

Media Release

9 December 2013

Foil the fraudsters this festive season

As the festive season approaches the New Zealand Bankers' Association has reminded people how to avoid fraud and scams over the holidays.

"Don't let fraudsters spoil this special time of the year. Whether we're shopping or away on holiday, it pays to take care," said New Zealand Bankers' Association chief executive Kirk Hope.

If you're shopping for Christmas or taking advantage of the New Year sales, here are a few tips to bear in mind:

Card safety:

- Guard your card. Treat it like cash. Don't leave it lying around. Make sure you know where your card is at all times.
- Protect your PIN. Never tell anyone your PINs or passwords – not even the Police, bank staff, friends or family.
- Cover up. When entering your PIN number at ATMs and EFTPOS terminals, shield the PIN pad with your other hand. Criminals may 'skim' your card details by attaching a device to the card reader, and then 'shoulder surf' or use hidden cameras to record your PIN.

When shopping and banking online:

- Logon to internet banking by typing in your bank's full web address. Do not use links that appear to take you to your bank's website.
- Check you have a secure connection, which is shown by a padlock symbol somewhere on the page, and that the website address starts with 'https://'. The 's' stands for 'secure'.
- Avoid public computers and public Wi-Fi for internet banking, e.g. internet cafes, libraries or hotels.
- Protect your identity information and only provide it to trusted people and organisations. This includes your date of birth, address, driver's licence number and passport details.
- Shop with trusted retailers. Before you provide personal information make sure they will protect that information.
- Keep your anti-virus and firewall software up to date.

If you use your mobile phone for banking:

- Only download apps from trusted sources
- Keep device operating systems up to date, and update apps when prompted
- Use your phone's password lock feature
- Shield your passwords from people around you
- Change your passwords periodically, and make sure they are not easily guessable
- If available, use anti-virus software
- Contact your bank immediately if you lose your phone.

"If you're planning to travel overseas, it's a good idea to tell your bank. That way, transactions you make in another country won't surprise your bank. It's also important that your bank has up-to-date contact details in case they need to get hold of you," Hope said.

Hope also cautioned people to be aware of so-called "phishing" scams.

"Online scammers use a range of ways to trick people into handing over personal information, usually by phone or email. Once they have that information, such as your account number, log-in details, or password, they can access your identity and your money."

How to avoid phishing scams:

- Don't give out account details over the phone unless you made the call and you trust that the number you called is genuine.
- Don't reply to, click on any links, or open any files in spam emails. Don't call any numbers in spam emails.
- Never send your personal details or accounts or passwords in an email.
- Check your statements. Advise your bank immediately of any unauthorised transactions.
- If you suspect you've been taken in by a scam, contact your bank immediately.

"As well as protecting yourself from financial crime, you can also help keep others safe by reporting anything you know about frauds and scams to the Police or anonymously through Crimestoppers," Hope added.

Crimestoppers is an independent charity that allows anyone to report crime anonymously by phone or online. More information is available at <http://www.crimestoppers-nz.org/>.

ENDS

For further information please contact Philip van Dyk on 04 802 3354 or 021 242 0428.