

# Neighbourhood Support New Zealand



Phone 0800 4NEIGHBOURS  
Phone 0800 463 444  
[www.ns.org.nz](http://www.ns.org.nz)

## Neighbourhood Support Fact Sheet

### Credit and Eftpos card fraud

The theft of credit and Eftpos (ATM) cards is a common crime in New Zealand. So, too, is the associated fraud.

While Police work closely with banks and retailers to prevent this type of fraud, there are a number of simple things you can do to assist.

Credit and Eftpos card account and Personal Identification Numbers (PINs) must be guarded carefully. They are the lock, and key, to your personal finances.

- Keep your own credit or Eftpos card safe. If it is stolen or goes missing, inform your credit card company or bank and cancel it immediately.
- Don't have an easily guessed PIN e.g. your birth date; the first set of numbers on the card itself; or sequential numbers such as 1234.
- Try and memorise your PIN, if you can't then never keep your PIN and card in the same place.
- Use different PINs for different cards.
- In no circumstances reveal your PIN number to anyone. There is no legitimate reason why anyone requires your PIN. Even during an investigation by bank staff or Police your PIN is not required.
- Always keep your PIN number well hidden when entering it - whether at a money machine, in a shop or other busy place.
- Keep an eye out for 'shoulder surfers' - people who watch you enter your PIN, then look for an opportunity to steal your card - especially in crowded places.
- Never let your credit card out of your sight - even in a restaurant. Fraudsters are often the most charming people and frequently seek work with high public contact.
- Ensure you get your card back after every transaction.
- Destroy expired cards and sign new cards immediately.
- Match credit card statements with your receipts.
- Keep a record of the card account number, expiry date and any numbers to call if your card is lost or stolen.
- Tell your bank or credit card company if you change your address, so replacement cards are sent to the correct place.
- Be on the look out for "skimming" devices that can read and store the encoded information on the magnetic strip of your card. These small devices have been found attached to money machines and in venues where credit cards are frequently used.

If receiving payment by credit card, it's good practice to do the following:

- Check if the card has been tampered with or altered in any way, particularly the signature panel.
- Check the expiry date on the front of the card.
- Check the account number on the front of the card matches the back.
- Compare the signature on the card and the sales slip.
- Check the 'hot card' list for every credit card sale.
- Obtain a telephone authorisation for sales exceeding the floor limit or if you are suspicious of the person's identity or behaviour.
- Ask for photo identification, such as a driver's licence.

Be wary of a customer who:

- is nervous, trying to hurry things up or buys a wide range of expensive items on a newly valid card;
- looks at the card before signing the transaction slip or signs awkwardly or slowly;
- has a large number of cards in their pocket and attempts to use several before one is 'approved';
- purchases an unusual amount of expensive items indiscriminately. A fraudster with a stolen credit card may not carry out the normal pre-purchase activities a legitimate buyer makes when purchasing expensive items e.g. product comparisons, warranty questions, technical questions or queries on cash discounts ...;
- makes random purchases with little regard to size and quantity;
- purchases large items and insists on taking them immediately;
- buys a large number of a single item;
- watches closely during authorisation request;
- can't provide photo identification when requested;

Internet or phone transactions:

- Know who you're dealing with online. Check the website you order from has a physical address, phone and fax number. Make a note of all details, including the company's name and Internet address, amounts to be charged, shipping costs, and the time and date you placed the order.
- Only make telephone transactions when you have instigated the call and are familiar with the company.

**REMEMBER:** if you haven't done everything you can to protect your credit card or PIN, you may have to pay for illegal purchases made on your card.

Your credit card provider or merchant can offer further detail on minimising mail, telephone and Internet card fraud.