



Media Release  
9 APRIL 2009

For further information: Mr Neville Parsons, CEO  
Holiday Coast Credit Union Ltd  
1 Commerce Street, Wauchope NSW 2446  
Phone: 02 6580 8226 Mobile: 0418 653 945  
Email: ceo@hccu.com.au

## PROTECT YOURSELF AND YOUR MONEY

Holiday periods are a traditional time of increased opportunity for fraudsters and an opportune time for crime. Holiday Coast Credit Union has issued this timely warning at this traditional busy time for fraudsters during the forthcoming Easter holiday period.

Neville Parsons, CEO of Holiday Coast Credit Union said fraudsters are using new ways to try to steal the money and even identities of people and personal vigilance is the best protection.

"You use a raincoat to protect yourself from rain, sunscreen to protect yourself from the sun, and insurance to protect yourself and your assets in case the unforeseen happens," Mr Parsons said.

"But we are constantly hearing of cases where people are handing over their PIN or password, or sending money overseas to people they have never met, seemingly without a second thought.

"We have a range of security measures in place to help protect our members from fraud, including adaptable external transfer limits, email notifications of all internet transactions on your account, suspicious transaction monitoring, first class fraud response procedures and even greater security enhancements for our internet banking members.

"But at the end of the day, the best protection in the world is only as good as the importance we each place on it."

Mr Parsons said remembering the following nine "fraud busters" are a good start:

1. Never, ever hand over your PIN, password or personal banking details to anyone. Your credit union building society or bank will never ask for your PIN or password in an email, an on-line message or in an unsolicited phone call. When using your PIN, password or personal banking details please ensure that no-one else can see over your shoulder and get access to that detail.
2. If you do receive an unsolicited phone call purporting to be from your financial institution requesting personal information, ask for the operators name and advise them you will call them back on their publicly listed phone number to be certain it is your financial institution calling you.
3. Ensure your details are up to date with your financial institution and that internet banking transaction receipts or alerts are switched on so that you are notified whenever an internet banking external transfer has taken place.
4. Never send money to someone you don't know personally, or know how to contact. Check names, addresses, phone numbers and referees of anyone before you even consider sending them money.
5. Always check the ATM before use to ensure that it looks normal and in particular that there is no additional device (Cameras or Skimming devices) attached to the card reader, cash dispensing chute or ATM surrounds.
6. Don't just bin your old bills, records or receipts – destroy them so no-one can read them and steal your identity.
7. Check your banking and credit card statements regularly to ensure that no-one is making unauthorised charges in your name.
8. Regularly check your credit file or subscribe to a credit alerting service to detect changes to your credit file to ensure your identification is not being used fraudulently to apply for credit in your name.
9. Be vigilant. If someone makes you an offer that sounds too good to be true. It probably is. Ignore it, report it and help slam the scams.

**ENDS**