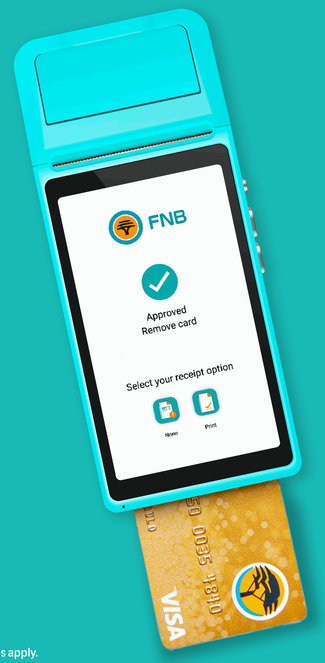
Protect your business against fraudulent transactions

For more information refer to your FNB Merchant Agreement or contact us on

+260 762 030 924



Terms, conditions and rules apply.

First National Bank Zambia Limited is a licensed Commercial Bank

Introduction

There is a real possibility that your business could be a victim of fraudulent card transactions given the sophistication of fraudsters who operate within the card payment environment. Losses related to card fraud could be very costly to your business if you don't employ the appropriate levels of diligence in preventing and mitigating fraud. With the evolving fraud trends, you need to ensure that your business is protected at all times and your staff are trained adequately to mitigate any risks.

This brochure aims to assist you in **detecting, preventing and minimising fraud** within your business by providing you with helpful tips and guidelines.

The rights and obligations of the parties ("FNB Merchant Services" and "the Merchant"), in respect of the acquiring service delivered by FNB Merchant Services to the Merchant, are set out in the Merchant Agreement terms and conditions available on www.fnb.co.za

What is a fraudulent transaction?

A fraudulent transaction is any transaction that is not approved by the cardholder. This is irrespective of whether or not the card transaction has been authorised by the Speedpoint® device or an authorisation code has been provided to you by the cardholder's bank (issuing bank).

These transactions can arise as a result of, but are not limited to:

- A transaction that is processed using a customer's financial detail, account information or payment instrument which is not authorised by the customer; or the use of a card which has not been issued by a genuine card issuer
- Non-compliance with the procedures set out in the merchant agreement
- The use of a card that has not been issued by an authorised card issuer
- The use of an invalid card
- The use of a card by a person other than the authorised cardholder
- The use of a "hotcard" (that is a debit or credit card that cannot be used as it has been reported as lost or stolen)
- The use of a card number when a card is not present

Merchant responsibilities

You must ensure that you understand your rights and obligations set out in the terms and conditions of your merchant agreement.

You must always adhere to the terms and conditions of your merchant agreement, card association rules and industry rules and regulations.

It is your responsibility to ensure that you and your staff receive fraud training from the FNB Merchant Services consultant at the time of sign up. If any additional training is required, it is your responsibility to contact FNB Merchant Services on +260762030924 to arrange this.

You must ensure that proactive measures are in place to prevent and mitigate the risk of fraud when accepting card payments including:

- Validating all cards and verifying the cardholders presenting cards for payment, as per the guidelines provided in the 'card security features' section of this brochure
- Ensuring that staff members who operate the Speedpoint® devices are appropriately trained

If you are an ecommerce merchant, you must protect your web-based business by ensuring that your business processes 3-D Secure transactions.

- No surcharging is allowed i.e. A surcharge is where you penalise a customer for using a credit card and/or debit card for a purchase transaction. The practice of surcharging is thus where you charge customers more for the goods and/or services than you would normally charge customers when they pay for the goods and/or services in cash. The amount charged to all customers must match the displayed or advertised price. The practice of levying surcharges is clearly prohibited by the card scheme rules and industry requirements
- You must be payment card industry data security standards (PCI DSS) compliant. Please refer to the FNB Merchant Services PCI DSS brochure

Types of card fraud

Lost card fraud

Lost card fraud refers to a fraudulent transaction that occurs on a card after a cardholder has lost their card.

Stolen card fraud

Stolen card fraud is when a fraudulent transaction is performed on a card that was stolen from the legitimate owner.

Counterfeit card fraud

This type of fraud mostly arises from a card that is illegally manufactured by stealing information from the magnetic stripe on the back of a card, by way of card skimming. In other cases, lost/stolen/old cards are encoded with information stolen from a card.

Card skimming

Card skimming (to create cloned cards) is a rapidly growing type of card fraud. In terms of this method, magnetic stripe information on a legitimate card is obtained and transferred to a cloned card that could later be used for fraudulent purposes. The legitimate card and the cloned card are electronically indistinguishable.

An example of this type of fraud could include an instance in which a collusive employee accepts a card from an unsuspecting cardholder, processes the correct transaction and performs an additional swipe through a skimmer, which the employee later provides to a fraudster.

The fraudster uses the captured data on the skimmer to create false (cloned) cards. A skimmer can be as small or smaller than a cellphone, making it easy to hide. Business owners must take special care when employing staff and ensure that all potential candidates go through a screening process.

Account used fraud
This usually occurs when a card number is used without the actual card being present, and is more common to ecommerce and mail order telephone order (MOTO) transactions.

Account takeover fraud
This occurs when an existing account is taken over by someone posing as the account holder, who uses the card for their own benefit. This type of fraud can only take place if the fraudster has access to the personal information of the account holder.

Intercepted card fraud
This kind of fraud relates to the interception of cards before they reach the authentic cardholder. After the card has been intercepted it could be used fraudulently.

Refund fraud
There is a new fraud trend where scammers change a purchase into a refund instead of punching in their PIN on the Speedpoint® device.

Only refund on the credit card that was used for the payment. Please note alternative means must be used for refunds on debit cards.

Red flags and precautionary measures

Performing a transaction:
- Do not split the transaction into smaller transactions
- Do not process transactions on your own cards
- Be vigilant and ensure that the cardholder does not tamper with the Speedpoint® device

Card security features:
Always verify the card by comparing the last four digits of the card number With the first four digits printed on the signature pad at the back of the card. If the digits do not match, you should immediately refuse to perform the transaction. You can also compare the card numbers printed on the card, to the card numbers on the Speedpoint® receipt.

If the numbers match, but you still feel suspicious, contact the **FNB Merchant services Help desk on +260762030924** and request a **code 10 authorisation**. As a business owner, it is your responsibility to verify that the person presenting the card is the legitimate cardholder. If you are suspicious, it is recommended that you request the If you are suspicious, it is recommended that you request the customer's identification documents.

Red flags and precautionary measures

Be cautious of the following:
When multiple cards are taken out of a **pocket** instead of a wallet
When a customer tries to **rush or distract** you during the sale
Repeated declines off multiple cards from the same cardholder
When a customer does not ask questions when making a **high value** purchases
When a customer makes **multiple purchases** at your store i**n one day**
When the cardholder tries to give you an authorisation number
When the cardholder **splits the transaction** to make several small purchases on the same card
Embossed card numbers which appear **unusual or are of an uneven type or style**
When the signature on the Speedpoint® receipt **does not match** the signature on the back of the card, you will be held liable
When a **'Hotcard', 'Code 10' or 'Hold and Call'** message appears on your Speedpoint® device screen

If you notice any of these things, do not panic and do not alert the customer. Simply contact the **FNB Merchant service authorisation centre on +26076 203 0924** and say **"I have a code 10 authorisation request".** Then follow the instructions given to you over the phone. However, do not keep the card or make the call if you do not feel safe.

Card security features

VISA card security features:
Check that the VISA card numbers begin with the number 4
Ensure that the VISA hologram on the card appears three dimensional when the card is tilted
Check that the VISA card is still valid and has not expired

Mastercard security features:
Check that the Mastercard numbers begin with the number 5
Lookout for the three dimensional hologram with interlocking globes
Ensure that the last four digits of the account number appear on the signature panel. These digits should be followed by the three-digit card validation code
Check that the card is still valid and has not expired

Fallback transactions

Due to the increase in card skimming and counterfeit cards, the 'Europay, Mastercard, and Visa (EMV) Chip & PIN' card was introduced to deter the number of counterfeit cards used in the industry.

When processing an EMV Chip & PIN card on your Speedpoint® device ensure that you always insert the card, and then follow the prompts.
If a card holder presents a magnetic stripe card for payment, and the Speedpoint® device prompts you to insert the card so it can read the EMV chip, be vigilant as this could possibly be a counterfeit card.

When a card is chip enabled, but the Speedpoint® device is unable to read the chip, it will prompt you to fallback to a magstripe transaction (i.e. the Speedpoint® device will prompt you to swipe the card). This should only be used when you are prompted by the Speedpoint® device. Do not force a fallback transaction and do not attempt to override a declined transaction. Please remember the liability for all fallback transactions lies with the merchant

When prompted by the Speedpoint® device to perform a fallback transaction, ensure that the cardholder signs the merchant receipt and compare the signature to that at the back of the card. Always store merchant receipts in a cool, dark and secure place for the period stipulated in your merchant agreement.

Chip\Contactless fraud

Due to an increase in card swopping instances noted, we have seen an increase in fraud reported on chip cards as well as contactless #JustTap transactions. We therefore urge merchants to be vigilant when processing high value transactions and ensure that all card acceptance procedures are followed as per terms and conditions and card association rules. If you you are unsure of a transaction, please contact merchant services

Help desk.

eCommerce 3-D Secure

Whether large or small, your ecommerce business could be exposed to high levels of fraud related risk. ecommerce transactions are made without the presence of a physical card, making it difficult to detect fraud. This kind of transaction is known as **card not present (CNP).**
It is important to take the necessary steps to prevent fraud in your business. An important step in preventing fraud is to ensure that your business processes 3-D Secure transactions.

Card not present (CNP) in standalone environment
All manual entry requests will go through internal approval processes before the functionality is added to a Speedpoint® device. A merchant remains fully liable for all manual entry transactions as stated in the terms and conditions of the merchant agreement.

Warning signs

To protect your business from fraudulent transactions, look out for the following:

1. **Billing and shipping addresses that do not match** Although it is common for shoppers to have two separate billing and shipping addresses, it is important to double-check any orders that do not have matching billing and shipping addresses.

2. **When customers order multiple quantities of the same item**
Fraudulent orders will often be made with the intention to resell or order different items from the same category. To protect your business, keep track of ordering trends and be aware of high value purchases. Especially when the items are in high demand.

3. **The failure to verify the card verification value(CVV)**
The CVV number is the last 3 digits on the back of the bank card. The failure to verify the CVV should immediately raise a red flag. The CVV verifies that the person placing the order has the physical card in their possession. It is therefore recommended that all merchants request the CVV to be submitted.

4. **Several unsuccessful attempts before the transaction goes through**
When a fraudster is using a stolen card, it is common for the card to decline several times before the transaction goes through. This could be due to an incorrect address, expiration date or mismatched CVV. One or two declines may be common, but multiple declines should be seen as suspicious.

5. **When customers' contact details appear suspicious.**
Fraudsters will often use bogus email addresses, contact numbers, and shipping addresses. Merchants should therefore be on the lookout for suspicious contact numbers and names such as 'Mickey Mouse' and '085 555 555'.

Chargebacks

When a cardholder disputes activity on their account with their issuing bank, the issuing bank raises a chargeback with FNB. You, as the merchant, may be liable for the chargeback
The merchant may then be required to submit the original merchant copy of the Speedpoint® receipt
It is therefore important to keep the original merchant copy of the Speedpoint® receipts in a cool, dark and secure place
Manual entry and non 3-D Secure authenticated ecommerce transactions carry a huge chargeback risk to a merchant's business
The provisions related to chargebacks contained in the FNB Merchant Services general terms and conditions applies to all transactions including QR-code transactions
All valid chargebacks arising from disputed QR-code transactions will be debited from the merchant's nominated bank account.
The merchant accepts liability for all QR transactions processed