

High-risk transactions could be identified by ...

- a cardholder insisting on paying for a transaction without having his/her card present;
- telephone/fax orders;
- high ticket values near closing time;
- cardholders being unusually charming, when they do not have to be; and
- the association logo not matching the first digit of the card number; 3 – American Express, 4 – Visa and 5 – Master Card.

If you pick up on any of the above, call our Authorisations Centre on 0860 321 222 and mention that the call is a 'code 10'.

Did you know?

Nedbank will pay a reward of R1 000 when you impound a 'hot card' or when requested to do so by the Authorisations Centre. More is paid for an arrest. Call our Fraud Department on 011 667 8816 or send an email to fraudrewards@nedbank.co.za.



Following the correct processing guidelines will reduce chargebacks and fraud.



Call our Merchant Helpdesk on 0860 114 966 for more information.



Sign up for eStatements and help protect the environment.



Call the Nedbank Merchant Helpdesk on 0860 114 966 or visit www.nedlink.co.za.

Nedbank Ltd Reg No 1951/000009/06, 135 Rivonia Road, Sandown, Sandton, 2196, South Africa. We subscribe to the Code of Banking Practice of The Banking Association South Africa and, for unresolved disputes, support resolution through the Ombudsman for Banking Services. We are an authorised financial services provider. We are a registered credit provider in terms of the National Credit Act (NCR Reg No NCRCP16).

Combat card fraud and reduce chargebacks



MAKE THINGS HAPPEN

NEDBANK

A Member of the OLD MUTUAL Group

Most common chargeback reasons and codes with explanations

| Code | Chargeback description | Explanation |
|------|---|--|
| 41 | Cancelled recurring transaction | You continued to debit a cardholder for recurring transaction despite cancellation notification. |
| 72 | Transaction exceeds floor limit | You did not obtain authorisation for a transaction exceeding the floor limit. |
| 77 | Non-matching account number | A transaction for an account number does not match any of the issuer's master files. |
| 79 | Non-receipt of copy request | An issuer did not receive a requested voucher within the specified time limit, ie 14 days. |
| 81 | Missing imprint without the cardholder's permission. | You did not obtain an imprint (manually or electronically) and processed the transaction. |
| 82 | Duplicate processing | A single transaction was processed more than once. Interchange logs reflect both transactions. Where two acquirers have processed the same transactions the chargeback is to be sent to the acquirer who processed second. |
| 83 | Non-possession of card | The card was not present and a hand-written transaction was processed without the cardholder's permission or a fictitious account number was used. |
| 85 | Non-receipt of credit voucher | You issued a credit voucher that was not processed. |
| 90 | Goods/Services not received, including cash dispensed at an ATM | Goods not received. Acquirer is notified via a letter from the cardholder. |
| 57 | Fraudulent multiple transactions | Multiple transactions at the same merchant without the cardholder's permission. |
| 60 | Requested copy/illegible | You did not provide a legible copy of the voucher. |
| 70 | Card recovery bulleting | A transaction is accepted at a POS/terminal 48 hours after receiving notification to add the account number to the hot-card file. |

| Code | Chargeback description | Explanation |
|------|----------------------------------|---|
| 71 | Declined authorisation /response | You completed a transaction after an authorisation request was declined. |
| 73 | Expired card | You completed a transaction with a card that had expired prior to the transaction date and did not receive an authorisation. |
| 74 | Late presentation of paper | An acquirer did not process a transaction within the required time limit, ie the transaction date is more than 30/180 days prior to the processing date. |
| 80 | Processing error | An acquirer processed a transaction using an incorrect card number, transaction code or amount. a Incorrect account number, ie mispost. b Incorrect transaction code, ie credit voucher processed as debit. c An addition or transposition error was made when calculating the transaction amount. |
| 84 | Missing signature | You did not obtain a cardholder's signature and the transaction was completed without the cardholder's permission. |
| 86 | Alteration of amount | A transaction amount was altered without the cardholder's permission. |
| 88 | Split sale | You processed two or more transactions that in total exceed the floor limit to avoid a single authorisation of the combined total amounts. |
| 62 | Counterfeit card | You processed a chip card by bypassing the chip via magnetic-stripe overriding 'CHIP & PIN' requirements. |

Card fraud

Card fraud is on the increase both locally and internationally, resulting in an increase in chargebacks. This brochure is intended to assist you in processing transactions correctly, as well as providing you with fraud prevention tips to help reduce your chargebacks and minimise your financial losses.

'CHIP & PIN' card transactions

How to process a 'CHIP & PIN' card transaction correctly



Step 1: Insert the card (chip first) into the chip reader. The card must remain in the chip reader for the full duration of the transaction.

Step 2: If the card supports multiple applications, eg CREDIT, CHEQUE or SAVINGS, ask the cardholder to advise which application is applicable when prompted by the POS device.

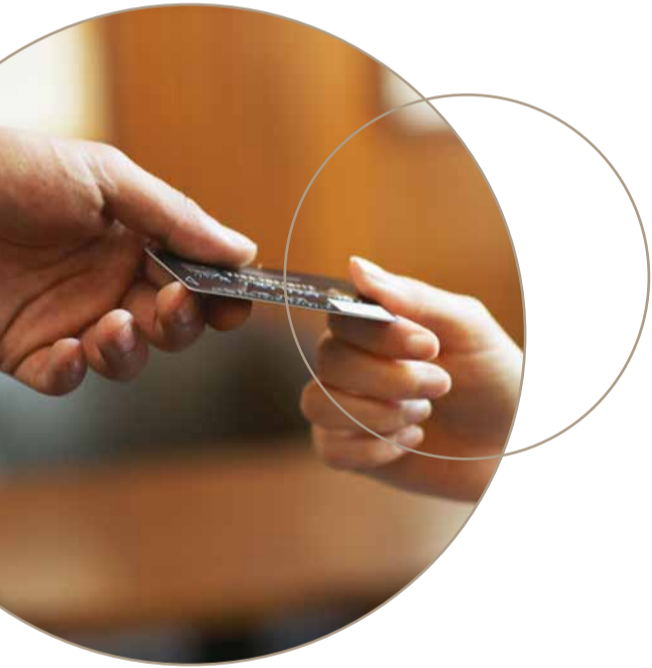
Step 3: Select the type of transaction, eg SALE, and enter the total amount due.

Step 4: Ask the cardholder to enter his/her PIN. No customer signature is necessary if the PIN is entered successfully.*

Step 5: Your POS device will authorise the transaction and issue a merchant and cardholder POS slip.

Step 6: Remove and return the card and receipt to the cardholder.

* A transaction authorised by the cardholder entering the correct PIN is the most secure.



Detect and refuse cloned cards and reduce chargebacks

First four digits of the card number

- Below the **FIRST** four digits of the embossed **CARD NUMBER** a laser-printed number should be printed on the face of the card, in much smaller black print.
- Check that these four digits are the same.
- If not, refuse to do the transaction.

Compare visible card numbers

- Compare the visible **CARD NUMBER** on the **CARD FRONT** to the **CARD NUMBER** on the POS slip.
- When you are too busy, check the **LAST FOUR DIGITS** of these **CARD NUMBERS**.
- These must always **MATCH**.

CHIP cards – damaged CHIP on card

- CHIP cards are intended to prevent fraud.
- CHIP cards must be dipped **INTO** your **POS CHIP SLOT** to ensure transaction data is captured on the CHIP.
- Never **SWIPE**, or **FORCE**, a chip card through a **POS** device to access a magnetic-stripe transaction.
- When a CHIP is damaged, **AVOID HIGH RISK – HIGH VALUE, SWIPED** magnetic-stripe transactions. The CHIP may have been damaged with the intent to defraud.
- Avoid **MANUAL ZIP-ZAP**-imprinted transactions with embossed chip cards. (Be suspicious when a CHIP transaction is unsuccessful; when in doubt, request a code 10 authorisation.)

Manual transactions

How to process a manual credit card transaction correctly

PS Debit cards cannot be processed manually.

Step 1: Ensure you have a zip-zap machine imprinted with your merchant identity plate and stock of bank-issued manual vouchers.

Step 2: Obtain an authorisation code from the Nedbank Authorisations Centre on **0860 321 222**.

Step 3: Ensure that the following details are recorded on the Nedbank-issued manual voucher:

- Authorisation number.
- Date of transaction.
- Rand value of transaction.
- A clear imprint of the detail from the embossed credit card.
- Your merchant details.
- The CVV/CVC number (last three numbers on the reverse of the card). Please note that the CVV/CVC number should be recorded below the printed card number and that the words 'CVV' and 'CVC' are not to be used on the voucher.
- Cardholder's signature.

Step 4: Attach the POS slip to the Nedbank-issued manual voucher and, using the details on the voucher, ensure that the manual transaction is entered into your POS device.

Step 5: Retain the voucher for a period of at least three years from the date of the transaction and in such a manner as to ensure the voucher retains its clarity.

TIP: Be extra vigilant when processing manual transactions since the majority of fraud is perpetrated on manual transactions.



Call our Merchant Helpdesk on **0860 114 966** for more information.

Cloned CHIP cards – no CHIP on the card

- If **NO CHIP** can be seen, yet your **POS** device shows that the card is a **CHIP** card, this indicates the card is a **CLONED CHIP** card. This means that the magnetic stripe on the card was cloned and contains data from an original genuine CHIP card.
- When this card is **DIPPED** into your terminal, the terminal cannot complete the transaction.
- **DO NOT** proceed with a **FORCED** magnetic-stripe transaction.
- Never use your **OVERRIDE** facility to force a magnetic-stripe transaction.

Card number embossed and raised, or laser-printed on card face appears unusual or is of uneven type or style.

- This is suspicious and may indicate that the card is a **COUNTERFEIT**.
- Refuse to do the transaction and call your Authorisation Centre for instructions.

Debit cards

- **DEBIT** card transactions are **PIN**-authenticated.
- When a clearly styled **VISA** or **MASTERCARD** debit card does not require a **PIN**, this is suspicious.
- This may indicate that the card is a **CLONED** card with a credit card number and not a debit card number captured on the magnetic stripe.
- Refuse to do a transaction if the POS device does not require a **PIN**.
- Refuse to do a transaction if the card numbers on the card face and the electronic slip are not the same.

PIN protection

- A **PIN** is an added security feature of **CHIP** and **DEBIT** cards.
- To complete transactions with **CHIP** and **DEBIT** cards the **PIN** must be entered into the **POS** device.
- Be aware of observers who attempt to see a cardholder entering the **PIN**.
- Advise the customer to block the **PIN** pad when the **PIN** is entered into the **POS** device.



Tips on fraud prevention

An authorisation:

- does not verify that the person presenting the card is the cardholder; and
- code indicates that the account used is in good standing and has sufficient credit available, but is not a guarantee of payment.

TIP: Request positive identification when accepting cards as a method of payment, especially with manual card transactions.

How to avoid common chargebacks:

- Ensure that the card is always present.
- Obtain a clear imprint of the card.
- Prepare a zip-zap voucher for every manual transaction as proof that the card was present.

TIP: Rubbing of the merchant POS receipt on the credit card is not accepted as proof of the card being present.

- Always get an authorisation when processing a manual transaction.
- Ensure the cardholder signs the voucher and compare the signature to the signature on the card.

CARD NOT PRESENT (CNP) transactions

- **CNP** transactions are only allowed when your merchant agreement provides for this.
- When your agreement does not allow **CNP** transactions, this may result in the **LOSS** of the transaction amount to your business.
- For **CNP** transactions additional security measures from MasterCard Secure, or Visa – Verified by Visa, are available to **HELP** protect customers and merchants against **CNP** fraud.
- Customers feel more secure and are more likely to purchase from protected businesses.
- When your merchant agreement does not allow **CNP** transactions, this means that the cardholder must be present when the transaction is made.

Financial-risk transactions (refer to merchant agreement)

- High levels of fraud may result in the termination of the merchant agreement and the retraction of card POS terminals.
- Take care to monitor revenue (volume and value) to identify unexpected and abnormal transactional behaviour.
- Abnormal transactions may indicate fraud.
- Report suspicious transactional behaviour to your bank to investigate.

Card skimming

- Card skimming to create **CLONED** cards is a rapidly growing type of card fraud.
- Skimming is a method by which magnetic-stripe information on a legitimate credit card is obtained and transferred to a **CLONED** card, which is later used fraudulently.
- The legitimate card and the **CLONED** card copy are electronically indistinguishable.
- Typically a collusive employee accepts a card from a non-suspecting cardholder, processes the correct transaction but also performs an additional swipe through a skimmer, which the employee later hands over to a fraudster. The fraudster uses the captured data on the skimmer to create false **CLONED** cards.
- A skimmer can be as small as a cellphone or smaller and could therefore be easily hidden under a jacket.

TIP: Business owners are requested to take special care before employing staff who have not been carefully screened and whose references do not come from known and trusted sources.

Stick this on your wall for easy reference.