how can we help you?

minimise **card fraud** in your business.

FNB
First National Bank

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.

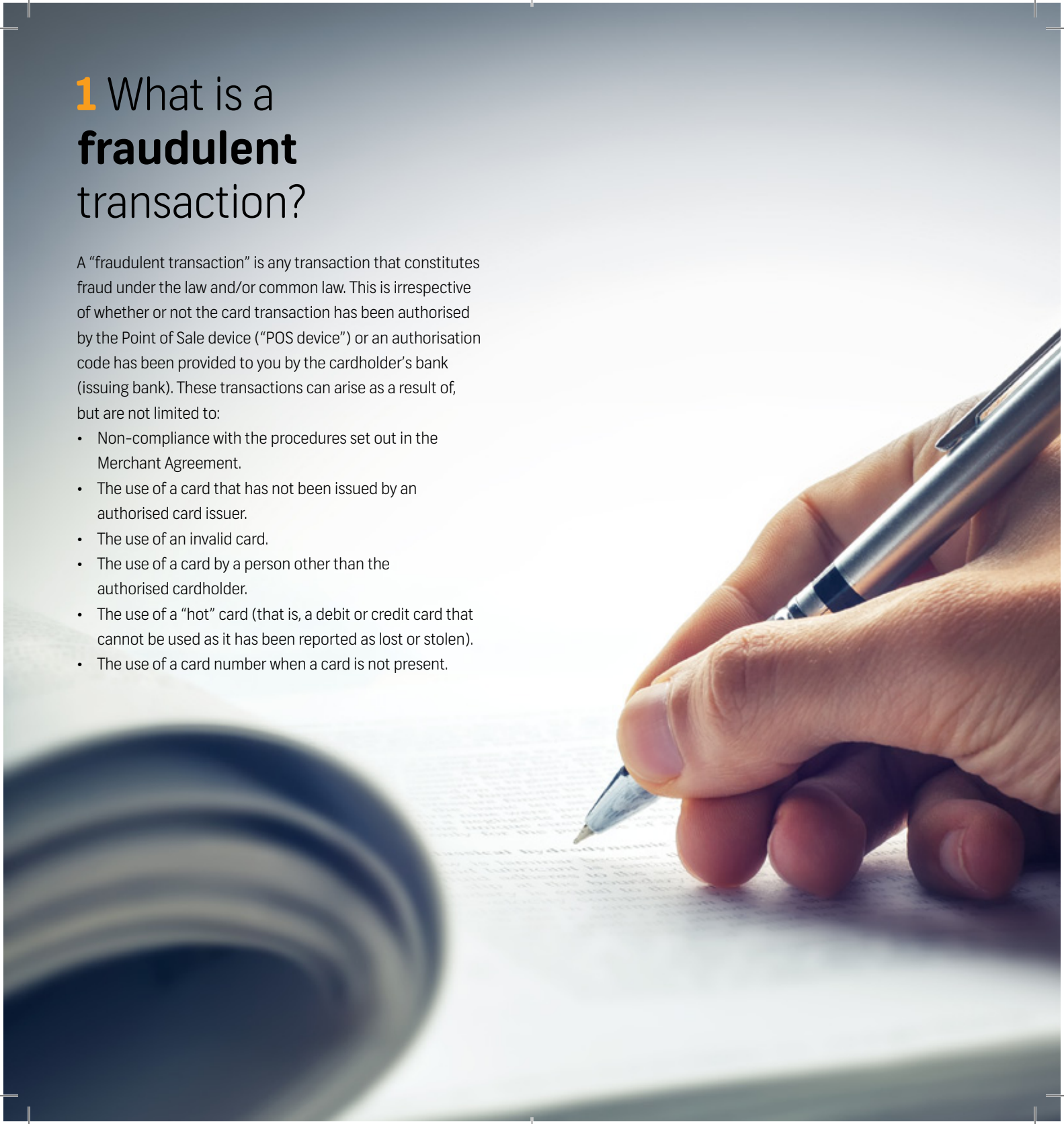
This brochure aims to assist you in detecting, preventing and minimising fraud within your business by providing you with helpful tips and guidelines.

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.fnbtanzania.co.tz**

1 What is a **fraudulent** transaction?

A “fraudulent transaction” is any transaction that constitutes fraud under the law and/or common law. This is irrespective of whether or not the card transaction has been authorised by the Point of Sale device (“POS 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:

- 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 “hot” card (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.



2 What are your **responsibilities** as a Merchant?

- You must ensure that you understand your rights and obligations as 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 to arrange this.
- You must ensure that proactive measures are in place to prevent and mitigate the risk of fraud when accepting card payments. This includes:
  - Validating all cards and verifying the cardholders presenting cards for payment, as per the guidelines provided in section 3 of this brochure.
  - Ensuring that staff members who operate the POS devices are appropriately trained.
- If you are an e-Commerce Merchant, you must protect your web-based business by registering for 3D Secure. Card schemes make use of the following:
  - Visa: Verified by Visa (VbyV).
  - MasterCard: SecureCode.
  - American Express: SafeKey.
- You must be PCI compliant.

What is PCI?

The Payment Card Industry Data Security Standards (PCI DSS) is a mandatory set of comprehensive requirements created by Visa and MasterCard to enhance payment data security. It forms part of industry best practice for any entity that stores, processes and/or transmits card data.

Being PCI compliant will:

- Protect your business from potential security breaches and fraud, and any financial losses that may occur as a result.
- Help you avoid having to pay costly fines, which could be charged to your business in the event of fraud.
- Increase peace of mind for you and your customers.

What do you need to do as a Merchant?

Every year, Merchants will be required to complete the Self Assessment Questionnaire (SAQ), which is compulsory for all types of merchants. Furthermore, integrated and e-Commerce Merchants will also be required to conduct a quarterly Network Vulnerability Scan, which can be done through any approved PCI Scanning Vendor.

3 Accepting card payments

Authorisation

You may only accept valid and current cards. By ensuring that all transactions are authorised in the manner provided for in the Merchant Agreement, you will be assisting in preventing fraudulent transactions.

It is important to note that an authorisation code does not protect you from fraudulent transactions. Obtaining voice authorisation from the cardholder's issuing bank or receiving an authorisation code from FNB are merely confirmations that there are sufficient funds available in the cardholder's account. These do not guarantee the legitimacy of transactions, nor do they imply that the person presenting the card is the legitimate cardholder.

If you suspect any fraudulent behaviour, verify the cardholder by asking for their Identity Document (ID), passport and/or driver's licence, but be aware of falsifications of these documents. Be wary if the same card is used multiple times in one day at your business.

Verifying the cardholder

It is your responsibility as the Merchant to verify that the person presenting the card is the legitimate cardholder.

Performing a transaction

- Do not split a transaction into smaller values in order to avoid authorisation or the floor limit.
- Do not test cards – perpetrators may request that you swipe the card for various reasons without making a purchase first.
- Do not phone for authorisation when the POS device has given a "Decline" response. Only call for authorisation if a "Please call your bank" message is displayed on the POS device.
- Do not process any transactions on your own cards.
- When performing manual or key-entry transactions, you must ensure that you take a clear imprint of the card in the booklet provided by the bank for every transaction.
- Be vigilant while the cardholder is inputting their PIN (Personal Identification Number) and ensure that the cardholder does not tamper with the POS device.
- You may only refund purchases on the card that was presented as means of payment.

NB: You are not allowed to process a refund on debit cards using the POS device. You must process refunds on debit card transactions by refunding the cardholder in cash or by any other means. You may not give cash refunds for credit card transactions; you must process the refund electronically to the same card that was used in the original transaction.

Note: In the event of POS device failure, the device will be unable to go online for authorisation and you will be unable to process transactions on debit and online-only cards.

Note: Manual entry is not a standard feature on our POS devices. This functionality is only available to Merchants who have applied for this facility and meet the required criteria. Activation will only take place once the application for manual entry has been successful, the required documentation and agreements are in place, and training has been provided by FNB Merchant Services.

For more information, call **FNB Merchant Services** on **076 898 9045**

Note: e-Commerce Merchants must ensure that delivery addresses are consistent with orders received. For example, if the cardholder has used a US bank-issued card for delivery of goods in another country, the Merchant must request further assistance from FNB Merchant Services to verify the legitimacy of the transaction.

4 Types of 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. As this type of fraud is most prevalent, it is important to ensure that you understand the card security features as detailed in section 8 of this brochure.

Account used fraud
This usually occurs when a card number is used without the actual card being present, and is more common to e-Commerce and Mail Order Telephone Order (MOTO) transactions.

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

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.

5 Concerning fraud trends

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 as or smaller than a cellphone, making it easy to hide. Business owners must take special care before employing staff and ensure that all potential candidates go through a screening process.

6 **Warning signs and tips** to help you detect fraud

- The card is taken out of a pocket instead of a wallet.
- The cardholder is attempting to purchase an unusual number of expensive items.
- A chip-enabled card cannot be read, in which case you should ask for positive identification before swiping the card.
- Performing any large transactions or swiping any foreign cards, in which case you should positively identify cardholders.
- Several small purchases are being made in order to stay under the floor limit, or you are asked what the floor limit is.
- The sales voucher is signed slowly or awkwardly.
- Expensive items are charged on a new card.
- Identification cannot be provided when asked for.
- The customer tries to distract or rush you during the sale, especially at the end of a work day.
- A large item is purchased and the customer insists on taking it at the time of purchase, even when delivery is included in the price, or a large amount of merchandise is purchased without regard to size, style, colour, quality or price.
- The customer asks no questions on large-value purchases.
- The customer makes purchases and leaves the store, then returns to make more purchases.
- Large purchases are made directly after the store opens, or as the store is closing.

7 What are **chargebacks**?

Chargebacks arise when a legitimate cardholder raises a dispute with their issuing bank.

Chargebacks will be investigated and resolved in accordance with Card Association rules. As part of the chargeback process and investigation, the issuing bank may ask for the original sales voucher. Ensure that all vouchers are kept for six months from the transaction date. Ensure that you only use FNB tally rolls at all times, as using incorrect tally rolls results in illegible copies of vouchers because the information fades on the slip.

In accordance with the terms and conditions of the Merchant Agreement, all Merchants must comply with chargeback rules and regulations and supply the original sales voucher upon request from the acquiring bank. Non-compliance can result in chargebacks and debits to the Merchant, should the chargeback be resolved in favour of the cardholder.

Some common reasons that a transaction may result in a chargeback include, but are not limited to:

- The cardholder did not make or authorise the transaction (frequently an indication of fraud).
- The cardholder cancelled a recurring transaction but this was not effected.
- The goods received are not as described.
- The goods are faulty, defective and/or damaged.
- The goods/services were not received.
- The Merchant's floor limit was exceeded and authorisation was not obtained.
- Transactions were split to avoid authorisation (frequently an indication of fraud with in-store collusion).

- Fraudulent, invalid, erroneous and/or illegal transaction(s) occurred.
- The Merchant made calls for authorisation after the transaction was declined.

How to minimise the risk of chargebacks

- Only process a transaction by swiping the card through the POS device or, if it's a chip card, by inserting the card into the POS device and allowing the cardholder to enter their PIN into the keypad. PIN refers to the unique number only known to the owner of the card, and must not be confused with the authorisation number that is granted by the authorisation centre of a bank.
- Always take a clear imprint of the card in the booklet provided by the bank when processing manual transactions. Imprint refers to the recording of the embossed number of the card onto a carbonised booklet.
  NB: A photocopy of the card is not regarded as an imprint and will not be accepted for chargeback purposes.
  Note: The risk in manual transactions remains with you.
- Ensure that authorisation is obtained for all transactions, whether it is via the POS device or via the authorisations call centre.
- Ask the cardholder to sign the receipt for all swiped transactions. You must compare the signature on the voucher to that on the back of the card to verify the signatures. This will also apply to a chip card that has been swiped due to damage to the chip or the chip reader.
  Note: Swiped chip card transactions are considered high risk and the liability for loss will, in most instances, remain with you.
- Avoid processing a single transaction more than once.
- Reconcile your daily sales vouchers to ensure that the transactions were processed correctly.
- Provide copies of sales vouchers to FNB Merchant Services within the requested timeframe.
- Check completed vouchers daily and be wary of:
  - The same card numbers recurring.
  - The same or similar signatures recurring.
  - The same cashier/attendant involved in the completion of suspicious transactions.
  - Supervisor overrides – these are itemised on your daily banking slip; pay attention to why they were performed.

8 Card security features to prevent fraud

- Compare the first six and last four digits printed on the voucher to the first six and last four digits on the card.
- Ensure that the hologram is three-dimensional and consists of different colours.
- Do not accept an unsigned card.
- Compare the signature on the transaction voucher to the signature on the reverse of the card.
- Below the first four digits of the card number, the same four digits will be printed in smaller print. If they are not, refuse to complete the transaction.

- The chip must be present on the front of a chip card. Some chip cards require a PIN number, while others do not. If no chip is visible but your POS device shows that the card is indeed a chip card, this indicates that the card is counterfeit.
- If the magnetic stripe on a card is faulty, do not proceed with the transaction. Do not use a supervisor card to process the transaction. Rather ask the customer for an alternative payment method.

Visa security features

Check the account number:

- All Visa card numbers begin with the number "4".

Check the hologram:

- The image of the Visa dove should appear three-dimensional and move when the card is tilted.
- The last grouping of embossed digits should extend into the hologram.

Check the signature:

- Valid signature panels are printed with the word "Visa" repeated in colour and at an angle.

The card must be signed:

- If the card is not signed, do not process the transaction.

Check the expiry date:

- The expiry date lists the last date on which the card is valid. Some cards may have a "Valid from" date as well.

MasterCard security features

Check the account number:

- All MasterCard card numbers begin with the number "5".

Check the hologram:

- A hologram with interlocking globes showing the continents should appear three-dimensional and move when the card is tilted.
- The word "MasterCard" will appear in the background of the hologram and the letters "MC" should be micro-engraved around the two rings.

Check the signature:

- The word "MasterCard" should be printed in multi-colours at a 45^{o} angle.
- The last four digits of the 16-digit account number should appear on the signature panel and be followed by the three-digit card validation code (CVC2).

The card must be signed:

- If the card is not signed, do not process the transaction.

Check the expiry date:

- The expiry date lists the last date on which the card is valid. Some cards may have a "Valid from" date as well.

UnionPay security features

Check the account number:

- All UnionPay account numbers are 16-digit permanent account numbers (PAN).

Check the hologram:

- A 3D image of the Temple of Heaven magnifier should appear on the upper-left, and the UnionPay stamp should appear in Chinese on the upper-right.

Check the logo:

- Some debit cards will feature the old UnionPay logo.
- Some debit cards will feature the UnionPay logo on the back of the card.

Check the expiry date:

- The expiry date lists the last date on which the card is valid. Some cards may have a "Valid from" date as well. On some cards, the expiry date is optional.

9 Code 10

If you are suspicious of a cardholder or card at any point during a transaction, you will need to make a Code 10 authorisation request.

What is Code 10?

A Code 10 authorisation request alerts the card issuer to the suspicious activity without alerting the customer. During a Code 10 call, you will speak to the card issuer's special operator, who will provide instructions on any necessary action.

10 What are the Code 10 criteria?

- The card presented appears to be a counterfeit or altered card.
- The purchaser or transaction seems suspicious.
- The signature on the transaction voucher does not match the signature on the back of the card. This does not apply to chip cards, except where the chip on a chip card has been damaged and the card is swiped.
- The card number on the printed voucher differs from the card number on the card.
- The message on the terminal reads "Hold and call" or "Hotcard".

11 Code 10 steps

1. Keep the card in hand to quickly respond to questions.
2. Call **FNB Merchant Services** on **076 898 9045** and say, "I have a Code 10 authorisation request."
   a) The call will first be received by FNB and you will be asked for your Merchant and/or transaction details.
   b) You will then be transferred to the card issuer and immediately connected to a special operator.
   c) A series of yes/no questions will be asked to determine whether you are correct to be suspicious of the card or cardholder.
   d) When connected to the special operator, answer all questions calmly and in a normal tone of voice.
3. Follow all operator instructions.
4. If the operator asks you to retain the card, comply with this request only if it is safe to do so.

12 Consequences of not managing financial risk

(Refer to the Merchant Agreement)

- High levels of fraud may result in termination of the Merchant Agreement and the removal of the POS device.
- Your business may also be listed for excessive fraudulent transactions.
- You may also be listed as a Common Point of Purchase (CPP) by associations for excessive fraud, which will result in all fraud losses and penalties being passed to you.

Contact us

FNB Merchant Services

076 898 9045

www.fnbtanzania.co.tz

fnbtz.mobi

Terms and conditions apply.