Protect your business from card fraud

Merchant Solutions

Standard Bank Moving Forward™

Fraudsters use a variety of methods to trick unsuspecting merchants. It is crucial that you understand how fraud can impact your business and that you know what steps you can take to minimise the risk of fraud losses mainly.

TYPES OF FRAUD

Lost cards

Fraudulent transactions made with real cards after cardholders have lost their cards.

Stolen cards

Fraudulent transactions made with real cards that were stolen from the actual cardholder.

Cloned cards

Card skimming is the cloning of a card to make fraudulent transactions. Fraudsters somehow get a hold of the magnetic stripe information on a legitimate card and transfer it onto a manufactured card which then becomes a counterfeit of the cloned card. The counterfeit card may look very similar to a real card. Fraudsters then use the counterfeit card to make fraudulent transactions.

A hand held skimming device may be used by an employee for skimming customers' cards. It is as small as a cellphone and can easily be hidden under clothing.

Make sure you can trust the people you employ and check that their references are genuine.

CHECKLIST TO PREVENT FRAUD

1. Card-present merchants

a) Check the card security features

Chip cards

- The first four embossed digits on the front of the card must be the same as the number below the embossed digits printed in smaller font size.
- Compare the visible card numbers on the face of the card against the card number on the electronic slip. These must match.
- Chip cards must be placed into the chip slot on the point-of-sale (POS) terminal. Never swipe or force a chip card.
- Look out when a POS terminal identifies a card as a chip card if the card presented to you does not have a chip. The card might be cloned. Do not complete the transaction.
- Look out for strange card numbers with different fonts and styles.
- If the card number on the front of the card and the number on the payment slip do not match, do not release the goods if it is safe to do so.

Maestro/Electron magstripe debit cards

- Debit cards transactions require a PIN to validate the card transaction.
- If the POS terminal does not ask for a PIN, don't do the transaction.
- Do not release the good, if it is safe to do so, in instances where the card number on the front of the card and the number on the payment slip do not match.
- When processing magstripe cards, a PIN is always required except for garage cards at forecourts (they don't require a PIN as validation is done via signature).

b) PIN protection

- A PIN is an added security feature to chip and debit cards.
- To complete transactions with chip and debit cards, a PIN must be entered into the POS terminal.
- Look out for suspicious individuals watching your customers closely as they enter in their PIN – they want to get hold of the customer's PIN.
- Advise your customers to block the PIN pad when they enter their PIN.

2. E-Commerce Merchants

- It is vital that each transaction is fully authenticated by the cardholder and their bank.
- You can only do card-not-present (CNP) transactions if you agreed to and signed a merchant agreement that allows such transactions.
- eCommerce Merchants must make sure that they are registered for 3D secure.
- Monitor revenue (volumes and values) to identify unexpected and abnormal transactional behaviour.
- Monitor unusual transactions – if the same card is used many times and it's declined more than once, it might be cloned.

3. MOTO

MOTO transactions are not authenticated by the Card Holder and are therefore very risky.

- You can only do card-not-present (CNP) transactions if you agreed to and signed a merchant agreement that allows such transactions.
- Monitor revenue (volumes and values) to identify unexpected and abnormal transactional behaviour.
- Monitor unusual transactions – if the same card is used many times and it's declined more than once, it might be cloned.
- MOTO transactions are done at your own risk and the bank will not be liable for any disputes arising from a MOTO transaction.

CHARGEBACKS

A chargeback is the term used when a customer disputes a transaction due to fraud or any other reason which results in the merchant's account being debited for a particular transaction or transactions.

Chargebacks occur due to various reasons such as processing errors, authorisation issues, the non-fulfilment of copy requests and in cases of fraud.

What chargebacks mean to you

If a chargeback is initiated against your merchant account, you may lose both the rand value of the transaction being charged back and the related goods and/or services. You will also incur your own internal handling costs to process a chargeback.

Chargebacks are time-consuming and inconvenient, often involving checking receipts and liaising with the relevant banks to resolve disputes – time you could have spent on generating additional sales and revenue.

The bank cannot be used as an arbitrator between cardholder and merchant. The merchant has the right to pursue legal or civil cases if they feel that the chargeback is unfair.

How to avoid chargebacks

Many chargebacks happen because of mistakes and omissions you could have easily avoided. So, if you have proper procedures in place, the less likely you'll do something that might lead to a chargeback.

If you adhere to the rules and regulations of your Merchant Agreement, and follow these simple tips, you can protect yourself and your business against chargebacks:

- Avoid risky transactions that are more likely to attract chargebacks, for example manual transactions, voice authorisations and swiping chip cards. Rather ask for an alternative card or payment method. If you have no choice but to do a manual transaction:
  - get a card imprint if you use a zip-zap machine, and
  - make sure that you capture all the details correctly on the slip if you use imprint vouchers
  - Avoid merchant initiated transactions and encourage cardholder initiated transactions.

Please ensure that all transactions are authenticated by the Card Holder. This will minimise the chances of a chargeback being raised against you.

In the event of processing a manual transaction, the imprint of the card or the imprint voucher is your proof that the card was indeed present during the transaction. A scan, fax or photocopy is not seen as proof that the card was present. Please note that you will no longer be able to use a "card imprint" to defend a chargeback for manual key transactions. Processing these transactions are high risk and you will need to complete an indemnity form should we approve the manual key option on your device.

- If your point-of-sale device asks you for an authorisation code, you must phone the authorisation centre personally – do not accept an authorisation code from a cardholder or allow a customer to phone on your behalf.
- Don't complete a transaction if the authorisation request is declined. Do not repeat the authorisation request after receiving the decline – rather ask for another form of payment.
- Don't use your own credit card to process refunds and don't buy anything with your own credit card at your store.
- Make copies of the sales vouchers within the retrieval request timeframes. Don't delay – return copies of sales vouchers promptly.
- Keep legible copies of sales vouchers, including copies of imprints. If these vouchers are not legible, there might be a chargeback.
- Keep all sales vouchers in a safe place for a minimum period of six months, as cardholders have a right to dispute transactions within six months of the date of the transaction.
- If your business has any policies about merchandise returns, refunds or service cancellations, you must disclose it to the customer at the time of the transaction, and it should also be visible on your sales receipts or invoices.
- If a customer is expecting a delivery and it gets delayed, let them know in writing about the delay and when the expected delivery date will be. DO NOT offer them another item unless the customer agrees to accept it. Make sure you keep invoices that show proof of delivery.
- If a customer cancels a transaction that is billed periodically (weekly, monthly, quarterly, or annually) cancel the transaction immediately or according to the customer's request.
- Log onto Merchant Online daily to validate that all your transactions have been reconciled correctly on your statements.
- If you are an eCommerce merchant:
  - Get written proof of consent from the cardholder for the billing to take place for the specific goods or services – and keep written proof that ties back to the cardholder together with the terms of billing.
  - Ensure that the transactions are fully authenticated (3D secure).

How to validate identity documents

Another way to prevent chargebacks resulting from fraud is to validate your customers' identity. When checking identity documents, look at the date of birth, the first six digits of the identity number and the photo to see if they match the appearance of the cardholder.

Check that the photo has not been tampered with and that it is positioned correctly within the block.

Make sure that the names on the identity document have not been changed, that it's in the same font as the rest of the page and in a straight line and that it has no initials.

We recommended that you ask for an identity document when:

- the customer is using a card that was not issued by a South African bank
- you have to process a manual transaction
- you are suspicious about a transaction
- you process large transaction values, for example jewellery, travel or accommodation transactions.

When to call for a 'Code 10' authorisation

If you're in any way suspicious about a card, the person who presents the card to you or the circumstances surrounding a transaction, call for a Code 10 authorisation. Do this when:

- you believe a fraudulent or altered card is presented to you
- the person who presents the card to you is suspicious
- the entire transaction is suspicious
- signatures do not match and you are feeling uneasy about the transaction or cardholder
- the account number of the printed sales voucher differs from the number on the card
- customers don't have alternative cards to pay with and insist on buying goods with their credit cards only.