the Prism system. The INCF currently contains more than 2 million records from South African card issuers and over 5 million records from other international card issuers"
This service was introduced due to the inordinate amount of fraud taking place at large merchant establishments (commonly referred to as "Blue Chip" merchants) and franchises. Fraudsters target these retail outlets due to the variety of goods sold and the probability that the fraudster's anonymity will be preserved as a result of the multiple purchase points (tills). The fraudster could shop at these merchants multiple times without anyone noticing the irregularity of this purchasing trend.

The large retailers also had an infrastructure to accommodate an industry negative card file. Conventional merchants, when signed-up by an acquiring bank, are issued with a point-of-sale device to facilitate processing credit card sales. Larger merchants have their own computer infrastructure that does not necessitate the installation of a point-of-sale device. More often than not, the computer infrastructure (referred to as an integrated solution) for these "host" merchants are more than a point-of-sale in that the merchant's inventory control system and ancillary financial services are hosted on a computer system. This infrastructure is supported by in-store client servers which allow the merchants to store more exception cards (fraud cards, collections-statussed cards, etc). These host merchants generally connect directly to the bank via dedicated telecommunications (leased lines). It is through this infrastructure and the burgeoning nature of credit card fraud at these establishments that Retail Decisions have offered to host an industry negative card file. The large banks in South Africa subscribe to this service which is aimed at reducing post-statussed fraud and bad debt. The post-status nature of these exception credit cards mean that transactions still take place below the merchant's designated floor limit after the card is statussed by the issuing bank (as the issuing bank does not "see" the transactions until they have received the settlement tapes from the acquiring bank). In order to mitigate these losses (post-statussed exception cards), the local issuing banks send their exception cards to Retail Decisions on a predetermined schedule, who in turn host the service or send the information to the large retail stores (which have the hardware and software infrastructure to accept larger volumes of these cards). Transactions concluded below the merchant's floor limit is referenced against this file and if the card is listed on the requisite file, the transaction is declined or the merchant is prompted to call the issuing bank.

Charge-backs

As mentioned previously, acquirers engage in commercial agreements with merchants. For a negotiated fee, acquirers process the merchant's transactions and arrange for the merchant to be financially reimbursed for the sales concluded on credit cards and recover this money from issuing banks whose cardholders transacted at the respective merchant. As part of the commercial agreement between the acquiring bank and the merchant, (and in accordance with predefined franchise rules governed by the Associations, namely, MasterCard International, Visa, American Express or Diners Club International), it is prescribed that should the merchant transgress their commercial agreement with the acquirer, it may incur the financial loss attributed to the disputed sale. Issuing banks also have financial recourse to the acquiring bank in cases where the merchant did not follow prescribed Association rules. This financial recourse to the acquirer or merchant is termed a "charge-back". An example of an Association rule regarding the acceptance of the credit card is that a merchant must not process a sale if the card is listed on a "hot" card file or in the event that the transaction is referred to the issuing bank for authorization and the issuer responds that the card is "hot". Should the merchant then process the transaction regardless of the exception status of the card, it will be liable for a charge-back by the acquiring bank and/or the issuing bank. Merchants are required to follow prescribed procedures to avert charge-backs. The complexity of cardholder and card authentication, coupled to the differentiated nature of the card products (branding, credit, debit, pre-paid, loyalty, etc cards), make it very risky for merchants to accept credit cards. The issuing bank has the responsibility to ensure that its product has sufficient inherent risk controls in order to mitigate fraudulent use. This is sadly not the case as the current cardholder authentication is signature which is too subjective to avoid fraud risk. The security features contained on the aesthetics of the card and that which are personalized to the magnetic strip are insufficient to mitigate fraud risk. Undue onus is placed on merchants to police the issuer's and acquirer's risk.

Research methodology

The research methodology that will be used is a qualitative study based on a proposition. The proposition will be supported or rejected by making use of logical reasoning and induction. The research problem is of such a nature that it is difficult to test hypothesis

with the data extracted as part of this research report. A set of propositions are used which is supported or rejected making use of logical reasoning and induction.

Alternative research methodology considered

It was initially proposed that the researcher would do a quantitative research methodology. The methodology would have been applied in the following manner; the purpose of the research is to explain and predict how point-of-sale devices and front-end processors will handle a zero floor limit environment. The data is numeric and comprises a large representative sample. Statistical analysis would have been used to analyze the data and their meaning with a focus on objective interpretation. A parametric test would have been used (One-Sample Chi Square Test).

A **"goodness-of-fit"** test would have been used to compare the extent to which the observed (i.e. empirical) frequencies "fit" the expected (i.e. theoretical) frequencies. The anticipated increase in authorisation volumes due to a zero floor limit environment would have been compared with the ability of Standard Bank's front-end processor (Postillion) to handle the volume of transactions (measured by its transaction per second processing capability). According to Diamantopoulos, Bodo and Schlegelmilch (2000), the One-Sample Chi-Square test is the test which compares a set of observed frequencies with a set of theoretical frequencies. The observed frequencies (calculated from empirical data) would have comprised the increase in authorisations as a result of a zero floor limit. This would have reflected the actual distribution of the variable concerned in the data. The theoretical distribution which would have reflected the researcher's expectations of the variable in the population would have been compared to the actual distribution of transactions conducted below the floor limit. This would have been related to the ability of Standard Bank's front-end processor to process the increase in transactions. The hypotheses were:

H_0: There is no difference between the observed and theoretical distributions

H_1: There is a difference between the observed and theoretical distributions

A simulator would have been used to test the ability of the front-end processor to handle an increase in the number of transactions as a result of a zero floor limit.

Limitations of the research methods and study

A stress test (simulator) requires a project to be raised, prioritised and takes approximately 6 weeks of extensive testing. This was confirmed with the test manager within Standard Bank's Group IT. It is due to the considerable cost and time involved that an existing stress test (done in 2006) was used. To develop a simulator to test "what-if" scenarios would not be feasible due to the complexity and variability of the system architectural components and intermediaries. A simple simulation would not be sufficient to cater for all of these actors and concomitant variables and would not adequately prove the ability of Standard Bank's front end processor to handle zero or reduced floor limits.

Per Diamantopoulos et al (2000) (154), the One Sample Chi-Square test is used when one wants to compare a set of observed frequencies with a set of theoretical frequencies. The question arises is whether the differences between observed and theoretical frequencies are significant.

H_0: authorisations frequencies = postings frequencies

H_1: authorisations frequencies $\neq$ postings frequencies

Postings refer to transactions that took place below the merchant's floor limit and as such did not go to the issuing bank for authorisation. These transactions are posted to the customer's account during a batch run.

The distributions being tested are those of authorisations (which have a time stamp) in conjunction with postings (transactions conducted below the merchant's floor limit) which *do not have a time stamp* for this test. The time stamp is not stored for transactions conducted below the merchant's floor limit by Standard Bank. A large sample of data (transactions below the merchant's floor limit) is available from the Group's data mart but no time is stored. This makes the use of the chi-square test irrelevant for testing the assumption that posted transactions follow the same distribution as the authorised transactions.

Method of primary data collection

The representative sample for data collection will be the period 01 January 2006 to 31 December 2006. The primary data comprising the sample will be collected from within Standard Bank. The sample reflects a convenience sampling method in that the sample is chosen on the basis of the data being readily accessible. The following primary data will be collected for analysis over the period mentioned above:

- All credit card authorisations
- All transactions conducted below the merchant's designated floor limit (non-authorisations). As mentioned in the assumptions, it is assumed that the non-authorised transactions will follow the same distribution as the authorised transactions.
- The maximum transactions per second (TPS) processing ability of Standard Bank's front-end processor (Postillion).

The authorisation and non-authorised data is currently stored within Standard Bank's data warehouse. The front-end processing capability in transaction per second is available on the application itself.

Data collected from Bankserv (a local transactions switch) for 2006 will also be collected and analysed to ascertain the maximum load that these processors can handle (authorisations and postings). This primary data also constitutes a convenience sample (non-probabilistic). The reason for obtaining this sample is that all domestic transactions where the issuer and acquirer are not the same institution are switched via this entity. The transaction switching comprises a substantial volume and is representative of the domestic credit card market.

The researcher had conversations and interviews with technical and business personnel from the following companies:

- Fraud Managers from various local banks
- Fraud representatives from the Card Associations
- Managers from the Merchant Services functional area in Standard Bank.
- Standard Bank technical personnel in the IT and telecommunications field.
- Computer Software Consultants that install point-of-sale software

- Fair, Isaac, (a vendor of fraud predictive and analytic software based in the USA)
- Retail Decisions (a vendor that manages the industry hot card file (INCF)) and is involved in telecommunications with large retail outlets.
- Fastnet (the vendor that supplies radio pads to merchants for microwave transmission to the acquirer)
- XLink (the vendor that supplies GPRS solutions to merchants for transmission to the issuer)
- Connectnet (the vendor that supplies GPRS solutions to merchants for transmission to the issuer)

The semi-structured interviews with these people included the following kinds of questions:

1. Can the local telecommunications infrastructure handle a zero floor limit environment?
2. How reliable is Telkom in servicing a zero floor limit?
3. Can issuing banks handle the volume of transactions that would be attributable to a zero floor limit?
4. Can acquiring banks handle the volume of transactions that would be attributable to a zero floor limit?
5. What are the perceived costs of introducing a zero floor limit?
6. Is below floor limit fraud a problem or is it a necessary cost of doing business?
7. Which technology is best-suited to sustain a zero floor limit considering cost, speed, efficiency and effectiveness?

The researcher transcribed the interviews and added comments as it was reviewed.

Method of secondary data collection

All fraud transactions on credit cards are reported by the South African issuing banks to SABRIC. The differentiation between below and above floor limit fraud cannot be ascertained using SABRIC's data due to the product differentiation between the banks.

Standard Bank's issuing fraud data will be used as a representative sample of the fraud within the domestic industry. Standard Bank represent 25% market share from a credit card perspective (DI 900, Standard Bank, 2007). This secondary data will be obtained by the researcher over the representative period of 01 January 2006 to 31 December 2006. The data will be segmented into transactions which took place below the merchant's floor limit and that which took place over the merchant's floor limit. This analysis will show the potential fraud savings which would have occurred had the floor limits been reduced to zero over the representative period. This data will be used to induce the effect that zero floor limits would have had on credit card fraud (Proposition 1). The sampling method used is also judgemental sampling (non-probabilistic) based on the researcher's judgement.

The second and third Proposition will be exploratory and qualitative in nature in terms of the research findings.

Stress tests (simulated volume test data) will be collected from Standard Bank's data mart over the period May and June 2006. A stress test is a simulation whereby the system architecture, notwithstanding all system components and intermediaries, are sent volumes of data (authorisations and settlement) to determine the maximum capacity that these entities can process. The volume or stress test results will be discussed as part of this research.

Data Collected

The sample data collected from the various populations comprised the following:

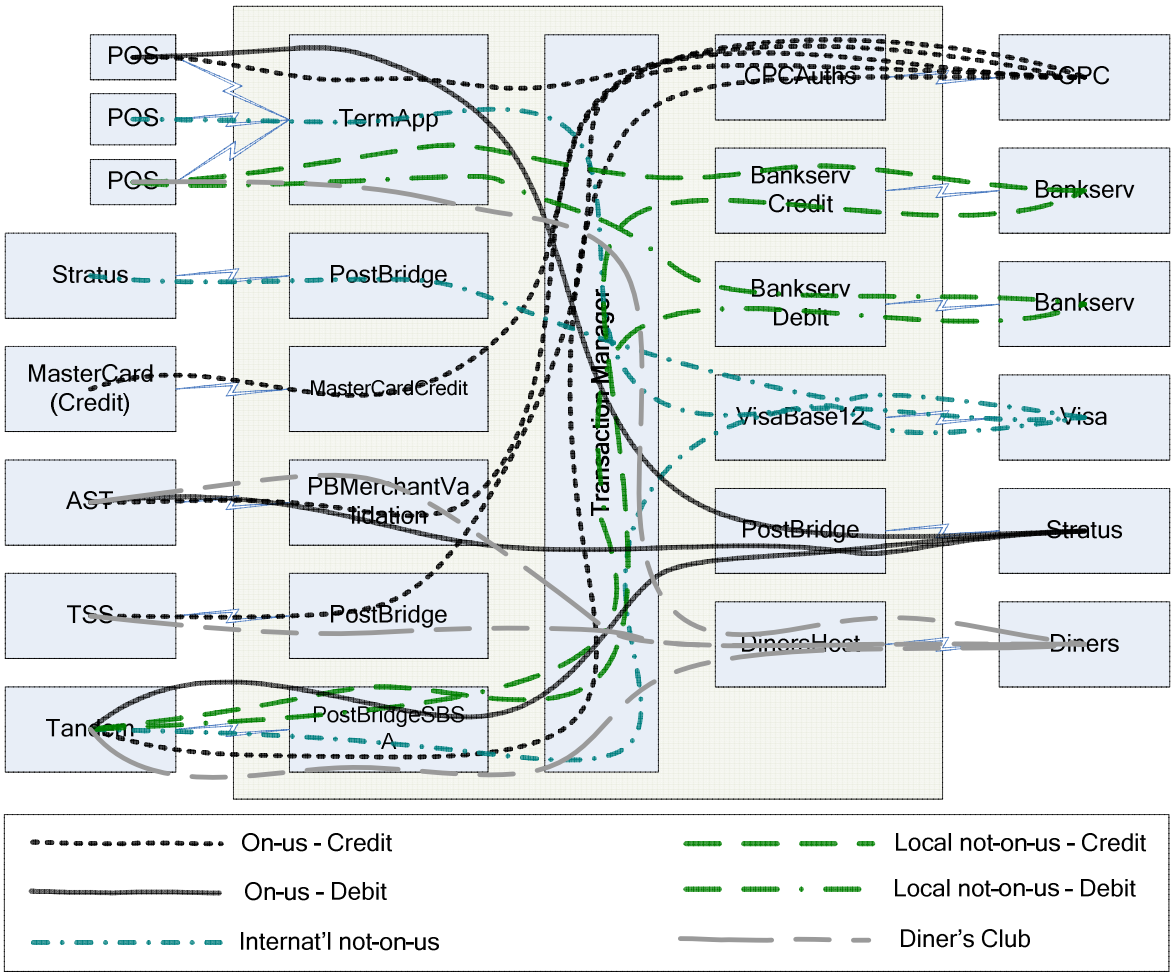
1. Data collected from SABRIC on credit card fraud in South Africa
2. Data contained within Standard Bank's data mart on all authorizations and postings from January 2006 to December 2006.
3. Data results from a stress test performed from May to June 2006.
4. Data from Bankserv over the period January 2006 to December 2006.
5. Samples from a survey to determine attitudes and opinions relating to floor limits and telecommunications.

The data had been collected and analyzed to support the Propositions from a quantitative and qualitative perspective. Many interviews and discussions were had with various stakeholders in the credit card industry.

Standard Bank's Stress Test – Determining Online Transaction Capacity

This test set out to determine the maximum sustained transaction rate that could be supported by the Postillion system. The system Architecture that was involved is reflected in figure 16 below:

Figure 12: Overview of Target Test System



The following test methodology was applied when performing the stress test:

1. A background Terminal Application load was generated by simulating 15 terminals constantly performing a banking session (including parameters, hot card downloads etc.). This equates to approximately 620 banking sessions per hour.
2. The Terminal Application and other source node simulators injected transactions into the system at predetermined rates (per *Appendix 3*).
3. Additional terminals were added to the system in groups of 80 to perform online authorizations.
4. Non-Terminal Application source nodes slowly increase their rate of transaction injection in a stepped fashion.
5. The number of transactions was increased until the average CPU load on the system exceeded 90% and Postillion started showing signs of stress.
6. Once the break-point had been reached the transaction load was gradually reduced to test the system's ability to recover.
7. Tests ran from 13:50:47 to 15:09:48 (elapsed time 01:19:01).
8. Over 409000 transactions were executed during this period.
9. The highest average transaction rate over a 5 second period was 141 TPS.
10. The highest average transaction rate over 1 minute period was 106 TPS.

The test results showed the following:

1. There was sufficient memory capacity to perform well above the levels at which CPU capacity was reached.
2. The following significant boundaries were encountered:
    a. CPU reached 60% utilization at 70 TPS.
    b. Response times degraded significantly after 88 TPS.
    c. Terminal Application's internal event queue remained constant until 65 TPS.
    d. Transaction Manager's event queue remained constant until 65 TPS (at approximately 60% CPU utilization).
3. The system was able to recover from its over-stressed state without intervention. Service was restored to normal as soon volumes returned to sustainable levels.

The results show that the system had three performance 'zones':

- Comfort – Up to 65 TPS the system performs optimally with no degradation in service. The system is capable of easily absorbing transient spikes of over 100 TPS.
- Stressed – Up to 88 TPS where the system is performing under stress. Response times have degraded (by up to 200%) and reduced service is being offered with some transactions being discarded as volumes grow towards 88 TPS. Transient volume spikes will temporarily decrease the grade of service further.
- Over-stressed – Over 88 TPS where performance is severely retarded. System behaviour is erratic with response times between 200% and 800% worse than those experienced at 65 TPS.

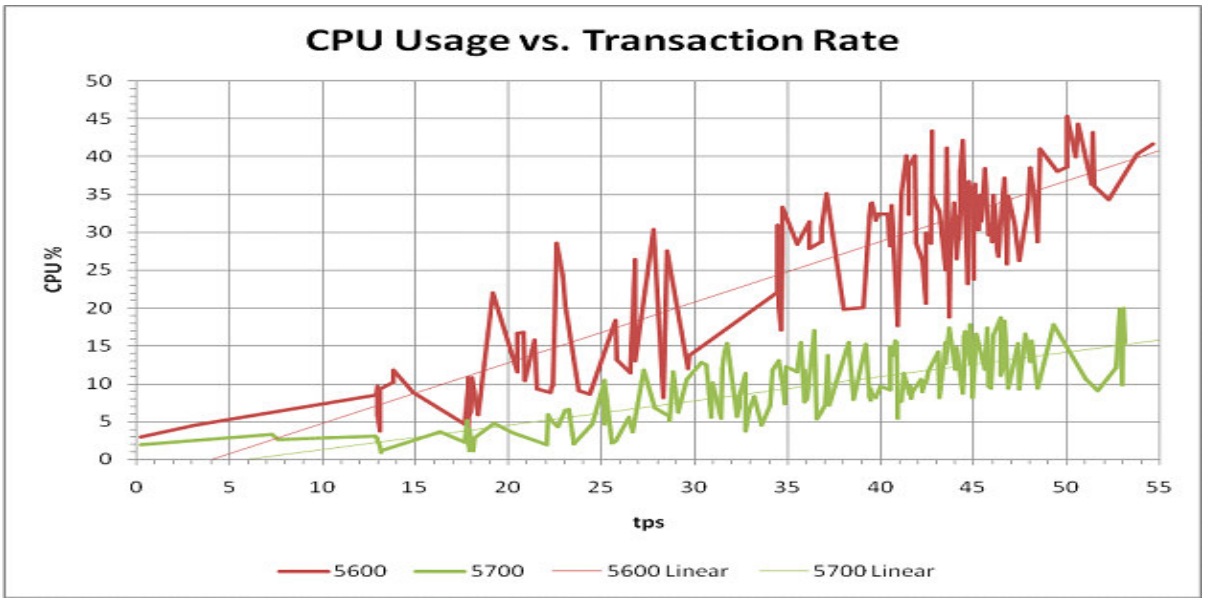
As of 9 November 2006 the busiest day in production was 28 October 2006 with 846,681 transactions during the day. 76,647 transactions were recorded during the peak lunch-time period of 13:00-14:00 on that day, for an average rate of 1277 per minute or 21 per second. At 65 TPS (in the "Comfort Zone") the system was capable of 3,900 transactions per minute or 234,000 per hour – approximately 3 times higher than the peak volumes thus far experienced in production.
A hardware upgrade (increase in available CPU capacity) would be required before transactions rates of more than 65 TPS could be sustained for periods exceeding a few minutes.

An interview was held with the Manager of Standard Bank's front-end processor and associated applications on the stress test performed by him with the commensurate results. The person being interviewed was Sean Baker (Baker, S, Manager IT Solutions Centre, 2007. Personal interview, 26 April 2007, 5 Simmonds Street, JHB). The following information was forthcoming based on the interview and the stress test results performed in May and June 2006.

Toward the end of 2006, the front-end processor had been upgraded and whereas it was dual processing with a comfort zone of 64 TPS, this figure can be mathematically doubled to 124 TPS as the front-end processor has been doubled in terms of its processing ability (quad processing).

The central processing unit and its processing speed is a key consideration in terms of front-end processing capability. Processing capability would be the most important systematic metric to propose a zero floor limit. The CPU ultimately determines the speed with which the transactions (authorizations are processed) and the load on memory consumption. The following diagram reflects the difference between the processing ability of the front-end processor's CPU prior to the upgrade (dual processing) and that after the upgrade (quad processing).

Figure 13: The difference between the CPU speeds before and after the front-end upgrade.

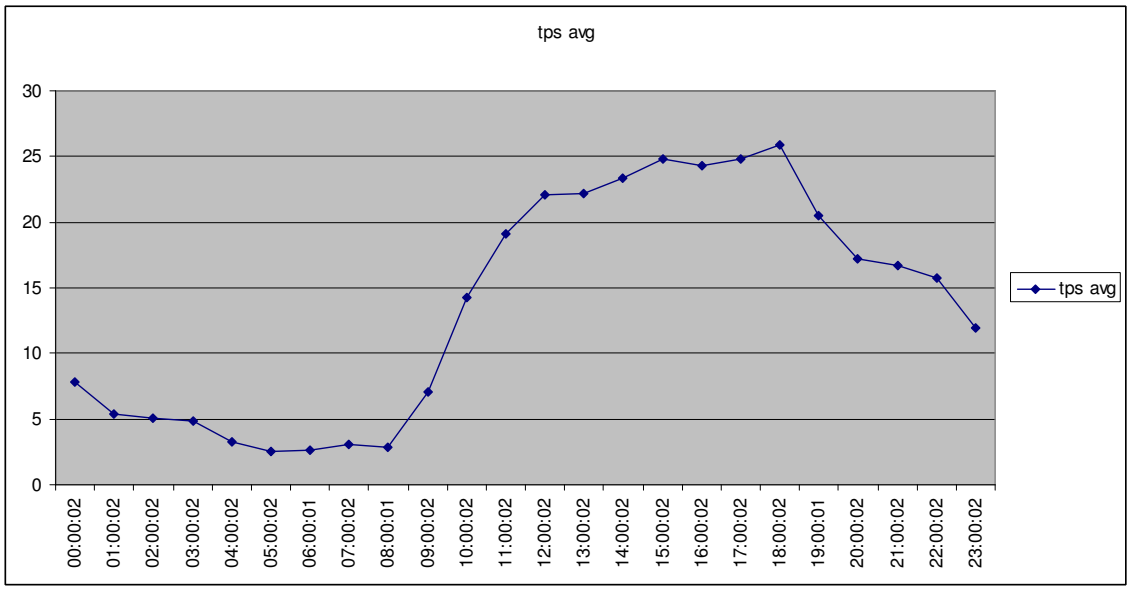


The red line (labeled 5600) reflects the front-end's CPU usage (as a percentage) versus the transactions per second processing *before the upgrade*. The green line (labeled 5700) reflects the front-end's CPU usage (as a percentage) versus the transactions per second processing *after the upgrade.* One can clearly see that the variability of the old CPU's processing is highly erratic when the transactions per second are increased. This variability is much less with the new CPU usage as more transactions are added to the processor. The Old CPU versus TPS linear slope is steeper than that of the upgraded CPU versus TPS slope. This reflects the ability of the new CPU to process more transactions faster and more efficient than the older CPU.

When Mr. Baker was asked whether the stress-tested comfort zone of 62 TPS (the old CPU processor) had been reached in a production environment, his answer was "*no*".

The busiest day in 2006 which was the historically highest volume of transactions processed was the 22nd December. The highest average TPS was at 18:00:02 at 26 TPS. The following run chart illustrates the volumes processed (average TPS):

Figure 14: The highest transactions ever recorded (December 2006)



Mr. Baker was asked whether the following mathematical assumption can be applied to ascertain the processing ability of the front-end processor after the upgrade:

- Highest TPS achieved in production: 25 (1500 transactions per minute)
- Comfort zone of old processor (TPS): 62 (3720 transactions per minute)
- Upgraded comfort zone (double the old processing speed): 124 (7440 transactions per minute)
- Difference between the highest TPS achieved in production and the new processing capability :**99 (5940 transactions per minute)**

Mr. Baker responded that he supports the logic on a mathematical basis, however, the relationship between the CPU usage, the TPS and system memory consumption is *not linear* (as suggested by the calculations) and cannot be argued mathematically as done above. CPU consumption is positively correlated to memory use and TPS (as shown in the stress test results). Mr. Baker confirmed that the relationship is not linear but rather

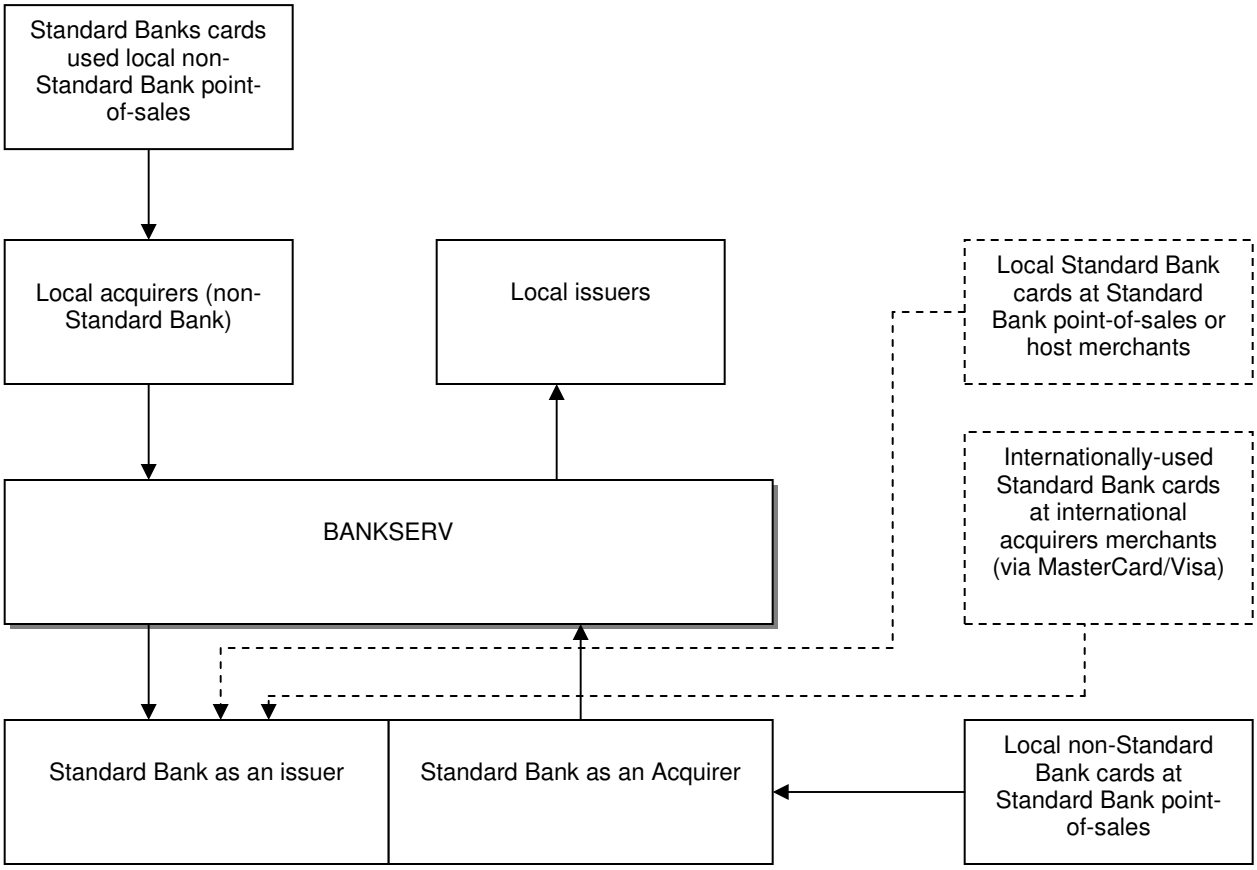
logarithmic and that no logarithmic scale is available to represent this relationship. He does however; believe that the logic is sound as represented above. In order to unequivocally prove whether the front-end processor could handle a zero floor limit, a stress test (Acid test) must be performed. As mentioned, a stress test (simulator) requires a project to be raised, prioritised and takes approximately 6 weeks of extensive testing. This was confirmed with the test manager within Standard Bank's Group IT. It is due to the considerable cost and time involved that an existing stress test (done in 2006) was used. To develop a simulator to test "what-if" scenarios would not be feasible due to the complexity and variability of the system architectural components and intermediaries. A simple simulation would not be sufficient to cater for all of these actors and concomitant variables and would not adequately prove the ability of Standard Bank's front end processor to handle zero or reduced floor limits.

Data Analysis – Bankserv

Bankserv is the largest operator (providing infrastructural components) in the South African payment and clearing system. A core function of this organization is the switching of electronic payments between banks (SASWITCH) and the clearing of South African payments systems (http://www.bis.org).

The following analysis was done by meeting with Bankserv and obtaining transactional volumes from them. Bankserv switch all local transactions for local issuers and acquirers based on the following macro-illustration:

Figure 15: Schematic representation of transaction flow



The above illustration positions the role of Bankserv. Bankserv only switch local transactions where the issuers cards used at the transactional channel are not synonymous with the selfsame acquirer. Let's say that a Standard Bank credit card is used at an ABSA merchant, the authorization and settlement will route via Bankserv. In the event that a Standard Bank credit card is used at a Standard Bank merchant, the authorization and settlement will *not* route via Bankserv as this routes directly to Standard Bank. This relationship is illustrated by the non-dashed stakeholders. All international transactions also route to the issuer and do not go through Bankserv. As mentioned previously, all international transactions have a zero floor limit and do not form part of the analysis regarding floor limits.

The following data was extracted from Bankserv over December 2006 which is traditionally the busiest time of the year for transactional volumes and authorizations:

The highest authorization activity on cards for the month occurred on the 22nd December.

Table 2: CPU average use (%)

MAX TPS	BUSY TIME	CPU AVE %
71.9	11:45 - 11:55	41.64

Table 17 indicates the maximum TPS and CPU usage. Bankserv have confirmed that their maximum TPS threshold is 156 TPS for one site. Bankserv process authorizations via two separate sites (continuous processing) to balance the load and each site can maintain 156 TPS concurrently (reference: Bankserv). This results in a total TPS threshold of 312 TPS processing capability.

Data Analysis – Standard Bank

The following data was extracted from Standard Bank's Data Mart for 2006. The data represents all authorizations and postings (transactions that did not come up for authorization and were below the merchant's floor limit).

The posted transactions that did not come up for authorization (below the merchants floor limit) did not have a time stamp to determine the time of the transactions. The authorizations however, (transactions above the merchant's floor limit or transactions originating abroad that have a compulsory zero floor limit) did have the respective time stamp.

Based on these constraints, the following assumptions were made:

- Posted transactions follow a distribution similar to authorization data
- The maximum authorizations per second are equally distributed.

With these assumptions, the following theoretical increases in transactions per second are evidenced:

Table 3: Standard Bank transaction increase month-on-month had a zero floor limit been adopted

Month	Increase (%)	Max Authorizations per Second
Jan-06	85%	61
Feb-06	77%	62
Mar-06	70%	62
Apr-06	69%	80
May-06	72%	66
Jun-06	67%	65
Jul-06	65%	77
Aug-06	70%	66
Sep-06	65%	86
Oct-06	70%	70
Nov-06	65%	69
Dec-06	59%	91

Highest theoretical TPS in the event that zero floor limits had been introduced in 2006: **91** (based on the December 2006 peak)

Upgraded comfort zone (double the old processing speed): **124** (7440 transactions per minute)

Difference between the highest TPS achieved in production and the new processing capability: **33 (1980 transactions per minute)**

The data thus theoretically illustrates that the 91TPS exceeds the comfort zone of 65TPS as evidenced in the stress test. At 65 TPS the system performs optimally with no degradation in service. The system is capable of absorbing transient spikes of over 100 TPS. When the system was stressed to 88 TPS, the system is performing under stress. Response times have degraded (by up to 200%) and reduced service is being offered with some transactions being discarded as volumes grow towards 88 TPS. Transient volume spikes will temporarily decrease the grade of service further. Over-stressed results (over 88 TPS) show that the performance is severely retarded. System behaviour is erratic with response times between 200% and 800% worse than those experienced at 65 TPS. The stress tests show that a hardware upgrade (increase in available CPU capacity) will be required before transactions rates of more than 65 TPS can be sustained for periods exceeding a few minutes.

Data Analysis – Card Industry Survey

The respondents to the questionnaire and focus sessions comprise a cross section of the card industry. The following companies and people are involved to a greater or lesser extent in credit card fraud, Merchant Services, telecommunications and system infrastructure. A brief overview of each company is presented below:

I. FastNet

FastNet is an industry participant as it pertains to point-of-sale terminals and the radio communications service it provides to merchants throughout South Africa. Their radio pad provides an efficient radio communication link between the card-swipe terminal and the banks' computers by replacing the telephone line.

II. X-Link

This company provides wireless data communications in the industry supplying a data communication interface to more than 10 000 merchants across South Africa. The company boasts the largest installed base of GPRS devices in the South African market.

III. ConnectNet

ConnectNet is a value added provider of wireless data communications and services for business-to-business and machine-to-machine applications. The ConnectNet boasts “A state of the art GPRS modem”. Applications include Point-of-Sale (POS), ATMs, pre-paid airtime, healthcare verification, telemetry and security.

IV. Retail Solutions

Retail Decisions (ReD) plc was founded in January 2000. ReD is a payment card issuer and a world leader in card fraud prevention and payment processing.

ReD's fraud prevention and payment processing operations located in Europe, South Africa and the US assists retailers, telecommunications companies, oil companies, e-commerce retailers and banks to prevent the fraudulent use of payment and credit cards in both card-present (CP) and card-not-present (CNP) payment environments.

V. Fair Isaac

Fair Isaac Corporation (NYSE: FIC) is the leading provider of decision management solutions powered by advanced analytics. Thousands of companies in more than 80 countries use Fair Isaac technology to acquire customers more efficiently, increase customer value and retention, reduce fraud and credit losses, lower operating costs and enter new markets more profitably.

Most leading banks and credit card issuers rely on Fair Isaac solutions, as do insurers, retailers, telecommunications providers, healthcare organizations and government agencies.

VI. CSC

Computer Software Consultants are a company that installs and maintains point-of-sale devices in the South African market. Most merchants acquired by Standard Bank utilize their services in the domestic arena.

VII. Standard Bank Front-End

The front-end staff maintains Standard Bank's front-end processor and ancillary systems, communications, hardware and software.

VIII. Standard Bank Merchant Services

This business unit within Standard Bank engages in commercial agreements with merchants to process transactions thereby fulfilling a business partnership.

IX. MasterCard

MasterCard is a multinational corporation based in Purchase, NY in the United States. Throughout the world, its principal business is to process payments between the banks of merchants and the banks of purchasers that use its "Mastercard" branded debit- and credit cards to make purchases.

X. Visa

Visa creates payment products, systems, services and standards on behalf of the banks that issue Visa cards and sign-up outlets to accept them. Visa also develops standards for global interoperability, security and new technologies

Research Findings

The analysis and research done to date on the formulated Propositions are discussed under this heading.

1. *Proposition 1*: The first Proposition is that merchant floor limits in South Africa have an adverse impact on bank-issued credit card fraud. The two major contributing factors are:
    - The settlement delay between the acquiring bank and the issuing bank,
    - The delay in closing the POS channel where the issuing bank and the acquiring bank are not synonymous.

    As already mentioned, fraudsters are aware of the window of opportunity available to them due to the infrastructural architecture. The fraudsters purposely purchase at merchants that are acquired by acquirers that are not the issuing bank with which the fraudster transacts (i.e. the credit card used by the fraudster is issued by an issuing bank that is not the same as the transaction acquiring institution). The data obtained from SABRIC as well as the data obtained from Standard Bank's data warehouse supports this statement. Domestic fraud in 2006 comprised R179M of which R62M is expected to represent the below floor limit component as calculated in chapter 5. This represents 35% of the transactions as a Rand value. If one had to consider the number of transactions (as a transaction count) as a percentage to the total fraud transaction count, a figure of 80 – 85% is apparent. The transaction counts were not available from SABRIC. Standard Bank's fraud as a transaction count for 2006 comprised 93%. The linear growth in fraud year-on-year from an industry perspective presents a concern to the domestic banking industry. The roll-out of chip and PIN is expected to take up to two years. This technology will reduce the number of lost and stolen transactions (as well as counterfeit and NRI) as the PIN and card must be present at the time of the sale. Card parameters personalised to the chip by the issuing bank will allow a certain amount of off-line transactions. In the event that the fraudster disables the chip (e.g. by placing adhesive tape over it or micro waving it), the transaction will default to the magnetic stripe which will automatically come on-line for authorisation. The key drivers for the anticipated increase in authorisation traffic will be the following:
        - The card parameters personalised to the chip

- The point-of-sale parameters personalised to the point of sale
- The number of default to magnetic stripe transactions
- The number of “face-to-face” transactions conducted via the physical channels
- The number of chip cards in the market
- The EMV roll-out strategy of the issuing and acquiring banks
- The card and merchant base growth and the propensity to use and accept credit cards in the domestic market.

Chip and PIN (EMV) may inadvertently contribute to increased authorisation volumes that are currently not experienced in production. In most instances the issuer cannot write-back to the chip to change the chip parameters initially personalised to the card. The only way to mitigate the increased authorisations where the issuing and/or acquiring bank are experiencing service degradation (due to system constraints) would be to:

- Recall the plastic from the customer and reissue cards with a higher offline transaction capability *and/or*
- Scale up the systems to accommodate the increase in authorisations.

A further exacerbation in that the fraud funding contained within the card interchange is insufficient to cater for the fraud losses incurred on the credit card products. As floor limits contribute substantially to the fraud losses, the profitability of the issuing bank is reduced due to the floor limit infrastructure. The fraud funding in the interchange in relation to the fraud losses experienced is not discussed in this research report due to the competitive nature of the calculations and the complexity of the various interchange rates and fees per product type. This is excluded in the delimitations section of this research report.

2. The second Proposition is that South African telecommunications can sustain a zero floor limit. The research done has provided evidence that the technology exists in the market to support and sustain a zero floor limit. The survey done with the telecommunications and technology service providers and vendors in the market has afforded confirmation to this end. If one considers the questions asked in the survey and the concomitant responses, it is apparent that this is indeed the

case. The following questions answered in the survey by the telecommunications service providers lend weight to this:

"The local telecommunications infrastructure (telephone, radio pad or GPRS) from the point of sale to the issuing bank during an authorization request has the ability to sustain a zero floor limit". The telecommunication and technology respondents answered "Agreed" and "Strongly Agreed". The mode for the decoded responses was "4" with the entire distribution of the responses under the "Agreed" and "Strongly Agreed" categories of the applied Likert scale. The technology is currently deployed in the domestic credit card market. The merchant decides on the respective technology that it will use to fulfill credit card processing. The acquirer gives advice to the merchant on the most efficient and cost-effective solution to accomplish the processing. The acquirer does not own nor maintain this network as it is not part of the core business of the acquiring bank. The merchant is responsible for signing up with a chosen service provider as it is the merchant that is accountable for the operational costs and overheads to that particular service provider. GPRS technology is the most cost effective and contemporary technology that can be used to meet the requirements of a zero floor limit. It is an "always-on" technology, as a user can remain connected for long periods without transmitting any data. GPRS has several unique factors such as the speed. The maximum speed of a GPRS connection is around 171.2 kbps when using all 8 of the GPRS timeslots at the same time. This is around three times as fast as the usual data transmission speeds over today's fixed telecom networks and ten times faster than the CSD or circuit switched data on the GSM Networks. GPRS works by allowing all the information to be transmitted more quickly, immediately and efficiently across the mobile network. GPRS is also less costly to send data than SMS and Circuit Switched Data. GPRS connects instantly so information can be sent and received immediately as and when the need comes up – depending on radio coverage. Connectnet commented that *"A zero floor limit is easily attainable when using GPRS, because transactions take less than 10 seconds to be processed. It will also not increase the customers cost per transaction, because monthly call charges are fixed on GPRS"*. Fastnet commented on authorizations and floor limits by stating *"Unlike the rest of the*

world (which doesn't use them as far as I know), floor limits exist because of two fundamental issues:

- *The slower speed of online transactions via telephone causing queuing issues at retailers.*
- *The increased volumes of online authorizations causing server load on the Bank's server.*

I believe that approximately 80% of Standard Bank's authorizations are below the floor limit. Making all authorizations go online therefore implies a five-fold increased in load (100%/20%) to the authorization servers. Since these servers already run at high loads during peak periods, this is a problem".

The comment on floor limits being introduced in order to mitigate the load that the volumes would have on the issuing and acquiring bank's hardware and software is supported by the research. The adoption of floor limits was a technological constraint when credit cards were initially introduced into the market in the latter half of the twentieth century. Technology has developed with the microprocessor being the culmination of the explosive growth in telecommunications and technology. This technology has enabled the growth of high-power, low cost computing which allow the microprocessor to encode, transmit and decode the vast amounts of information along electronic highways. The cost of microprocessors continues to fall while their power increases (a phenomenon known as Moore's Law, which predicts that the power of the microprocessor technology doubles and its cost of production falls in half every 18 months). As this happens, the costs of global communications are plummeting.

The GPRS may be a viable solution but it has its constraints as well. Interviews had with technology experts within Standard Bank (D, Els, N, Jansen, Network Architects – Infrastructure Solutions Design, 2007 Personal Interview, 06 August 2007, 5 Simmonds Street, JHB) have warned about the time slots and coverage of GPRS services. The resource is neither infinite nor infallible. The 8 time slots are not dedicated to data transmission only. The time slots are shared with voice (caller conversations) transmission. The prioritization of the time slots and the concomitant load balancing, depending on the GPRS coverage, are key

considerations to fulfilling a zero floor limit. To rely solely on GPRS for a zero floor limit may be counterproductive. Should a particular merchant trade in an area that has a high density of human traffic that are using their cellular telephones for voice transmission, the occupancy of the 8 time slots for data transmission pertaining to credit cards is not dedicated. This also needs to be seen in the context of the merchant's location in relation to the coverage afforded by the GSM base stations. Further constraints may include infrastructural restrictions in terms of the coverage barriers (e.g., high density concrete). Because service delivery and fulfillment to the merchant and the customer transacting with a credit card are vitally important, it is not prudent to rely solely on GPRS technology in light of the constraints mentioned above.

"The reduction of floor limits will not have a negative impact on cardholders at the point of sale". The majority of the respondents "Strongly Agreed" (the mode was "5"). This lends evidence to the fact that the telecommunications respondents have confidence in the infrastructure and technology to support a zero floor limit environment. This response is understandable due to the telecommunications technology available to the credit card industry. What is debatable is the issuer's ability to handle the increase in authorization traffic as well as the data switches that route the authorization requests to the issuing bank. This is discussed under the fourth Proposition. The respondents' answer to this question is congruent to their answers *to "An increase in authorization volumes attributable to a zero floor limit will adversely affect issuers in their ability to process the transactions"* and *"An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions."* The majority of the responses were "Disagree" which provides an insight into the confidence these respondents have on the ability of the bank to handle the volume of authorization requests. One needs to consider the position of the acquiring bank in handling the authorization volumes. If a transaction is conducted on a credit card where the acquiring bank is not the issuing bank, it will need to receive the transactions from the merchant and route the authorization to the issuing bank. The concomitant authorization response would then be re-routed back to the acquirer from the issuing bank. The acquirer's ability to handle the authorization requests and

responses is as important as the issuer's ability to process the authorization request.

The Merchant Services personnel that service the merchant base from a sales and support perspective answered differently to the questions. Their answer *to "Local acquirers have the technological capacity to entertain a zero floor limit environment in terms of handling an increase in authorization requests"* was "Disagree". This response was harmonious to their answer to *"An increase in authorization volumes attributable to a zero floor limit will adversely affect acquirers in their ability to process the transactions"* which was "Agree". The Merchant Services personnel do not get involved in the technical installation of the point-of-sale device nor the telecommunications services and support. It is their perceptions that are important in considering the technology school of thought as posited in by the researcher.

The stress test performed on Standard Bank's front-end processor (Postillion) suggests that the optimal metric for system performance is 65 TPS (prior to the upgrade after the stress test where the front-end processor has now doubled the processing capability as mentioned earlier). The data obtained from Standard Bank's data warehouse implies that had zero floor limits been introduced in 2006 under the old processing capability (assuming that postings followed the same distribution as authorizations), an increase in TPS ranged from 61 TPS to 91 TPS. This range exceeded the comfort zone on more than one occasion. At 65 TPS the system performs optimally with no degradation in service. The system is capable of absorbing transient spikes of over 100 TPS. When the system was stressed to 88 TPS, the system is performing under stress. Response times have degraded (by up to 200%) and reduced service is being offered with some transactions being discarded as volumes grow towards 88 TPS. Transient volume spikes will temporarily decrease the grade of service further. Over-stressed results (over 88 TPS) show that the performance is severely retarded. System behaviour is erratic with response times between 200% and 800% worse than those experienced at 65 TPS. The stress tests show that a hardware upgrade (increase in available CPU capacity) will be required before transactions rates of more than 65 TPS can be sustained for periods exceeding a few minutes. This upgrade took place but has not been stress tested yet. The calculated expansion in TPS as a result of a

theoretical zero floor limit (up to 91 TPS), does not take into consideration the growth in the card base over time which will increase sales and concomitant TPS. This further suggests that service degradation could occur in terms of responding to authorization requests in a timely manner. An upgrade to the front-end system infrastructure would need to be done to accommodate the full zero floor limit environment. As Standard Bank may encounter system constraints as an issuer in processing the authorization requests (and adversely affect its cardholders), it will also encounter constraints as an acquirer (and adversely affect its merchants and issuers' cards used at the merchants). The 65TPS threshold mentioned includes all transactions including those acquired by Standard Bank. *Figure 16* illustrates this scenario:

Figure 16: Standard Bank's distinction between issuing and acquiring authorisations

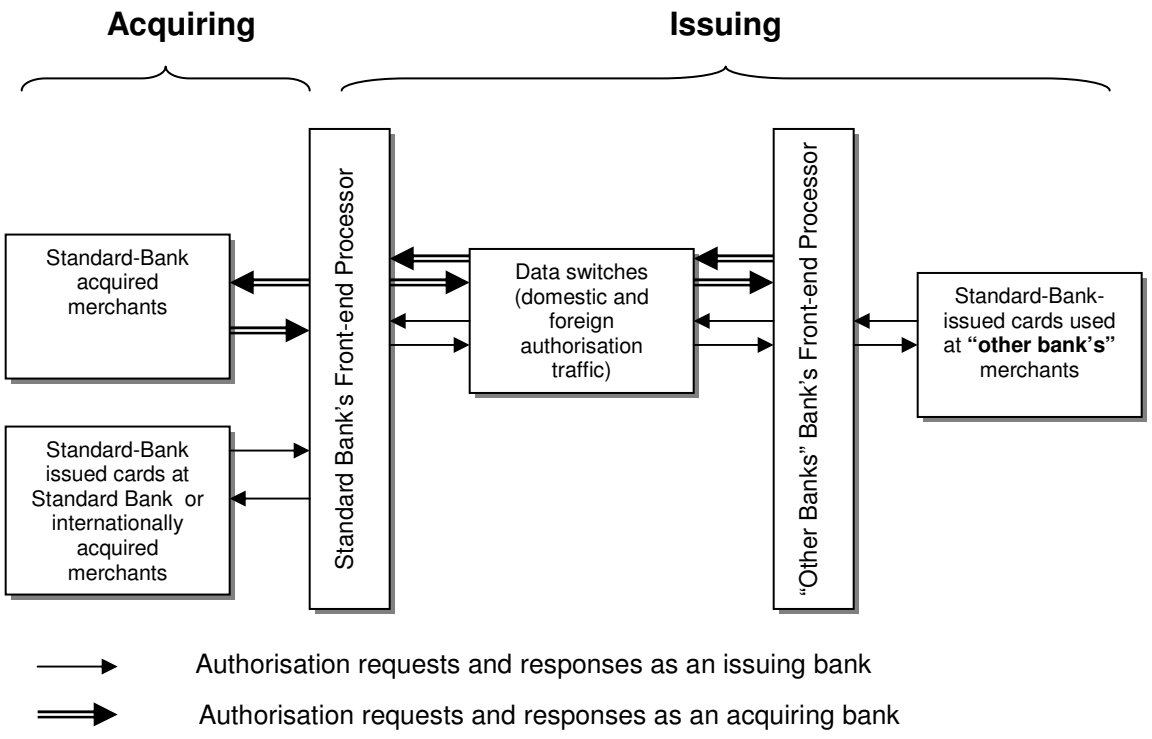


Figure 16 illustrates the role that Standard Bank's front-end processor plays in authorizing transactions. Standard Bank will authorize cards issued by it as well as route transactions where other card issuer's cardholders transacted at Standard

Bank merchants (the acquiring segment illustrated in the figure). The service degradation due to not being able to service the increase in TPS, will affect other role-players in the domestic market notwithstanding the following:

- Domestic agent banks (as card issuers),
- Standard Bank-issued cards and their cardholders,
- Standard Bank acquired merchants,
- International banks whose cardholders use their cards at Standard Bank merchants,
- Transaction switches (Bankserv).

The technology and telecommunication respondents' response to *"Issuers and acquirers can wait for the full implementation of EMV (CHIP and PIN) as a solution to reducing fraud"* was "Disagree". The respondents acknowledged in their comments that the roll-out of chip within the South African industry would be slow. This is further supported by the Merchant Services and Fraud Risk Management personnel. The implementation of EMV is expected to curtail fraud losses due to the on-board chip parameters personalized to the card and the merchant's point-of-sale device. This, coupled to the fact that a PIN is used to authenticate the cardholder other than signature, is a further risk mitigation expectation. PIN is more secure than signature as a cardholder authentication mechanism. The doubt expressed by the respondents is related to the lethargic roll-out of chip (EMV). As most magnetic-stripe credit cards enjoy two year expiration dates (whereupon a renewal card is sent to the customer), it is expected that the chip roll-out to the entire card issuing base could take up to two years. A further risk mitigation is that should the on-board chip be damaged, the transaction will automatically revert to the magnetic stripe which will by design be subject to a zero floor limit. This operational functionality must be taken into consideration as it may further exacerbate the ability of the issuing and acquiring bank to handle the authorization volumes. The dependency on when an EMV transaction goes for authorization is dependent on:

- The EMV parameters personalized to the chip
- The EMV parameters personalized to the point-of-sale device
- The functioning of the chip at the time of sale

In the event that the issuing and acquiring bank do not do the respective research in setting the chip and point-of-sale parameters, coupled to the chip functionality (whether the card is used at an EMV-enabled point-of-sale device or fallback to magnetic stripe), the authorization volumes may prove to be onerous for the issuing bank.

3. The third Proposition is that the cost of introducing a zero floor limit in South Africa is negligible in relation to the fraud which floor limits sustain. It has already been mentioned that the domestic fraud within the South African credit card market in 2006 was R179M of a total of R257M. This comprised 70% of the South African bank-issued credit card fraud that was perpetrated in South Africa. Of this figure, a further anticipated 35% was perpetrated below the merchants designated floor limit (based on the calculations done in chapter 5). The costs of the various technologies are listed below:

Table 4: Telephone Line

Service	**Tariff**
Business installation	R342.30
Monthly Rental	R132.75
Local calls (0-50km) – peak rates	
Minimum charge for the first unit of 89 seconds	R0.59
Long distance calls (> 50km) – peak rates (per minute)	R0.72
Outgoing calls to mobile network (1 minute)	R1.89
International calls to the United States – peak rates (per minute)	R1.20

Source: Telkom South Africa, BMI-T, 2006 (387)

Table 5: GPRS

	Lite	Standard	Express
Monthly charges (ex VAT)	R 175.00	R 195.00	R 295.00
Nº. of Transactions per month	600	1800	3000
Data Cap per month	0 - 1.5MB	1.5-2.5mb	2.5-10mb

Source: www.xlink.co.za

Table 6: Fastnet Radio Pad Tariffs

Purchased Radio PAD (becomes the property of the customer)

Option	Connection Fee (Once-Off)	Monthly Maintenance Fee	Call Charges (Peak Hours)	Call Charges (Off-Peak Hours)
Radical	R75.30	R30.75	11.5 Cents	11.5 Cents

Rented Radio PAD (Remains the property of FastNet)

Option	Connection Fee (Once-Off)	Monthly Maintenance Fee	Call Charges (Peak Hours)	Call Charges (Off-Peak Hours)
Benefit	R75.30	R80.50	43.5 Cents	18.0 Cents
Merit	R75.30	R126.40	31.5 Cents	18.0 Cents
Value	R75.30	R178.50	18.0 Cents	18.0 Cents

Source: www.fastnet.co.za

If one considers the costs mentioned above, it becomes apparent that from a merchant's perspective, the cheaper telecommunications option for authorising transactions is GPRS. A break down of the costs shows the following:

Telephone fixed cost range (excluding installation): R132.75 per month
Telephone variable cost range: R0.59 to R1.89 per call

GPRS fixed cost range (excluding installation): R175,00 to R275,00 per month
GPRS variable cost range: **Nil**

Radio Pad fixed cost range (excluding installation): R30.75 to R178.50 per month

Radio Pad variable cost range: R0.115 to R0.435

To work out a generic telecommunications cost for a merchant would not be viable as their credit card volumes are dependent on many factors notwithstanding:

- The merchant's location
- The merchant's patrons and their propensity to purchase with a credit card
- The nature of the merchant's merchandise
- The seasonality of the merchant's sales.

In considering the costs associated with the telecommunications deployed, one must also consider the speed and efficiency and reliability of the service. In obtaining the comments from the telecommunications service providers survey, XLINK mentioned *that "Yes, the merchant's telephone costs will increase substantially if they dial up through Telkom. Merchants using GPRS bill might increase slightly as this is dependent on X.25 and if they go over the packaged number of transactions".* A further interesting statement made by X-Link that supports the mentioned disintermediation of X.25 mentioned in chapter 3 is "*X.25 is another point of failure – acquiring banks should consider moving to IP"*. Connectnet mentioned in their survey *"A zero floor limit is easily attainable when using GPRS, because transactions take less than 10 seconds to be processed. It will also not increase the customers cost per transaction, because monthly and call charges are fixed on GPRS".* Both of these statements support the research done on the speed and efficiency of GPRS. It is clear that GPRS is the better technology to adopt if one is considering speed, cost and efficiency. The questionable component of GPRS technology as mentioned above is the dedication and reliability of the service due to the occupancy rates of the 8 time slots for data and concomitant infrastructural considerations. Fastnet commented on telephone telecommunications as a data conduit from point-of-sale by stating *"telephone dialup authorizations take 40 to 60 seconds to connect and complete (versus 10 to 15 seconds on Radio PAD and GPRS), which causes queues to form at retailers during peak periods".*

The costs of introducing a zero floor limit are not only restricted to the telecommunications from a point-of-sale perspective as positioned above. One needs to consider the following costs as well:

- The cost for the issuing bank and acquiring bank to scale up their hardware and software to deal with an increase in authorization volumes.
- The cost to the merchant in terms of the increase in their operational costs to fulfill a zero floor limit environment (principally telecommunications costs).
- The cost to the merchant in the event that the telecommunications selected to support a zero floor limit environment loses sales due to the "timing-out" of the authorization request
- The cost to the acquiring bank of losing market share due to merchants moving to competitive acquirers which may still offer floor limits as negotiated with the issuing banks.
- The potential loss of interchange revenue by the issuing bank and reduced commission revenue by the acquiring bank. The merchants may argue that the risk associated with the credit card transactions does not warrant the interchange rate paid on these transactions due to the lesser risk associated with the authorized transaction. As already mentioned in this research report, acquirers pay issuers interchange to cover the issuer's cost of funds (in funding the credit), fraud and credit risk and other operational costs the issuer may incur. The acquirer recovers this fee from the merchant by charging a commission on every transaction.

Almost every merchant in South Africa has electronic point-of-sale devices (stand alone or integrated solutions). This requirement is a prerequisite to facilitate card transactions. The most feasible telecommunications solution purely from a cost perspective would be GPRS.

4. The fourth Proposition is that the local banking infrastructure and technology can accommodate an increase in authorisations as a result of a zero floor limit environment. The analysis done on the ability of the domestic switch (Bankserv) and Standard Bank (as an issuer and as an acquirer) to handle the authorisation traffic attributable to a zero floor limit environment was discussed in chapter 5. It

appears that the domestic switch has the ability to handle the anticipated increase in Standard Bank authorisation traffic. As mentioned, the highest authorization activity on cards for the month occurred on the 22nd December, peaking at 71.9 TPS. Bankserv have confirmed that their maximum TPS threshold is 156 TPS for one site. Bankserv process authorizations via two separate sites (continuous processing) to balance the load and each site can maintain 156 TPS concurrently (reference: Bankserv). This results in a total TPS threshold of 312 TPS processing capability. The anticipated increase in authorization volumes in a zero floor limit environment from a local industry perspective has not been determined. This is due to the sensitivity of the data amongst the local competitors and the differentiation between transactions that are switched by the domestic switch and transactions that go directly to the issuer bypassing the domestic switch altogether. The analysis done with Standard Bank's data for 2006 presents the following theoretical increase in authorization traffic had zero floor limits been introduced in 2006:

Table 7: Anticipated increase in authorisations had a zero floor limit been introduced

Month	Increase (%)	Max Authorizations per Second
Jan-06	85%	61
Feb-06	77%	62
Mar-06	70%	62
Apr-06	69%	80
May-06	72%	66
Jun-06	67%	65
Jul-06	65%	77
Aug-06	70%	66
Sep-06	65%	86
Oct-06	70%	70
Nov-06	65%	69
Dec-06	59%	91

The anticipated increase in authorisation traffic had zero floor limits been introduced in 2006 is reflected in the table above. The combination of authorisations and postings (batched transactions – i.e. transactions conducted below the merchant's floor limit) comprises the increase in authorisation traffic above. The maximum TPS that occurred was in December 2006 at 91 TPS.

Albeit that Standard Bank had scaled-up its front-end processor (Postillion) where it originally had a comfort zone of 62 TPS to double the capacity (from a comfort zone perspective) to a theoretical 124 TPS, it cannot be alluded that the spare capacity is 33 (the difference between the 124 TPS and 91TPS). The logic may be sound on a mathematical basis, however, the relationship between the CPU usage, the TPS and system memory consumption is *not linear* (as suggested by the calculations) and cannot be argued mathematically as done above. CPU consumption is positively correlated to memory use and TPS (as shown in the stress test results). No logarithmic scale is available at Standard Bank to represent this relationship. In order to unequivocally prove whether the front-end processor can handle a zero floor limit, a stress test (acid test) must be performed where a zero floor limit based on production volumes is used. This stress test will differ from the original stress test performed in that its primary objective is to test zero floor limits (as opposed to stress test the Postillion with injecting multiple transactions). The two stress tests are not dissimilar from each other in that they both put the front-end processor and ancillary systems under stress (volume testing). The key differentiator however, is that zero floor limits are tested which will give us a clear indication of the processing ability, queue lengths, queue waiting times, CPU usage and response times of the front-end processor and peripheral systems. This stress test must consider the increase in volumes as an issuing bank and as an acquiring bank as illustrated in *figure 48*. If the domestic industry follows suite in terms of introducing zero floor limits, the multiplier effect on Standard Bank's front-end processor as well as the domestic agent banks (as issuers and acquirers) and local switches would need to be determined. The research done has been on Standard Bank's ability to process transactions in a zero floor limit environment. With the exception of the stress test performed, Standard Bank–issuing volumes have been considered only (Standard Bank cards are used in the domestic credit card market at all acquiring bank's merchants). The acquiring portion of Standard Bank in terms of routing authorization requests to other issuing banks have not been taken into consideration. In the event that merchants which are acquired by Standard Bank are placed on a zero floor limit, the multiplier effect would be substantial. The reason for not incorporating the acquiring volume is that this has not been readily available at the time of this research report. Card and sales growth (including merchant sales and banking

growth) would need to be tested as well to determine the anticipated growth in the number of transactions over time.

Based on the initial stress tests performed on Standard Bank's front-end processor as well as Bankserv's ability to theoretically handle an increase in Standard Bank's authorization traffic provides a theoretical baseline to suggest that Standard Bank cannot sustain a zero floor limit environment. This however is not a complete synopsis of the entire industry as the selfsame studies need to be performed by the domestic banks with due consideration on Bankserv as the domestic switch on their concomitant volumes.

Conclusions

Below floor limit fraud is a worrisome concern for domestic issuers and acquirers. The advent of chip and PIN is expected to reduce the below floor limit fraud initially. The migration to other fraud types is expected notwithstanding false application and card number used fraud. Albeit that issuers and acquirers adopt chip and PIN in the South African market and follow the rest of the world in adopting this technology, the magnetic stripe is expected to be part of the credit card transactability in the next 5 years at least. The reason for this is that many merchants and acquirers in the world are lagging behind the investment in chip and PIN. Many merchants' point-of-sales will only accept the magnetic stripe technology and in order not to lose potential sales, the issuing bank will still issue cards to its cardholders with this technology. The impact that chip and PIN will have on the domestic issuer's ability to process an anticipated increase in online transactions is not completely known. Standard Bank is theoretically able to handle the anticipated increase in authorization traffic assuming a zero floor limit, but this statement is based on the stress test performed on injected transactions and not an assumed zero floor limit scenario. The processing ability of the upgraded front-end processor (doubling the old processing speed (124TPS of assumed comfort zone)) was not stress tested. The stress test volumes over the tested period suggest that production volumes will not reach the thresholds reached during the stress test. This however, excluded the assumed increase in authorization volumes for a tacit zero floor limit. The stress test performed 409,000 transactions over one-hour and twenty minutes which suggests an average TPS of 85. If one considers the anticipated increase in authorization volumes had a zero floor limit been introduced (from an issuing perspective only) in 2006

(Appendix 4), it becomes theoretically apparent that this average will be met in production. The stress test goal was to increase the injected transactions to put the hardware and software under stress. The increase in injected transactions amplified the average TPS before the system returned to normal processing.

The multiple data systems and intermediaries (and their concomitant systems and processing capability) in the credit card model are key dependencies to ensure that the transactions is sent to the issuer and acquirer and processed within reasonable time frames. If one takes the theoretical production volume spike in December 2006 (an estimated 91 TPS) and compares this to the processing capability of the front-end processor and peripheral front-end systems (124 TPS), this represents a capacity cushion of 33 TPS (or 1980 transactions per minute). This may not be contingency enough to cater for a zero floor limit environment. The data obtained and analyzed represents averages (TPS) only and may not accurately represent transient spikes in a production environment (peak purchasing times or seasonal credit card spend). As the relationship between TPS processing capability and authorization requests is not linear (it is more logarithmic), the ability to ascertain the actual impact of zero floor limits is difficult. The CPU processing ability, and queue lengths and waiting times for the authorizations are further considerations that need to be tested.

The convenience and speed of use of the card product at point-of-sale and other physical channels from a customer's perspective is integral to the value proposition. This is coupled to the customer's expectations of security in using the product. The disintermediation of the X.25 network In Standard Bank (as discussed in Chapter 2) would assist in the speedier transportability of the transaction. It was confirmed that the X.25 protocol is archaic and outdated. Standard Bank would be better positioned to service its merchants and their customers by using GPRS and receiving the transactions directly into its infrastructure and avoiding the X.25 protocol. GPRS is a potential solution to reducing the merchant's costs in deploying a technology that would facilitate quicker authorization requests and responses (again dependent on the issuer's and acquirer's ability to process transactions). The reliability of the service is questionable due to the time slots and channels afforded to data and voice and the coverage that the base stations afford. To rely solely on this technology where the load balancing and capacity planning by the service providers may be dependent on the above factors is too risky for acquirers The risks and associated costs are mentioned below. A further consideration

is the merchant categories where fraudsters generally spend. The majority of the fraud takes place at supermarkets, grocery stores and department stores. These merchants generate the greater part of the retail volume. These large retailers see the customer as one of their patrons and invest large sums of money in increasing their patronage and prompting repeat purchases. If their clients are continually negatively impacted by delays in purchasing with a credit card attributable to the technology adopted (slow telecommunications and issuer/acquirer response rates), they will lobby against the domestic issuers and acquirers. The issuing banks' brand integrity and that of the associations (MasterCard and Visa) is at risk as well as that of the retailers themselves. The large retailers have a substantial market of customers that take-up their in-store credit cards. This is currently a competitive value proposition to credit cards issued by domestic banks. The competition in this arena may increase and result in bank-issued credit card patronage attrition to the competitor products.

The commercial engagement with merchants necessitates a responsible approach by acquirers. To negotiate a single technology in the form of GPRS and rely on the service providers to fulfill the data requirements in terms of increased authorization traffic may cause the merchants to lobby for reduced commission fees. The reduced risk of sending authorizations online for issuers to process may further exacerbate the lobby issue (fraud and credit risk for the issuing bank). As fraud funding is inherent in the interchange (which is part of the merchant commission that is paid to the acquirer), merchants may argue that risk is reduced and hence interchange should be adjusted accordingly. As interchange on an entire card base (where this fee is applicable) is a key revenue stream for issuing banks, the costs of reduced interchange in relation to the fraud savings (on a small portion of the card base) may present an interesting analysis. If acquirers promote GPRS to its merchants and transactions are not fulfilled due to technological capacity constraints (as already mentioned), the following will occur:

- Slower response times from issuing banks. This may cause the cardholder to question the product in fulfilling the cardholder's needs of speed, convenience and ease of use. This may also cause the cardholder to question the merchant's ability to fulfill the selfsame needs.

- The merchant's operational costs will increase as the authorization request may "time-out" resulting in the merchant telephoning the acquiring or issuing

bank for authorization. This not only results in increased telephony costs but delays the sale and causes queues to swell at the purchase point which may lead to loss of sales on the part of the merchant.

- The loss of revenue for the merchant may result in them seeking recourse from the acquirer.

In order to implement a zero or reduced floor limit policy, it has to be introduced by the domestic issuing and acquiring banks collectively. The timing of the implementation is an important consideration. In the event that an issuer or acquirer defers the respective implementation, it would trade-off its fraud losses for increased market share. Merchants and/or cardholders may migrate to the late adopter of this initiative as the costs and convenience from a merchant or cardholder perspective would be better fulfilled by the laggard. The regulation of this adoption is currently under the ambit of MasterCard in their publication. The 2005 MasterCard International published mandate (*Appendix 5*) states that "Effective 8 April 2006, MasterCard will require a card acceptor *(acquirer)* to obtain an authorization from the issuer for:

- All non face-to-face transactions, regardless of the transaction amount,
- All face-to-face transactions, card-read or key-entered, occurring at a location with a point-of-sale (POS) device that has both online and magnetic stripe-read capability, regardless of the transaction amount"

Recommendations

The following recommendations emanate from the research and represent the most feasible solutions in adopting reduced or zero floor limits. Each recommendation is interdependent of the others and comprises a holistic solution for the domestic industry.

1. Incrementally reduce floor limits based on high risk methodologies

   To implement a zero floor limit across all merchant categories may not be feasible in light of the technological constraints involved. A more prudent approach may be reducing floor limits incrementally based on a collective methodology. It is proposed that the high risk merchant categories and their respective geographies

be determined first. The roll-out of the zero floor limits must be aimed at these establishments.

The roll-out must take into consideration the nature of the merchant's average ticket value which is based on the merchandise that the merchant sells. Those merchants that generate the majority of the authorization volumes due to the nature of their merchandise are also a key consideration. The large retailers that have the technological infrastructure to host an industry negative card file must be differentiated from the smaller merchants that use a conventional point-of-sale machine.

Once these segmentations have been performed, it is possible to implement a strategy to reduce or zero floor limits. The incremental roll-out approach is supported by the respondents in the survey done. This roll-out is envisaged to include high risk merchant category codes in high risk geographical areas. The following high-risk merchant category codes namely, service stations, restaurants and liquor stores in the greater Johannesburg area can be placed on a zero or reduced floor limit by the domestic banking industry as an initial pilot. These merchants generally have a stand-alone point-of-sale device (and the INCF file is not a current solution for these establishments). This solution is, in itself, a proactive step toward reducing below-floor limit fraud. The problem, however, is that the fraud is expected to migrate to other merchant categories in the same area or the same merchant categories in other geographical areas.

2. <u>The industry negative card file roll-out to large retailers.</u>

Many large retailers currently subscribe to the industry card file as provided by Retail Decisions. Not all large retailers however, receive the full negative card file and may only receive subsets which list the most recent compromised cards. This solution has reduced post-statussed fraud (by the issuing bank) at the subscribed establishments. Post-statussed fraud is fraud that takes place after the card has been statussed lost, stolen or fraud by the issuing bank. The post-status nature of the fraud is as a result of the four-day fraud life cycle as detailed in this research report. The problem with this type of solution is the following:

- Pre-statussed fraud (by the issuing bank),
- Reliance on the merchant's hardware and software infrastructure,

- The segmentation of merchants receiving a full file as opposed to a subset file,
- The reliance on merchants to invest in upgrading their infrastructure to accommodate an industry negative card file,
- The reliance on acquirers to incentive merchants to adopt this solution,
- The migration of fraud to non-subscribed merchants and other channels,
- The service only confirms whether a card is on the restricted list and does not cater for generating exceptions based on abnormal usage or deviations from the cardholder's spending profile.

The service provider is merely an intermediary in the provision of these services and relies on merchants, issuers and acquirers to provide the solution for its services. The decentralization of the issuer's exception file (compromised cards and cards abused by cardholders) is the best option in an environment that supports a floor limit. It would be better to disintermediate this service provider by allowing all transactions to go to the issuing bank for authorization as the issuers are able to detect questionable cardholder activity. This is due to the fact that the cardholder's transaction history and other information are contained at the issuing bank. To centralize the solution (i.e. all transactions go online to the issuer for authorization) is too risky as an initial adoption (due to the envisaged technological constraints that may prevent this from happening). This assumption is based on the analysis done on Standard Bank's front-end processor (and in the absence of a stress test centered on zero floor limits alone as already discussed).

In order to leverage the decentralized model (and mitigate the technological issues from an issuer's perspective), it would be prudent to adopt the recommendation set out in section 1 *and* investigate the possibilities of:

- Providing incentives to merchants to upgrade their infrastructure or
- Networking shopping malls and similar retail configurations
- Adopt GPRS as an initial telecommunications technology with a secondary technology to cater for GPRS "time-outs"
- Provide telecommunications hardware and software using existing telecommunications networks

3. Network shopping centers

A possible solution to mitigate the constraints with the decentralized restricted card file concept (the industry negative card file) is to create a local or wide area network within shopping malls. The constraints mentioned in 6.5.2 can be mitigated if the industry negative card file resides within large shopping malls and all merchant's point-of-sales communicates with a centralized server. The maintenance of the local area network can be outsourced to the current (or other) service provider. The issuing bank will transmit their exception cards to the service provider who in turn will ensure that the cards are placed on the server. The issuer currently trickle feeds statussed cards on a 15 minute basis to the service provider. This methodology can still be adopted in the decentralized model. Those retailers that have their own integrated solutions (a client-server in store as opposed to a stand-alone point-of-sale) can be networked with the respective shopping mall server. Those merchants that have a stand-alone point-of-sale device can be configured to communicate with the server using telephone line, radio pad or GPRS. This will cut down on the telecommunications costs associated with connecting with the acquiring or issuing bank from a remote site.

4. Adopt GPRS as the first dial-up with a secondary technology for contingency purposes

The merchants can be prompted to use GPRS technology as opposed to radio pad and telephone. Most merchants have a landline for telephone calls. A hybrid point-of-sale can be configured to first attempt to use GPRS and if there is a telecommunications failure, to automatically divert to telephone for dial-up. Technology exists in the market whereby the point-of-sale can be connected to telephone line and GPRS. As already discussed, there is no guarantee that the 8 time slots used in GPRS can be dedicated to data (as opposed to voice). Albeit that the fixed costs for merchants may be doubled (GPRS and telephone line), the costs associated with GPRS are negligible for those merchants that do a substantial amount of credit card transactions. The GPRS monthly rental can be subsidized to an extent by the issuing and acquiring banks.

5. Chip and PIN

The deployment of chip and PIN is an integral part of the floor limit solution. An off-line chip transaction where a PIN is keyed-in by the cardholder and the chip parameters mitigate fraud risk is a solution for lost, stolen, NRI and counterfeit fraud. Should the chip be rendered inoperable by a fraudster and the transaction defaults to the magnetic stripe, it will automatically be subject to a zero floor limit. The chip parameters allow the customer to spend offline subject to limits (accumulative transaction counts and amounts) before the chip recommends to the point-of-sale device to go online for authorization. The limits comprise lower cumulative counts and amounts and upper cumulative counts and amounts. If the lower cumulative counts or amounts are reached, the point of sale will attempt to go online for authorization. In the event that the authorization attempt is unsuccessful, the transaction can still be performed offline (subject to PIN authentication). In the event that the upper cumulative counts and amounts are met, the transaction must go for authorization. In the event that this attempt is unsuccessful, the chip will not allow and further transactions to take place. In authorizing the transaction, the issuer sends a script back to the chip to reset the accumulated counters on the chip.

The ability to change the personalized chip parameters during an authorization is key to ensure that the load in terms of authorization traffic is reduced. At the moment, the chip parameters (upper and lower cumulative counts and amounts) are set on the chip and cannot be changed during an authorization request.

6. Service codes.

Contained within the magnetic stripe is a 3-digit numeric value (service code) that communicates with the point-of-sale on the nature of the product and where it can be used. The service code advises the point-of-sale whether the card is subject to a magnetic stripe transaction or alternative technology (i.e. chip), whether PIN must be keyed-in by the customer (or the transaction is signature-based), whether the transaction must come online for authorization, where the card can be used (domestically only or domestic and international) and the type of devices where the card can be used (point-of-sale devices, self service devices, etc). The issuing

bank sets the service code for the product. For high risk products, the issuer can personalize the service code to force all transactions online or be subject to PIN (in which case all transactions must come online). Petrol cards and service stations represent a large portion of fraud as represented in section 1 above. As petrol is regulated in the South African market by the government, the economics in terms of commission and interchange is different. No interchange is charged on petrol transactions and the issuing bank pays the acquiring bank a transaction fee for every sale. As petrol prices are subject to fluctuation and more often than not increase on a regular basis (fuelling inflation), the floor limits increase as the petrol price increases. The floor limit increase is based on collaboration amongst issuing and acquiring banks. In lieu of the growth in fraud perpetrated on these cards, it is not feasible to continue increasing the floor limits. It is questionable whether the pricing caters adequately for the growth in fraud losses and it is necessary to reduce floor limits at garages or change the service code of these products.

7. Bankserv

The domestic switch (Bankserv) can be used to deploy a restricted card file. As all online transactions conducted at merchants where the acquirer and issuer are not synonymous must be switched by this entity, it makes good sense to host the industry negative card file here. Bankserv's core competence is in the data switching realm and they invest to this end. To mitigate potential issuer and acquirer processing delays, all transactions can be sent online to Bankserv. Point-of-sale devices are personalized with "network user addresses (NUA)" that comprise the numbers or addresses the point-of-sale devices must connect to for authorization. There is more than one address personalized to the point-of-sale that allows the device to switch to different NUA's depending on the response time from the host machine (acquirer). For those merchants that do not switch via Bankserv (the acquirer and the issuer are synonymous), one NUA can be captured to send transactions to Bankserv for reference against the industry negative card file. Bankserv can potentially host the industry negative card file for all merchants that have a zero floor limit.

8. Issuer and acquirer scaling-up.

The issuing and acquiring bank can scale up their front-end processors and ancillary devices to handle a zero floor limit.

9. Pricing

Issuers and acquirers can reduce the interchange and commission fees to promote a zero floor limit environment. The reduction in fees can be used to subsidize the merchants operational costs and the fees themselves can be subsidized from the fraud savings. The issuers can reduce their interchange rates and the acquirers can pass this discount to the merchants by reducing their commission fees.

Glossary of terms

3G (Third Generation): 3G is an ITU specification for the third generation (analogue cellular was the first generation, digital PCS the second) of mobile communications technology. 3G promises increased bandwidth, up to 384 Kbps when a device is stationary or moving at a pedestrian speed, 128 Kbps in a car, and 2 Mbps in fixed applications. 3G will work over wireless air interfaces such as GSM.

Acquirer: A member that maintains the merchant relationship and acquires the data relating to a transaction from the merchant.

ADSL (Asymmetrical Digital Subscriber Line): ADSL is a broadband technology that utilized copper telephone lines, but which is much faster than a regular telephone connection, and can carry data communications and voice communications simultaneously. This is achieved by dividing the total capacity of the line into multiple, independent bandwidth channels, where each channel operates only on a specific range of frequencies. ADSL is typically capable of speeds of up to 10 or 12 Mbps. Unfortunately ADSL is available only to subscribers who are located close to Telkom switching centers.

Authorisation: A request by an acquirer for issuer approval to complete a transaction involving a credit card.

ATM: Automated Teller Machines, cash points, allow you to access cash with a credit card or other card associated with your bank account. You need to enter your personal identification number (PIN) into the machine to access cash.

Broadband: A transmission medium capable of supporting a wide range of frequencies, typically from audio up to video frequencies. It can carry multiple signals by dividing the total capacity of the medium into multiple, independent bandwidth channels, where each channel operates only on a specific range of frequencies. This term has become a generic term for communication technologies that can carry data at high speeds. For example ADSL, WiFi, and Ethernet, which are all broadband technologies.

Cardholder: The authorised user of a card issued by a licensed member.

Chargeback: A procedure whereby an issuer charges (reverses) all or part of the amount of a transaction back to the acquirer in accordance with Association regulations.

Circuit Switching: Circuit switching is only maintained while the sender and recipient are communicating, as opposed to a dedicated circuit, which is held open regardless of whether data is being sent or not. This is the main technology used for legacy voice telephony and which is now gradually being replaced by more efficient packet switched technology.

CNP (Card not present) Fraud: The card number, expiry date and unique card values are compromised and used in a non-“face-to-face”, or card-not-present channel**.** These channels are traditionally the internet, mail order or telephone order.

Counterfeit Fraud: Fraud perpetrated on a card where it “is an instrument or device embossed, printed, or otherwise bearing MasterCard (or branding marks) marks, so as to purport to be a MasterCard (or proprietary or other Association) card issued by a member or affiliate; but that is not a MasterCard (or proprietary or other Association) card because the embossing or printing thereon was not authorised, or because the MasterCard (or proprietary or other Association) card has been altered or refabricated, even though it was issued initially.

Credit: A contractual agreement in which a borrower receives something of value now, with the agreement to repay the lender at some date in the future. Also, the borrowing capacity of an individual or company.

Credit cards: Any card that may be used repeatedly to borrow money or buy products and services on credit. Issued by banks, savings and loans, retail stores, and other businesses.

Ethernet: Ethernet is one of the oldest and most successful LAN technologies. It was developed to run over co-axial cable, although it can now run over twisted pair. LAN-based Ethernet currently runs at speeds of up to 100 Mbit/sec.

Face-to-face transactions: These transactions are referred to “card-present” transactions. The authority to charge is provided in person, and the cardholder signs a voucher to evidence their agreement to the transaction.

False App (False Application) Fraud: A credit card application is made to an Issuer containing misleading or false information which is intended to induce a positive decision to grant a payment card facility.

Floor limits: The floor limit value is a maximum amount above which the merchant must obtain an online authorization from the issuer before completing the transaction.

Fraud: The unlawful and intentional misrepresentation or concealment of information with the intention to deceive or mislead to the prejudice of a third person.

GPRS: GPRS or the General Packet Radio Service is a non-voice value added service which allows you to send and receive data across a mobile phone network.

IP (Internet Protocol): A portion of the TCP/I[suite of protocols that specifies how information is addressed, sent and received between systems.

ISDN (Integrated Service Digital Network): ISDN is an international standard of the International Telegraph and Telephone Consultative Committee (CCIT) that covers a range of voice, data and image services. It provides end-to-end, simultaneous, digitized voice and data traffic on the same links via the same exchanges.

Issuer: A bank which issues credit cards to customers

Kilobit (per second) (Kbps): One thousand bits of data transmitted in a second, where 1 Kbps = 1024 bits per second (210 bits)

LAN (Local Area Network): A LAN describes a high-speed data communications network (usually Ethernet based) that covers a limited area. The machines linked by a LAN may all be in the same building or groups of buildings in relative close proximity.

Lost Fraud: The cardholder reports that the card had been lost. The loss of the card has resulted in fraud on the account.

Megabits (per second) (Mbps): One thousand kilobits of data transmitted in a second, where 1 Mbit = 1024 kilobits or 1 048 576 bits (220 bits)

Member: A corporation or other organisation that has been approved as and has entered into an agreement with MasterCard or Visa to be a MasterCard or Visa member.

Merchant: A retailer or any other person, firm, or corporation that, pursuant to a merchant agreement, agrees to accept credit cards

Merchant agreement: A written agreement between a merchant and an acquirer containing their respective rights and performance obligations with respect to card acceptance.

NRI (Not Received Instances) Fraud: A card dispatched to a cardholder is intercepted before receipt and subsequently used fraudulently.

Packet Switching: This is a method of switching data in a network where individual packets of a set size and format are accepted by the network and delivered to specified network destinations. The sequence if the packets is maintained and the destination established by the exchange of control information (contained in the packet header). The packets can be sent in any order, as the control information sent at the beginning of the transmission ensures that they are interpreted in the correct order at the receiving end. Because each packet carries its own control instructions, it can use any route to reach its destination. The link only lasts as long as the transmission. This also enables many users to use the same network at the same time.

Point-of-sale: A device placed at the point of interaction connected to a bank's system through telecommunication lines, designed to capture and forward transaction information by electronic means. A point-of-sale is capable of capturing data from a magnetic stripe, an integrated circuit card, or both, and it has key-entry capabilities for manual data capture. Thus a personal computer (PC) accessing the internet qualifies as a point-of-sale terminal.

Radio pad technology: Installation is as simple as connecting the antenna and the 12 V power source. Users then simply attach their computing device to the **Radio Pad** which then instantly connects them to the Telkom (x.25) packet data network. This in turn connects the user to a linked organization, be it a bank, credit card company, or burglar alarm company

Stolen Fraud: The cardholder reports their card was physically removed from their person or that they are aware of the person(s) that took the card. The fraud then took place as a result of the card being stolen.

Take-over Fraud: Fraud which occurred as a result of a person masquerading as the customer and changing card, demographic or biographic details with the issuing bank with the purpose of obtaining a card from the issuer. This fraud generally occurs when a fraudster purports to be the customer reports the card damaged. Collection (of the card) address details are given to the issuing bank.

Telecommunications: Telecommunications refers to the electronic transmission of signals for communications, including such means as telephone, radio and television.

Transaction: An action between a cardholder and a merchant or a cardholder and a member that results in activity on the cardholder account.

Twisted pair: Two insulated copper wires twisted together, with the twists varied in length to reduce potential signal interference between the pairs.

WiFi (Wireless Fidelity): WiFi is the popular term for a high-frequency wireless local area network. The WiFi technology is an alternative to a wired LAN that uses twisted pair

cabling WiFi operates in the 2.4GHz range offering data speeds of up to 11Mbps over an Ethernet network.

X.25: X.25 is a robust packet-based protocol designed to send packet data across old, unreliable telephony circuits.

Zero floor limits: A situation where a merchant must obtain an online authorization from the issuer before completing a transaction on all credit card transactions. No floor limits will be assigned to the merchant.

List of references

Akers, D, Golter, J, Lamm, B & Solt, M, 2005. *Overview of Recent Developments in the Credit Card Industry*, Volume 17, No.3: FDIC Banking Review

Anonymous, 1993. "A wave of protests forces Visa to modify its floor limit policy", *Credit Card News*, 5 (24): 3, Proquest

Anonymous, 1994. "Fighting the war against fraud", *Banking World* , 12(3): 28, ProQuest

APACS.org.uk. 2005. *Card Fraud The Facts*. Available from www.APACS.org.uk [Accessed 28 April 2007]

Baker, S, Manager IT Solutions Centre, 2007. Personal interview, 26 April 2007, 5 Simmonds Street, JHB

Bankserv, Selby, 2007

Bocij P, Chaffey D, Greasley A & Hickie S, 2006. *Business Information Systems: Technology, Development & management for the E-Business*, 3rd Edition, England: Pearson Education International

Cardwatch.org.uk. 2005. *The Cost of Card Fraud.* Available from<www.cardwatch.org.uk> [Accessed 28 April 2007]

Cellular.co.za. No date*. Fastnet Radio Pad as a microwave service provider* .Available from <www.cellular.co.za> [Accessed 02 February 2007]

Crockett, B, 1992. "Visa Requirement Could Hurt Some Banks Revenue Would Fall if Authorization Rule Drives Away Small Merchants Series:14", *American Banker*, 157 (217): 3

Diamantopoulos A, Schlegelmilch B, 2005. *Taking the Fear Out of Data Analysis*, 5th Edition, Thomson Learning

D, Els, N, Jansen, Network Architects – Infrastructure Solutions Design, 2007 Personal Interview, 06 August 2007, 5 Simmonds Street, JHB)

Standard Bank, Economic Profile of South Africa, 2005 (6)

Guerin, D, 2003 *"Fraud in Electronic Payments"*. Available from <www.trintech.com> [Accessed 11 March 2007]

Eccles, M.G, Julyan, F.W, Boot, G, van Belle, JP, 2000. *The Principles of Business Computing,* 5th Edition, Lansdowne: Juta & Co. Ltd.

Fastnet.co.za. No date. Available from <http://www.fastnet.co.za> [Accessed 02 February 2007]

Hill, C, 2005. *International Business, Competing in the Marketplace.* McGraw – Hill, New York.

GPRS.ORG.UK. No date. *GPRS Related Information* [online]. UK: GPRS.ORG.UK. Available from :<Http://WWW.GPRS.Org> [Accessed 02 February 2007]

Khanna, P, 2004. "Toys R Us unwraps POS System in Time for Holidays", Technology @ Work, 26 November, 1

Leedy P.D, Omrod J.E, 2005. *Practical Research, Planning and Design*, 8th Edition, New Jersey: Pearson Education International

Levi, M, Bissel P, Richardson, T, 1991 "The Prevention of Cheque and Credit Card Fraud", Crime Prevetion Unit Paper No.26, London

M, Keegan, *CNP Growth in the United Kingdom*, Bankserv, 2007

Markowitz, A, 1994 "Technology powers renewal, customer service", *Discount Store News*, 33 (4): 54

MasterCard International Incorporated. 2006 *MasterCard Quick Reference Booklet*, (23)

MasterCard International Incorporated, 2002. *MasterCard International Operations Manual*. (glossary 6).

MasterCard International Incorporated, 2005 *Global Operations Bulletin* No. 12 (59-75)

Newton, H, 2002, *Newton's Telecom Dictionary* 18 ed, 733

P, Marais, MIS Manager, Card MIS, 2007 Personal Interview, 03 March 2007, 6Simmonds Street, JHB

SABRIC (South African Bank Risk Intelligence Centre), Midrand, 2006

Smith, R.G, 1997. "Crime Prevention in the Digital Age", Australian and New Zealand Society of Criminology: 15 - 20

South African Card Fraud Forum, Midrand, 2007

Stair, R. and Reynolds, W. 2001.*Principles of Information Systems,* 5th Edition, United States of America: Thomson Learning.

Telkom South Africa, BMI-T, 2006 (387)

Thornton, L, Carrim, Y, Mtshaulana, P and Reburn, P (2006), "Telecommunications Law in South Africa", STE Publishers, Parktown South Africa (18)

UNISA, 2002 (42), Certificate Programme in Law, Module 3, Public Law, LexisNexis Butterworths, 2002.

Visa, *Visa Bank Card Education*, 2007 (18)

Ward.S.2007. *"Be Alert For These Credit Card Fraud Tip-Offs",* About Small Business Canada. Available from *http://sbinfocanada.about.com/od/insurancelegalissues/a/ccfraudbehavior.htm* [Accessed 11 March 2007]

Wikipedia.org. No date. *X.25* Available from <http://en.wikipedia.org/wiki/X.25> [Accessed 02 February 2007]

www.apacs.org.uk, 2007. "*Transactions with your chip and PIN terminal"* Available from http://www.apacs.org.uk [Accessed 12 September 2007]

www.biz-community.com. 2006. "*The benefits of wireless data communication"* Available from http://www.biz-community.com/Article/196/87/9916.html [Accessed 02 May 2007]

www.bis.org. 1996. The Payment System in South Africa [online]. Available from: <http://www.bis.org/cpss/paysys/SouthAfrica> [Accessed 02 May 2007]

www.finextra. 2002. South African Banks Create National Fraud Net. [online]. Available from: <http://finextra.com/fullstory.asp?id=4561> [Accessed 02 May 2007]

www.southafrica.info. 2003. Doing Business in South Africa [online]. Available from http://www.southafrica.info/doing_business/economy/infrastructure/telecoms.htm [Accessed 02 May 2007]

www.balancingact-africa.com.2007. Balancing Act News Update. *Grintek Develops Smart Power Supply Units For POS Terminals*. Available from: <www.balancingact-africa.com/news/back/balancing-act_213.htm> [Accessed 02 May 2007].

www.xlink.co.za. 2007. XLink Communicator. Available from: http://www.x-link.co.za/rates.php?pId=1&cmssitemenuid=74> [Accessed 02 May 2007].