Fraud prevention tips from Merchant Services

First National Bank
how can we help you?

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 festive period.

Please take the time to view the important information which we have put together for you in our Merchant Services Fraud Awareness Newsletter.

Protection of your Supervisor / Manager PIN

Continue reading

Chip Cards vs Fallback

Continue reading

Card Present Tips and Tricks

Continue reading

Card Not Present Tips and Tricks

Continue reading

For any queries or to report fraud contact the **Merchant Services National Contact Centre on 059 000 7835**

Fraud prevention tips from Merchant Services

Protection of your Supervisor / Manager PIN | Chip Cards vs Fallback | Card Present Tips and Tricks | Card Not Present Tips and Tricks

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

Best practices for 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 amongst staff.
- 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 accesses.
- Change your PIN as often as you can.
- If you feel that your PIN has been compromised, change it immediately, and if applicable, report this to your line manager / supervisor.

To change your Supervisor / Manager PIN please refer to the Merchant Services User Guide.

Fraud prevention tips from Merchant Services

First National Bank
how can we help you?

Protection of your Supervisor / Manager PIN | Chip Cards vs Fallback | Card Present Tips and Tricks | Card Not Present Tips and Tricks

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

When processing an 'EMV Chip and PIN' card on your 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 **fall back 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 fall back transaction and do not attempt to override a declined transaction.
Please remember the liability for all fall back transactions lies with the merchant .

When prompted by the Speedpoint® device to perform a fall back 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.

Fraud prevention tips from Merchant Services

First National Bank
how can we help you?

Protection of your Supervisor / Manager PIN | Chip Cards vs Fallback | Card Present Tips and Tricks | Card Not Present Tips and Tricks

Card Present Tips and Tricks:

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.**
- Please remember 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 cardholder **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 cardholder does not ask questions when making **high value purchases.**
- Be cautious when a cardholder 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 cardholder.**

Fraud prevention tips from Merchant Services

First National Bank
how can we help you?

Protection of your Supervisor / Manager PIN | Chip Cards vs Fallback | Card Present Tips and Tricks | **Card Not Present Tips and Tricks**

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

Be cautious of 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 a cardholder 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.

3. **The failure to verify Card Verification Value (CVV).**
   The CVV number is the **last 3 digits on the back of your 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 **0242 435 050 / 050 158 0838.**