News Release

For Release: 19 June 2025

ANZ reminds Australians to stay scam alert this EOFY

ANZ is reminding customers to be on high alert this end of financial year as scammers attempt to target Australians during tax time.

From tax-related impersonation scams to dodgy shopping websites offering massive EOFY discounts, the bank is warning that scam tactics are becoming increasingly targeted and is urging Australians not to be complacent when it comes to protecting their finances.

ANZ Head of Customer Protection, Shaq Johnson, says while ANZ has a number of measures in place to protect customers against fraud – preventing more than $50 million in suspicious transactions linked to scams between October 2023 – September 2024 alone, it's important customers remain vigilant and cross-check all contact with their bank, the Australian Taxation Office (ATO), or other government organisation at this time of year.

"Tax time is already a confusing period for many Australians and in the businesses of lodging a return, it's easy to let your guard down. Cybercriminals will look to exploit this, so it's crucial Australians understand the warning signs to avoid falling victim to a scam.

"During the end of financial year period, scammers may use targeted, sophisticated tactics to attempt to steal money or personal information. While many Australians have a good understanding of how to spot a scam, it's important to be aware of the specific red flags related to this time of year.

"Common watchouts include unexpected text messages or emails claiming to be the ATO or your bank alerting you to an unclaimed refund or outstanding tax bill. These messages will often include a link to click and have a sense of urgency to the request.

"We're urging Australians to stop, think, and consider. If you are ever unsure that a message is legitimate, or simply would like the peace of mind, call your bank or relevant government organisation. We're here to help," Mr Johnson said.

During tax time in 2024, ANZ saw a spike in attempted rebate and extortion scams during the end of financial year period, with the volume of rebate scams (total number of scam cases created) surging by 50% in July before dropping sharply in August. Extortion scams followed a similar trend, rising significantly in June (41%) and July (64%).

- **Rebate scams** refer to instances where scammers attempt to convince victims they are entitled to a rebate or reimbursement from a bank or government service such as the ATO or myGov. To claim the amount owed to the victim, the scammer will ask for a small initial payment to cover 'administration fees' or taxes.
- **Threats and Extortion scams** refer to situations where scammers ask victims to complete a payment or risk punishment such as arrest or deportation. In these scenarios, scammers often make direct threats or detriment to the customers' living circumstances due to an 'outstanding' charge, such as an unpaid tax bill.

As well as a heightened risk of tax return and payment related scams, ANZ is reminding Australians to be on the lookout for online shopping scams when making the most of the EOFY sales.

"We know Australians love to snap up a bargain during the EOFY sales, and we also know scammers will attempt to take advantage of this. Common red flags to look out for when shopping online this EOFY include inconsistent or unfamiliar contact information, significantly cheaper offers compared with other sellers, or any deal that seems too good to be true," Mr Johnson concluded.

How to spot a rebate scam this EOFY:

- **Someone contacts you unexpectedly** via a phone call, email, phone message, or letter. They claim you have unclaimed money which you'll have to pay a fee to access. Or, they might ask for your personal information to verify or process the payment.
- **You receive an unexpected email or letter** that looks official, which asks you to pay an upfront fee to receive your tax refund or rebate.
- **There's a suspicious link in the message** that appears to be from the government, bank, or other institution. The link may not match the company it's claiming to be from or looks unusual, such as having hyphens, symbols or typos in it.

- **The message sounds urgent** and is pressuring you to quickly share personal information or pay a fee.

How to spot a threat and extortion scam this EOFY:

- **Getting a call out of the blue** from an 'official' who is aggressive or threatening.
- **Messages or automated calls from someone you don't know** claiming to have compromising information about you.
- **Someone sending you an email with a password you used in the past** (or one you currently use), as proof they can access your accounts.
- **There are short deadlines** for you to transfer funds.

How to spot an online shopping scam this EOFY:

- **Inconsistent domains:** Cybercriminals may use email and website domains that appear similar to the legitimate sender. Compare the domains to the company's official domain online.
- **Uncommon payment methods**: Fake sites may ask for unsecure methods of payment such as direct transfers or gift card payments when shopping online.
- **Overly positive reviews:** Search for independent reviews of an online trader to ensure legitimacy, particularly if the brand is unfamiliar to you.

It can be hard to spot scams and fraudulent activity. In a genuine ANZ call, SMS message, letter or email, we will never ask you to:

- Share sensitive banking details (like passwords, PINs, ANZ Shield codes, token codes, or one-time passcodes for payment).
- Click a link to log in to your account or type a particular website address into your browser.
- Grant remote access to your computer, phone, tablet (or any other mobile device).
- Transfer money to another account.

For media enquiries contact:

Kate Power
Public Relations Manager
Tel: +61 481 547 556

Julia Bruhn
Media Relations Coordinator
Tel: +61 408 143 059

ANZ's customer protection teams and systems operate 24/7. Customers who believe they may have been a victim of a scam should contact us immediately, on 13 13 14 or visit us at http://www.anz.com.au/security/report-fraud/ for more information.

For more information on the types of scams and how to protect yourself visit http://www.anz.com.au/security/types-of-scams.

About ANZ Scam Safe: To assist the community in remaining aware and alert to the constantly changing scams and fraud environment, ANZ has launched *Scam Safe.*

Scam Safe highlights the latest cyber security and fraud issues impacting the community and what ANZ is doing to help protect our customers.

To stay *Scam Safe,* ANZ encourages customers to learn their security ANZ's:

A: Always be wary

N: Never share personal information, with anyone

Z: Zoom in on the details, they matter