News Release

ANZ urges customers to be wary of scams following rate changes

ANZ is warning customers to be on alert for a potential rise in scam activity following the recent decision from the Reserve Bank of Australia (RBA) to lower the cash rate target by 25 basis points. The bank says it's the kind of event that cyber criminals could look to exploit by posing as financial institutions or advisers in an attempt to steal money.

In particular, ANZ asks customers to watch out for some of the common tactics that scammers use following major financial announcements, including fake loan or mortgage offers, phishing links, promises of "high return" investment opportunities, and fake financial advice.

At a time where customers might be considering to refinance their loans or secure a strong rate for their savings accounts, ANZ Head of Customer Protection, Shaq Johnson, says that it's important to remain cautious.

"We urge customers to be hyper-vigilant around major financial announcements like these. Cybercriminals are using technology in increasingly sophisticated ways and always looking for new and convincing ways in.

"A change in the RBA cash rate could give them the opportunity to exploit confusion or create a false sense of urgency around locking in strong rates and transferring large sums of money.

"Stop and think – if something sounds too good to be true, it probably is. Scammers will often advertise higher savings rates on fake websites impersonating a bank, preying on individuals looking for a stronger rate.

"It's important to cross-check all of the contact you receive directly with your bank. Customers and businesses can keep across the latest scam tactics and trends on our website, and we implore you to learn the signs that indicate a scam, and what to do should you be met with one.

"If you are ever unsure, or you feel like you are being pressured to share sensitive information or lock in a deal, call or visit your bank to verify the contact and offer is legitimate," Mr Johnson said.

What to look out for in investment scams:

- **Higher rates:** If it seems too good to be true, it probably is. Scammers will often advertise higher interest rates on websites, preying on individuals looking to maximise their savings. If a rate is suspiciously high or marginally better than those advertised elsewhere, pause and do some further research before transferring any funds.
- **Email/social media ads**: If you receive an email or see a social media ad with a well-known celebrity spruiking an investment opportunity guaranteed to make money fast, treat it with caution. Scammers will publish fake news articles and use deepfakes to make you believe it is legitimate.
- **Unexpected contact via SMS/messaging app**: If you are contacted unexpectedly by an unknown person via SMS or a messaging app (e.g. WhatsApp/Telegram) who attempts to befriend you initially, but the conversation shifts to investment, be wary.
- **Limited online footprint**: A legitimate investment company should have a visible online footprint. If you search for information online about the company and there's hardly any information, that's a red flag. Always search the investment company on the Investor alert list on the Moneysmart website. Also ask the company for their Australian Securities and Investments Commission (ASIC) registration or Australian Financial Services (AFS) license.
- **Difficulty withdrawing funds**: If you have deposited funds into an investment platform and when you attempt to withdraw, you're advised you have to pay a fee on your earning to access them, it is likely to be a scam.
- **An urgent tone**: Your bank will not contact you and create a sense of panic or fear about your finances or advise that you must lock in a rate immediately.
- **Downloading remote access software**: If an employee of the investment company you're dealing with suggests downloading Remote Access Software to help set up accounts with other investment platforms, this is a red flag.
- **Cryptocurrency investment**: If the investment company you're dealing with advises you to open an account with a cryptocurrency exchange to purchase and send cryptocurrency to a wallet address they provide you, this is highly likely to be a scam.
- **Recovery of lost funds**: If you have previously been the victim of an investment scam and you're contacted unexpectedly by someone advising they can help recover your funds for a fee, this is likely to be a continuation of the original investment scam.