

# Neighbourhood Support New Zealand



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

## Neighbourhood Support Fact Sheet

### Identity theft

Identity theft has become an increasingly common and widespread crime overseas. It is also on the rise in New Zealand.

Identity theft occurs when a criminal uses another person's personal information to take on that person's identity. This mainly involves stealing personal details to commit theft or fraud.

Theft of your personal information takes many forms, from stealing your wallet to intercepting your mail.

Once the thief has successfully assumed your identity there are many things they can do with it, from buying and using a mobile phone to writing cheques and opening a credit card account in your name.

Identity theft can ruin your good name and credit rating, which can be very time-consuming and expensive to rectify.

The following items can be used to obtain and assume someone else's identity:

- Credit card
- Drivers Licence
- Firearms Licence
- Birth Certificate
- Passport
- Any other card or documentation carrying personal details such as a bank statement, power or phone bill.

The following tips provide practical advice for reducing the opportunity of identity theft.

- Keep your personal information secure (see the fact sheets on [cheque](#), [credit](#) and [Eftpos](#) card fraud)
- Order a copy of your credit report at least once a year and check it carefully
- Restrict the number of people you share personal information with either in person, over the phone or online
- Shred or burn bank and credit card statements and other items with personal information before putting them out with the rubbish
- Put a lock on your letterbox

- Check you are receiving credit card statements or bills regularly and on time (someone may have changed your address details)
- If providing personal information, ask why it's needed, how it will be used and how it will be kept safe
- Only make telephone transactions when you have instigated the call and are familiar with the company

Online Internet trading and e-mail scams are also common ways of obtaining bank account or credit card details for fraudulent means, so:

- 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
- A secure server is usually used to send confidential information across the Internet. This information is encrypted and can only be decoded by the host site that requested it. Secure sites generally advertise this fact and provide information about the security of their server. Sending personal identity information over the Internet to an insecure server is not recommended
- Use virus protection software, install a firewall programme or password protect personal documents on your computer
- Delete personal information if you dispose of your computer
- Avoid using publicly accessible computers for online transactions. There have been instances in New Zealand of people installing keystroke recording software, returning to the computer after it has been used and retrieving other people's access codes, personal and account information
- Never create access codes with numbers that may be easily discoverable, such as your phone number or car registration
- Change access codes frequently and delete them when no longer required

If you ever need to obtain proof of identification from someone, a photo driver's licence or passport should be the only form of identification accepted. Document details should be recorded.

Even then be wary, as some fraudsters have obtained a photo driver's licence or passport using the birth certificate of someone they are pretending to be or intend to steal from.

Bankcards should not be accepted as ID, because it's possible for a fraudster to remove the original hand-written signature and replace it with a signature in their own handwriting.

If you believe you are a victim of identity theft, contact your bank or credit card provider immediately and explain the circumstances. You should also notify Police.

To minimise the risk of identity theft, remember to manage your personal information wisely and cautiously.