RICHARDS FINANCIAL

Is it a scam?

New data released

Naturally, people aspire to get the most out of their investments, especially if a great opportunity is presented by a 'trusted' organisation. However, investment scams occur more often than you may think, highlighting the risk both self-directed investors and SMSF trustees may potentially face when seeking new investment opportunities.

New data released from Scamwatch Australia has reinforced the sophistication and rapidly growing number of scams each year in Australia – which has caused a loss of over $851 million* in total in 2020 – $328 million of which related to investment scams. It is extremely important for you to remain vigilant and reach out to me, your trusted SMSF professional, before investing your retirement savings in a new product or service.

*ACCC Media Release 7 June 2021

What does the data reported to Scamwatch Australia tell us?

During 2020, the average monetary value lost to scams has increased by 23%. Scammers have become more sophisticated in their approach, claiming to be from well-known investment organisations or government bodies, with the aim of extracting personal information from an individual.

Investment scams have caused the most financial harm to the Australian population throughout 2020 resulting in $328 million lost. Advancements in both technology and software design allow scammers to recreate websites to look

CONTACT US

Email
enquiries@richards.net.au

Phone
02 4782 1148

Postal
PO Box 744, Katoomba

Address
180 Katoomba St, Katoomba

Website
Richards.net.au

identical to an actual organisation's site, meaning it is becoming increasingly difficult to identify what is a scam and what isn't.

Older Australians (65+) are often more at risk of being approached by scammers as they perceive this particular age group to have more accumulated wealth.

The top contact methods used by scammers include phone (47.7%), email (22%), text message (15%), internet (6.3%) and social networking (4.5%)*. Scammers will often inject a sense of urgency into their messaging, propose threats (particularly with tax scams), and request personal and banking information.

*Scamwatch Australia Targeting scams report 2020

What should you do if you suspect a scam?

If someone attempts to scam you, there are several things you can do:

- Report the scam to Scamwatch Australia - www.scamwatch.gov.au/report-a-scam or ReportCyber - Report | Cyber.gov.au immediately.
- Do not provide any personal information that will allow a scammer to impersonate and retrieve your funds.
- Do not click on links you have received via text or email that have a substantial number of letters and numbers.
- If you have lost money to a scam, contact your financial institution immediately.
- If you have provided personal information and you are concerned your identity may be compromised, you can contact IDCARE for free support on 1800 595 160.
- Consider contacting the organisation the suspected scammer claims to work for – the organisation may be able to confirm your suspicions.

If you have been scammed or believe you have been scammed, you shouldn't feel embarrassed or ashamed. Financial scams are now crimes which are occurring regularly – many scams are very sophisticated and professional, and very experienced investors have lost money to scams. It is becoming increasingly important to discuss the risk of scams with family, friends, and peers.

How can we help?

If you need assistance with identifying whether you are being approached by a scammer, please feel free to give the office a call on 02 4782 1148 to discuss in more detail. We are here to support you and it's important that we start the conversation as scamming is a continuous risk in our technologically advanced world.

If you would like to seek more information about scams to protect your SMSF, you can refer to the SMSF Association's trustee education platform, SMSF Connect.

How to spot a scam

4 Practical Tips

Advancements in technology has allowed scammers to become more professional in their approach. According to Scamwatch Australia, a reported $851 million was lost to scams in Australia in 2020, with $328 million comprising of investments scams, some of which may have impacted SMSFs.

As an SMSF professional, it is extremely important to be able to spot the difference between a real investment opportunity and a scam. So your clients can rest assured that you have your scam radar ready, here are **4 practical tips:**

Is the individual, organisation, or government body who they claim to be?

If your client receives a phone call from someone claiming to be from a well-known organisation asking for personal or financial information, advise them to:

- Hang up immediately.
- Consider contacting the organisation as they may be able to confirm their suspicions.

Consider using tools to help protect and secure digital devices from scams.

Protecting devices and online security is critical and should occur continuously. You can advise your clients to:

- Install an anti-virus software.
- Monitor credit/debit card transactions to ensure there is no unauthorised activity.
- View IDCare's complimentary Cyber First Aid Kit and follow the prompts.

Do not click on any suspicious links sent via text or email - even if it states it is from a trusted organisation like AusPost.

If your client receives a text or email containing an urgent call to action followed by an unusual link with suspicious random numbers and letters, it is most likely a scam. Advise them to avoid clicking on the link provided, and delete the message immediately.

Often, if something seems too good to be true, it usually is.

If your client receives a great investment opportunity, promising high returns and minimal fees, there's a good chance this is a scam. Encourage a conversation and thorough due diligence before making an investment decision.

If your client has been approached by a scammer, there are several things they can consider

- Report the scam to SCAMwatch Australia immediately – scamwatch.gov.au/report-a-scam
- If they have lost money to a scam, they should contact their financial institution immediately.
- If they have provided personal information and are concerned their identity may be compromised, they should contact IDCARE for free support on 1800 595 160.