FACT SHEET

FACT SHEET: Investment Scams

There are three common types of investment frauds:

1. The investment opportunity is fraudulent and does not exist
2. The investment opportunity presented is legitimate, but your money never actually goes into it
3. The financial or investment firm is legitimate, but the individual contacting you does not actually work there

Quick Facts

- Almost 80% of investment fraud clients to engage IDCARE were initially responding to a fraudulent advertisement or news article on a social media platform, such as Facebook.
- The majority involved investment in cryptocurrencies or binary options (speculating on the rise and fall of the market value of investments).
- In the first quarter of 2021, callers to IDCARE reported the average amount of money lost to investment scams was $33,000, with many individuals investing $200,000 or more.
- On top of the financial losses incurred, many callers had also shared credentials such as driver licences and passports, or provided remote access to their devices as part of engaging in the investment scam.

Detection – Is this an investment scam?

The majority of investment scams begin online, although some IDCARE clients also report having responded to a telephone cold-call. IDCARE has also seen relationship and employment scam attempts divert to investment scams, and vice versa.

If you are concerned that you or someone you know may be involved in an investment scam, this checklist provides some of the common elements of an investment scam. The more times you answer "yes", the more likely it is that this is an investment scam.

- ☐ The investment opportunity was first discovered online via a social media advertisement or online media article.
- ☐ The investment opportunity was endorsed by a celebrity or other public figure.
- ☐ The investment opportunity appeared to be endorsed by a well-known television program.
- ☐ The investment broker contacts you quickly, perhaps within fifteen minutes, of completing an online form.
- ☐ Communication with the investment broker moves from the initial website to alternative methods, such as telephone, online audio (eg. Zoom without video), or email.
- ☐ In order to invest, you must set up a "trading profile" which may also require:
    - Copies of your driver licence or passport to open
    - Your investment broker to access your computer remotely to help with setup or guide you through the trading process
- ☐ The initial investment was under $500 (often paid in US dollars) and accepted as a credit card payment.
- ☐ The small investment is highly successful, and you are encouraged to invest larger amounts quickly.
- ☐ You are encouraged to invest larger amounts in order to access premium support with a dedicated broker.
- ☐ You build a strong rapport with your investment broker, despite never meeting in person.
- ☐ Your investment broker appears to be calling from either Australia, New Zealand or the United Kingdom.
- ☐ They may be listed as a scam company on the International Organization of Securities Commissions (IOSCO), despite not appearing on ASIC (Australia) or FMA (New Zealand).
- ☐ Your investment broker does not have an Australian Financial Services Licence or does not appear on the New Zealand Financial Services Provider Register.
- ☐ Your money is invested offshore.
- ☐ Your online trading platform displays graphics and balances that consistently show positive returns, above what investors in other markets are experiencing.
- ☐ You are encouraged to recruit others into the investment opportunity.
- ☐ You receive small reimbursements or expensive gifts initially.
- ☐ You have not been able to access your invested funds when requested. Reasons provided may include:
    - You will lose too much money if you withdraw funds now
    - Your broker claims to be a "joint investor" – if you withdraw your money now, they will lose their money
    - Complicated international tax arrangements
    - Foreign currency fees need to be paid first
    - Your broker has left the company, is ill, or has died and they need to review your account

FACT SHEET

FACT SHEET: Investment Scams

Response – What do I do now?

- ☐ Cease all communication with the scammer – phone, email and online.
- ☐ Tell a trusted person what has happened, and let them know you need their support as you work through your financial, emotional and practical recovery.
- ☐ Contact your GP if you feel you need additional support to work through your grief over the financial and emotional losses.
- ☐ Contact and advise your banks and any other financial institutions of the investment scam, and request increased security on your accounts, including blocking international transfers.
- ☐ Notify the relevant document issuing organisations for any of the credentials that the scammer may have accessed. Common credentials include:
  - Driver licence
  - Passport (Australian passports contact DFAT on 131 232, for NZ passports contact DIA on 0800 22 50 50)
  - Medicare card (Australian residents contact Services Australia on 1800 941 126 or email the Scams and Identity Theft Helpdesk)
  - ATO details (Australian residents call 1800 467 033) or IRD details (NZ residents call 0800 257 777)
  - RealMe details (NZ residents call 0800 664 774 or online at RealMe)
  - Bank account details, including login information
- ☐ Contact your superannuation fund/s to increase security on your accounts.
- ☐ Contact all Credit Reporting Agencies for your free credit reports and to arrange credit bans.
- ☐ Update or add passwords, PINs, and multi-factor authentication to all accounts, apps, and websites requiring logins.
- ☐ Check if forwarding rules have been changed on your email accounts.
- ☐ Be aware that you may see an increase in scam attempts unrelated to the relationship (via telephone, email and SMS).
- ☐ Contact the police to report any misuse of your identity, and keep your police report number.
- ☐ In Australia, submit a report via ReportCyber. In New Zealand, call police on 105 or submit a report online (choose "Report a Police non-emergency"), and report the scam online with Netsafe.
- ☐ Remove all instances of remote access software or take your device to a trusted IT provider. You can also ask your IDCARE case manager about our free Cyber First Aid support service.

Prevention – How can I avoid an investment scam?

- Research the investment opportunity thoroughly before engaging. Check out whether it has been listed as a scam company with the International Organization of Securities Commissions (IOSCO).
- Check if the company is authorised to provide financial services. ASIC (Australia) and FSP (New Zealand).
- It is easy for scammers to copy logos and layouts from legitimate company websites.
  - Call the company directly, using a number you find independently from that used in the initial contact.
  - Look at the URL carefully and see if it is uses strange punctuation, or uses numbers in place of similar letters (eg. "1" instead of "l").
  - Do a reverse phone lookup on the number provided and check for reviews (but be careful, as the number may have been "spoofed" or copied from a legitimate person or company).
- Take your time when deciding to invest – don't be pressured or rushed.
- Discuss the investment opportunity with family, friends and work colleagues before deciding if you will invest.
- Talk to your bank, other financials institutions, and accountant before investing any money.

For additional support or information, contact IDCARE by submitting a Get Help Form or call 1800 595 150 (Aus) or 0800 121 068 (NZ).