

Before returning the card to the customer, make sure the bank has approved the sale.

For credit card transactions, always ensure the signature on the receipt matches the one on the card.

Be alert for customers who:

- appear anxious
- arrive on closing time
- have no identification
- appear in a hurry
- purchase large quantities of goods or expensive items
- request transactions to be entered manually

If you suspect the card has been altered, or have any doubts about the person presenting it:

- keep the card
- check the warning bulletin to see if the number is listed
- ask for additional identification
- call your supervisor
- contact the card authorisation centre to verify information.



Authorising Credit Transactions

Contact the Card Authorisation Centre to obtain authorisation for credit card transactions when

- the value of the transaction exceeds your floor limit
- conducting a manual or off-line transaction

EFTPOS and Debit Card Fraud

You can take steps to safeguard against EFTPOS fraud by making sure you:

- set at an appropriate limit for refund or cashback for each EFTPOS terminal
- change regularly and keep confidential the EFTPOS password or PIN
- maintain physical security of EFTPOS terminals

Did you know...

...if you fail to seek authorisation for transactions when necessary, you may be held liable for the full amount!

For further information please contact:

Major Fraud Investigation Group
Queensland Police Service
200 Roma Street, Brisbane, Qld 4000

Phone: (07) 3364 6622
Facsimile: (07) 3364 6549
Website: www.police.qld.gov.au

Crime Stoppers 1800 333 000

Crime Stoppers TTY 1800 333 000

Emergency only 000

Cartoons by Rob Wann

Produced with the assistance of the Media & Public Relations Branch
Reproduced from information supplied by the NSW Police Service

Queensland Police Service Vision Statement

We are determined to be a professional police service, dedicated to excellence and committed to working in partnership with the people of Queensland to enhance the safety and security of our community.



'Foiling the fraudsters'

Your guide to stopping

Credit card & EFTPOS fraud

What's Fraud?

Fraud is behaviour that's deceptive, dishonest, corrupt or unethical.

For a fraud to exist there needs to be an offender, a victim and an absence of control or safeguards.

Here in Queensland, the laws on fraud involve dishonesty in any of these situations:

- obtaining property belonging to someone else
- applying someone else's property to one's own use
- causing a detriment to another person or entity
- gaining a benefit or advantage for any person; and
- inducing or causing any person to deliver property to another person

Fraudulent activity in the workplace often results in the loss of revenue and property, while increasing operational costs and service charges. It can also mean obligations to employees, customers, suppliers or contractors can't be met.

The knock-on effect for businesses may:

- damage credibility
- compromise confidentiality
- result in public criticism

Common frauds include using false

- identities
- cheques
- credit and EFTPOS cards

Fraud Risks and Prevention Measures

With the rapid advancements in technology, frauds are becoming more sophisticated, widespread and complex. As a result, stamping out fraudulent practices becomes a huge challenge and requires extra vigilance on the part of businesses and individuals

Credit Cards and EFTPOS

As we evolve into a cashless society with more and more businesses and individuals using credit cards and electronic banking, the likelihood of becoming a victim of fraud increases.

Criminals have embraced modern technology to pursue their dishonest activities. Methods used include credit card skimming, false and stolen identities and taking advantage of ineffective security systems to obtain Internet banking passwords and account particulars.

Why does it happen?

The main risks with credit and debit cards involve

Theft

Cards may be intercepted in the post, sent or delivered to the wrong address

Counterfeit cards

False identities may be used to produce counterfeit cards

Fraudulent transactions

Stolen cards may be used to purchase goods or obtain cash advances or stolen credit card details may be used for telephone orders.

What can you do?

To avoid becoming a victim of credit and debit card fraud, you can:

- arrange to personally collect new or replacement cards from your financial institution
- ensure you keep your credit card and debit card secure
- never keep your PIN number with your card
- when using an ATM, be aware of anyone standing close by or watching over you

- take steps to conceal the keypad when you enter your PIN
- when paying for goods or services at a point of sale, don't allow your debit or credit card out of your sight

When accepting payment by card, always check the following details:

- **Account Number** - the embossing should be clear and uniform in size and spacing and match the number on the back of the card. The last 4 digits of the embossed number on the front of the card should be the same as the reverse indent italic number on the signature panel on the back of the card. This number is also printed on the sales receipt or displayed on the terminal. **Printed Number** – a 4 digit number may be pre-printed on the card and must match the first 4 digits of the embossed account number.
- **Valid Date** - all cards have a "Valid To" date, and some cards also have a "Valid From" date. Make sure the card is current.

Mastercard, Bankcard and Visa

- **Security Character** – Mastercard has "MC" embossed on the card, Visa has a "V" and Bankcard has a "B"
- **Hologram** – they all include holograms that should appear three dimensional and move when the card is tilted
- **Signature Panel** – the words Mastercard, Visa or Bankcard should be printed at a 45 degree angle on a tamper-proof signature panel.
- **Validation Code** - There should also be a three digit card validation code printed on the panel after the last 4 digits of the card number.

Businesses

It's just common sense!

When accepting payment by credit or debit card, always check for any visible signs of damage to the card.