Fraud prevention tips

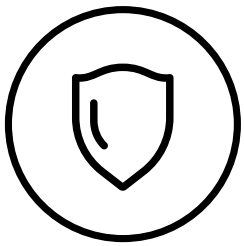
Next

First National Bank
A div of FRB Ltd. An Authorised FSP(NCRCP20).

The holiday season is upon us and with it comes an increase in criminal and fraud activities. It is vital that you remain vigilant over the holiday period.

Please take the time to view the important information in the Merchant Services Fraud Awareness Newsletter.

Fraud prevention tips



Protection of your supervisor/manager PIN

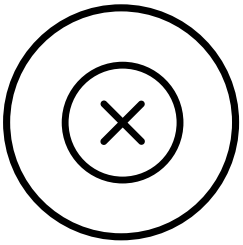
Read more

Chip cards vs fallback

Read more

'Card present' tips

Read more



'Card not present' tips

Read more

Your supervisor/manager PIN is a very valuable tool and needs to be protected. If your PIN gets into the wrong hands, it can expose you to fraud and losses.

Protection of your supervisor/manager PIN

- Choose a strong PIN
- Never write down your PIN
- Never share your PIN with colleagues or communicate your PIN via email or telephone
- Your PIN must be kept confidential
- Do not share a PIN
- Never let someone see you type or enter in your PIN
- Never give out hints about your PIN (for example birthdays, phone number or house number)
- Avoid using the same PIN for various access points
- Change your PIN as often as you can
- If you feel that your PIN has been compromised, change it immediately, and if applicable, report it to your line manager/supervisor

To change your supervisor/manager PIN please refer to the Merchant Services user guide.

Terms and conditions apply

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

Best practices for chip cards versus fallback

- When processing an 'EMV Chip & PIN' card on your FNB Speedpoint® device ensure that you always **insert the card,** and then follow the prompts
- If a cardholder presents a magstripe 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 card holder 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

Terms and conditions apply

‘Card present’ tips

Some tips and tricks to assist you in protecting your business against fraudsters

- 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
- Be cautious of 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**
- Be cautious when a **‘Hotcard’, ‘Code 10’** or **‘Hold and Call’** message appears on your Speedpoint® device screen
- **Do not split** the transaction into smaller transactions
- Do not process transactions on **your own cards**
- Be vigilant and ensure that the card holder **does not tamper** with the Speedpoint® device
- Be careful when a cardholder tries to **rush or distract** you during the sale
- Be vigilant when multiple cards are taken out of a **pocket** instead of a wallet
- Be cautious of **repeated declines off multiple cards** from the same cardholder
- Be vigilant when a card holder does not ask questions when making **high value purchases**
- Be cautious when a card holder makes multiple purchases at your store in **one day**
- Always **follow the prompts** on the Speedpoint® device and do not follow instructions from a cardholder on how to process a transaction
- **Never accept an authorisation number from a card holder**

Terms and conditions apply

Ensure that your business is registered for 3D-Secure and that you process 3D-Secure transactions.

'Card not present' tips

- **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
- **When a card holder orders multiple quantities of the same item**
  Fraudulent orders will often be made with the **intention to resell.** To protect your business, keep track of ordering trends and be aware of high value purchases, especially when the items are in high demand
- **The failure to verify Card Verification Value (CVV)**
  The CVV number is the **last 3 digits on the back of your bank card.** The CVV verifies that the person placing the order has the physical card in their possession. The failure to verify the CVV should immediately raise a red flag. It is therefore recommended that all merchants request the CVV to be submitted
- **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
- **When the customer contact details appear suspicious**
  Fraudsters will often use bogus email addresses, contact numbers and shipping addresses. Merchants must be on the lookout for **suspicious contact numbers and names** such as '**Mickey Mouse'** and **'085 555 555'**

Terms and conditions apply

Please contact **087 575 0012** for any queries

Get the help you need

Explore FNB