

Introduction

Investment scams are deceptive schemes designed to convince people to invest money with the promise of financial gain. Most investment scams begin online, although some IDCARE clients also report having responded to a telephone cold-call offering an investment opportunity. IDCARE has also seen relationship and employment scams turn into investment scams.

There are three common types of investment scams:

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 work there.

Prevention checklist

How can I avoid an investment scam?

- ☐ Research the investment thoroughly before engaging. Check whether it has been listed as a scam company with the International Organisation of Securities Commissions ([IOSCO](#)). You can also search [ASIC Investment Scam Alerts](#) as part of your due diligence. Please be aware though, that not being listed on these sites is not a guarantee that it is a legitimate investment opportunity. Additionally, do not rely on online reviews and social media comments, as these may not be verified.
- ☐ 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. Look at the URL carefully and see if it uses unusual punctuation or uses numbers in place of similar letters (e.g. "1" instead of "l").
- ☐ 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 or financial advisor/accountant before investing any money.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Detection checklist

If you are concerned that you or someone you know may be involved in an investment scam, this checklist may help:

The more boxes you tick, the more likely it's a 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, other public figure, or a well-known television program.
- ☐ An investment broker contacts you promptly after completing an online form.
- ☐ Communication with the investment broker may occur via encrypted or private messaging platforms.
- ☐ To invest you must set up a "trading profile" which may also involve providing identity documents and possibly requests for remote access to your device to help setup the account or trading platform or to guide you through the trading process
- ☐ The initial investment is successful, and you are then encouraged to invest larger amounts, or you are presented with time limited offers.
- ☐ You can withdraw a small amount initially, but subsequent requests to withdraw money are met with resistance, or you are told to pay upfront fees to access your funds.
- ☐ You build a strong rapport with your investment broker, despite never meeting in person.
- ☐ Your investment broker does not have an [Australian Financial Services](#) Licence or does not appear on the New Zealand [Financial Services Provider Register](#).
- ☐ A company possessing an Australian Financial Services licence, or an [Australian Business Number](#), does not guarantee they are legitimate.
- ☐ Your online trading platform displays graphics and balances that consistently show positive returns, often above what investors in other markets are experiencing.
- ☐ You are encouraged to recruit others into the investment opportunity.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Detection checklist cont.

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.

The scam company does not appear in the Australian Financial Complaints Authority [Financial Firm Search](#). If the name does appear in the search results, this does not confirm the company's legitimacy. It may indicate that the scammers are impersonating a genuine business. Investigate further to verify whether the company is authentic.

Response checklist

If you or someone you know has been involved in an employment scam, the below checklist outlines some measures you can take to prevent further financial harm.

- ☐ Cease all communication with the scammer.
- ☐ Tell a trusted person what has happened if you need support as you work through the financial, emotional and practical recovery.
- ☐ Advise your bank(s) and superannuation company of the investment scam (if this information was provided).

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)
 - 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](#))

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Response checklist cont.

- ☐ If you have provided government issued identity documents, contact both credit reporting agencies for your [credit reports](#) and to request a [credit ban](#).
- ☐ Be wary of organisations claiming that they can recover your investments for a fee. These 'money recovery' scams are well known to target previous victims of investment scams. They may even engage with the details of your investment and claim to be involved with law enforcement or other regulatory bodies.
- ☐ If you have sent or received money or goods online, provided remote access to your computer, or shared credentials online that would enable identity theft and fraud, you can alert police through:
 - [ReportCyber](#) (in Australia)
 - Call 105 or [online](#) and choose "Report a Police non-emergency" (in New Zealand)
- ☐ Contact your GP if you feel you need additional support and strategies to deal with the stress of your situation.
- ☐ Be aware that you may see an increase in scam attempts.

Relevant websites

- [Moneysmart](#)
- [Australian Securities & Investments Commission](#)

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.