

Fraud Prevention

Criminals are constantly attempting to profit from stolen/counterfeit credit and debit cards and merchants are urged to be alert and aware, and to always follow the correct card acceptance procedures. Similarly, it is important that you ensure that all your staff members, including temporary staff, are regularly updated and trained on and adhere to the guidelines provided. Your supervisors and managers must be fully aware of these guidelines.

The guidelines here will help to recognise when your business may be at risk of fraud. Should there be a suspicion of any transaction, please contact the relevant Authorisation helpdesk and request a code 10. By taking some simple measures, merchants can protect themselves from avoidable losses.

General card acceptance procedures – Card present

- For magstripe transactions the card should be swiped and for smart card transactions the card should be inserted into the chip reader. This will ensure that information is properly recorded.
- All above the floor limit transactions/budget/fallback transactions (smart cards) will automatically result in your device dialing up for an authorisation.
- Please contact the relevant Authorisation helpdesk if you experience any of the following:
 - The NedLink device is unable to read the magstripe on the card.
 - The transaction is below the floor limit but you are suspicious of the cardholder or the card.
 - Your NedLink device prompts you to call for authorisation, PLEASE CALL.
 - If the cardholder presents an authorisation number that he or she obtained from his or her issuing bank, in no circumstances should the number be accepted.
 - The transaction receipt cannot be printed even though the card is present.
- Request positive photo identification (ID document or passport) from cardholders with international cards and write down the identification number on the merchant copy of the sales receipt.
- No one except the cardholder can sign for the transaction. Hence, never accept or process a transaction where an individual is using someone else's card.
- With smart cards and chip technology, if the chip on the card is damaged or the NedLink device is malfunctioning, the transaction will fallback to magstripe. In these instances, a merchant password or supervisor card and PIN may be required. All fallback transactions will go online to the Issuing bank for authorisation.

Manual transactions

No manual entry is allowed unless you have obtained prior written consent from Nedbank. However, in the case of a damaged card, where the transaction is processed on the manual 'zip-zap' imprinter, it is vitally important that an imprint of the card be taken by using Nedbank supplied equipment and stationary. The CVV/CVC number (last three digits on the back of the card) must also be recorded on the voucher. This CVV/CVC number must be printed next to the card number that is imprinted on the voucher. The recording of the CVV/CVC number and the imprint of the card will prove that the card was present at the time of the sale.

General card acceptance procedures – card not present

- Merchants should insist, where possible, on physically seeing the card and taking a 'zip-zap' imprint of it before delivering any goods. The CVV/CVC number (last three digits on the back of the card) must also be recorded on the voucher. This CVV/CVC number must be printed next to the card number that is imprinted on the voucher. The recording of the CVV/CVC number and the imprint of the card will prove that the card was present at the time of the sale.
- All internet transactions have a zero floor limit and must receive authorisation prior to processing.
- A debit card using a PIN cannot be used for telephone, fax or internet transactions.
- If a transaction is mistakenly processed, immediately process a refund (credit card) or a reversal (debit card).
- Merchant's trading name must appear on the customer's card statement and must be recognisable to the cardholder.

Note: If the details of the cardholder were sent via telephone, fax or internet, the merchant will be responsible for any chargeback that occurs.