EUROZ HARTLEYS

Dear Client,

On 15 October 2024, the Australian Securities and Investment Commission (ASIC) released the following article. We believe it is important that all of our clients understand the increased risk of scams and fraud and the potential impact.

ASIC is warning investors to be on high alert following a significant increase in reports of stolen shares since August 2024 from people who have had their personal identity compromised.

Fraudsters are impersonating individuals and stealing their shares, with many victims unaware their shares have been transferred or sold until they receive a confirmation letter in the mail from a share registry or the Clearing House Electronic Subregister System (CHESS).

Australians previously affected by data breaches should be particularly alert to the increased likelihood of identity theft, given the availability of their personal information online.

Fraudulent activity using stolen identities is increasingly sophisticated, so it's important to be vigilant and follow through with checks when you receive notifications that are unexpected or do not look right to you.

How does share sale fraud work?

A fraudster claiming to be 'Jane Citizen' creates a share trading account to sell shares owned by the real Jane Citizen. The ID used to open the account is stolen or fake, with the security reference number or holder identification number for Jane Citizen's shares illegally obtained. A bank account may also be fraudulently opened with the name 'Jane Citizen' to receive proceeds from the share sale.

ASIC said it was important people know fraudsters can gather personal information not only from information available online but also by stealing mail from letterboxes.

ASIC strongly encourages all investors to be on the lookout for suspicious activity when it comes to their share registry, share trading and bank accounts, and to take steps as soon as something doesn't look right.

EUROZ HARTLEYS

How to be vigilant and act if something looks suspicious

1. Review your share portfolios regularly, regardless of whether they are issuer-sponsored holdings registered with share registries or held in share trading accounts with stockbrokers, so you're quicker to detect unauthorised activity. It is also prudent to regularly review your other investment accounts such as super and managed funds.
2. Use passphrases rather than simple passwords for online accounts.
3. Turn on multi-factor authentication, if it's available, as this can add an extra layer of security to prove your identity.
4. Lock your letterbox to prevent mail theft and check it frequently.
5. Ensure you have provided your most up to date contact details to your stockbroker, share registries and financial services providers.
6. If you receive a new bank card or correspondence that is unexpected, like an update on how your shares are held, the creation of a new account, a notification of sale of your shares or confirmation of a change in contact details, don't ignore the correspondence.
7. If something is unexpected or feels wrong, act quickly. Call your stockbroker, the share registry or bank if there is activity you didn't authorise and change your passwords.
8. Contact the party that sent you the correspondence using the contact details from the organisation's official website (not the email or letter which may be fraudulent).
9. Report any incidents to Scamwatch.
10. Contact IDCARE, a free government-funded service, which can help to develop a specific response plan if your identity has been compromised.
11. If you're a victim of fraud, you may also request that credit reporting bodies place a ban period on your consumer credit report, so it can't be used as part of a credit check.

Where to go for more information

See the ASIC Moneysmart website for a range of tips to protect yourself from identity fraud.

You can also find further information on the Government's IDMatch website.

If you have any concerns regarding this, please do not hesitate to contact your Euroz Hartleys adviser.