News Release

27 June 2023

ANZ boosting customer protection against card fraud

Off the back of burgeoning scam and fraud cases, ANZ Bank New Zealand has bolstered its existing protection measures to better support customers on the go.

ANZ Fraud Check is a new tool that will allow the bank to communicate more efficiently with customers who have unusual transactions flagged on their eftpos, credit or debit card transactions.

Currently, when the bank identifies an unusual transaction, we phone the customer to ask them to confirm if the transaction was legitimate. The bank may also block the customer's card while they try to confirm this.

Fraud Check will streamline this process by alerting customers to any transactions identified as unusual via text message. Customers will receive a text message to their listed mobile number asking them to validate the transaction with a "yes" or "no". We will never ask a customer to click on a link to verify a transaction.

The message will include details about the transaction (amount, merchant name and the last four digits of the card used) or account activity triggering ANZ Fraud Check.

ANZ NZ Managing Director of Personal Banking Ben Kelleher says like all banks, ANZ is seeing an increase in fraud and scam activity.

"While moving quickly to block a customer's card is a great way to stop funds being lost to fraud, it is frustrating for customers when it is a legitimate transaction. Fraud Check will mean customers can just confirm quickly via text and take out some of that hassle."

ANZ's fraud detection system regularly detects and stops payment fraud.

"While only 0.06% of transactions are fraudulent, because ANZ processes 67 million transactions per month these add up quickly. We invest millions per year on our fraud detection systems which identify a high percentage of fraudulent transactions and stopping them before they are processed."

Mr Kelleher says it's important that people keep their contact details up to date so that the bank can reach them.

"We also encourage people to familiarise themselves with ways to stay safe from scams."

There are number of ways for people to protect their banking with the top three reminders being:

- Never give strangers access to your devices.

- Don't click on links in unexpected texts or emails.

- Hang up if unknown callers ask for personal information.

If you receive an unexpected phone call, voice message, email, or text, you should never provide credit card details, Internet Banking log in details, VISA secure codes, two-factor authentication codes, or other confidential information.

We encourage people to hang up and phone back on a publicly listed number if they want to check if the call was genuine.

Mr Kelleher says people should not feel embarrassed or ashamed if they have been scammed.

"It's really important to let us know if you think you have been the victim of a scam, or if you spot anything that seems suspicious," he says.

If you think you have been the victim of a scam, please call us immediately on 0800 269 296.

People can keep up to date with the latest banking safely information on our website. We regularly update this with information on the latest scams.

For media enquiries contact Kristy Martin 021531402