



Forensic Services

Australian Scam Culture Report

September 2023 Quarter



Introduction

In today's continually evolving digital landscape, scammers are constantly looking for newer ways to deceive the vulnerable via email, text messages, phone calls, and social media. Through convincing marketing and the latest technology, scammers leverage authority, urgency, and emotion, costing hard-working Australians and the industry millions of dollars and untold emotional distress. In the second quarterly edition of BDO's Australian Scam Culture Report, we provide a comprehensive analysis of the scam activity for FY24 – Q1 (September 2023).

A record level of scam activity continued during the September 2023 quarter, with [Scamwatch](#) reporting an approximate financial loss of over AUD \$105 million.

“ *Investment scams, while not the highest by number of occurrences, still account for the highest dollar amount of losses in the quarter. However, in the September 2023 quarter, losses attributed to investment scams decreased by over \$13 million in comparison to the June 2023 quarter. This may in part be the first results of proactive action including [ASIC's](#) new investment scam and phishing website takedown capability which forms part of the government's Fighting Scams initiative and supports the work of the National Anti-Scams Centre (NASC) which commenced operation on 1 July 2023. It will be interesting to see the impact this may have in future quarters in relation to monies lost by way of investment scams.*”

Michael Cassidy
BDO National Forensic Services Leader

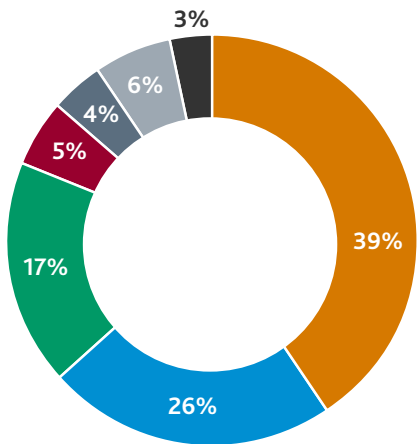


The results

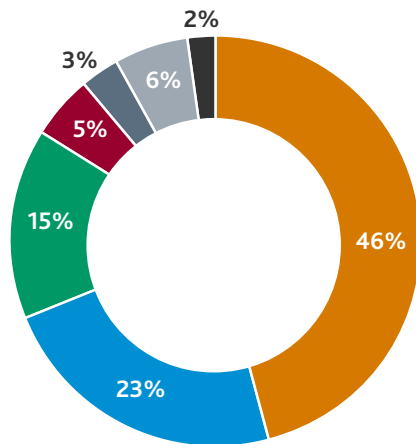
Scam delivery method (four-quarter comparison)

Emails have surpassed phone calls, and increased by 4% this quarter, becoming the primary method for delivering scams. This shift may be attributable to the increasing reliance on digital communication and the inherent capability of email systems to be 'individually' tailored yet be sent out in bulk to large volumes of recipients.

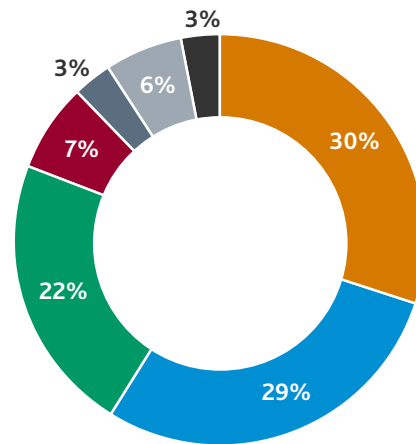
December 2022 quarter scam delivery method



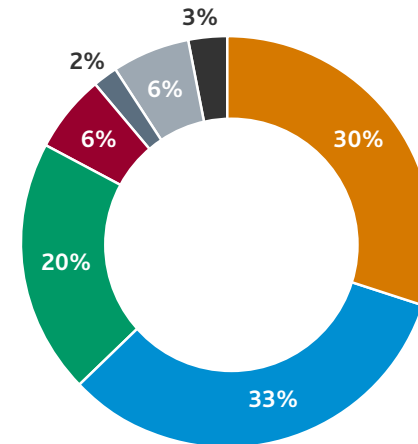
March 2023 quarter scam delivery method



June 2023 quarter scam delivery method



September 2023 quarter scam delivery method

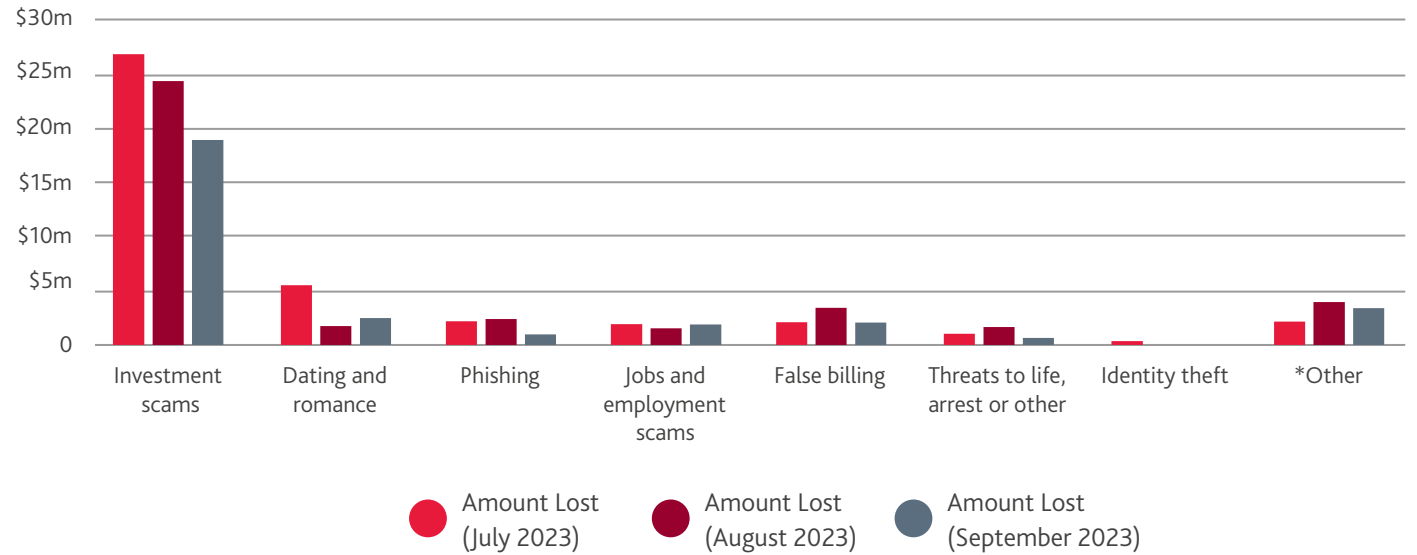


- Text message
- Email
- Phone calls
- Internet
- Mobile applications
- Social networking
- Other

AUD\$ lost by scam type

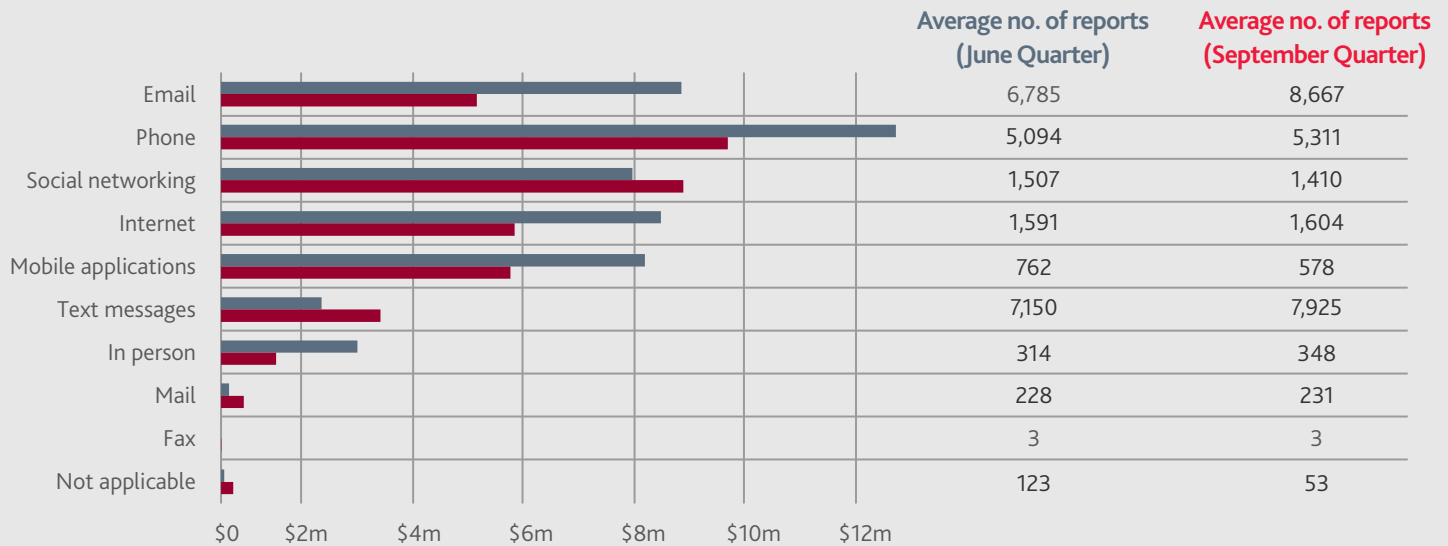
Investment scams continue to be the type with the highest impact, contributing to 66% of the total monies lost reported in the September quarter. Common types of investment scams include Crypto scams, Ponzi schemes, Imposter bonds, and fake initial public offering scams.

*Other includes: Remote access scams, classified scams, rebate scams, online shopping scams, pyramid schemes, and health medical products scams.



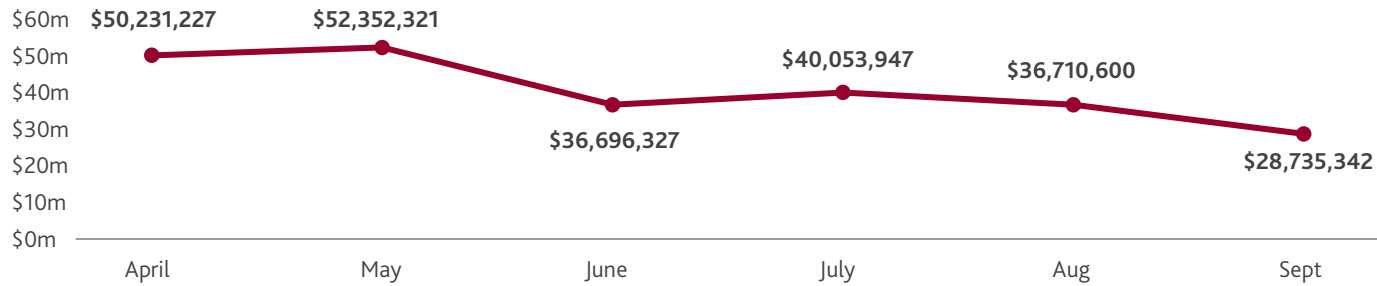
AUD\$ lost by delivery method (two-quarter comparison)

In the September quarter, phone calls, emails, and text messages equal 84% of reported activity, which resulted in 45% of reported value lost. The monetary value lost to scams has dropped by 24% from the June quarter to the September quarter, although the number of reports has increased by 11%.



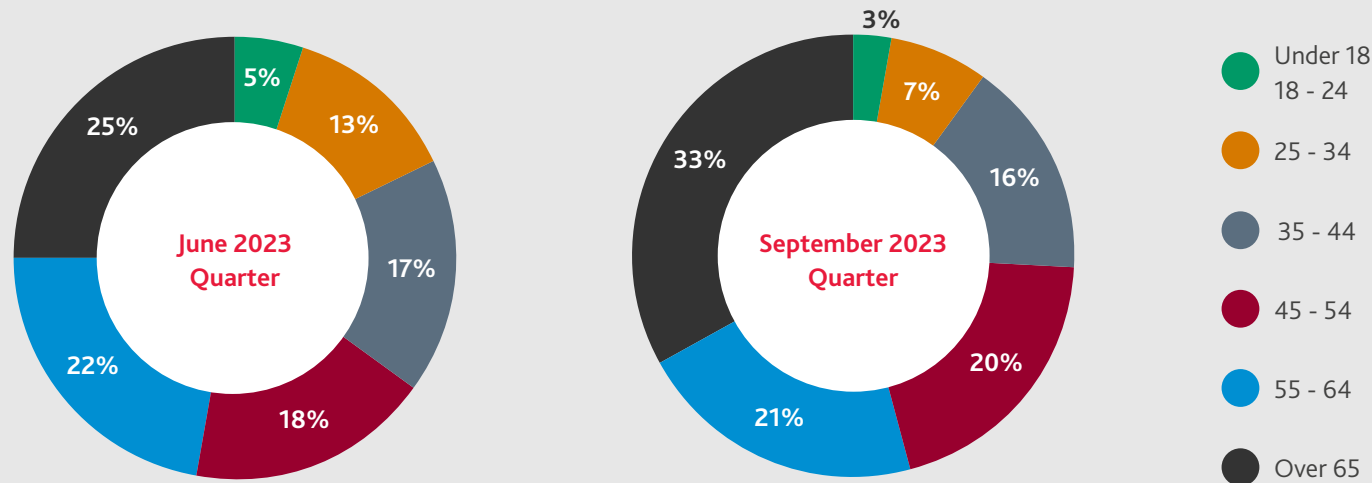
Total AUD\$ lost by scams (two-quarter comparison)

The total losses in \$AUD from reported scams in the September quarter have decreased by 24% compared to the previous April to June quarter. The total amount lost in the June quarter was \$139,279,875 compared to the total amount lost in the July - September quarter of \$105,499,889.



Age groups targeted in scams (four-quarter comparison)

In the June quarter, 47% of individuals subjected to scams were aged 55 and over. In the September quarter, this figure increased to 54% - a 7% increase illustrating that scammers continue to target the 'Generation X' populations.



Source: 2023, All scam types stats - [Scamwatch](#), Australian Competition and Consumer Commission, ©Commonwealth of Australia



A snapshot: dealings on the dark web

The dark web - a hidden part of the internet that is not indexed by traditional search engines - plays a significant role in the global landscape of cybercrime and scams. It provides a platform for user anonymity for the sale or trade of personal data, including stolen credentials, financial information, and personal identification details. Scammers can purchase this data to execute identity theft and phishing scams.

As compared to the previous quarter, we find (next page):



Identity Information



- ▶ Passport: Various nationalities \$1,399 (currently discounted from \$2,800)
- ▶ COVID-19 Certificate \$139 (up from \$119 in June 23 quarter)
- ▶ Digital COVID-19 certificate \$123
- ▶ Drivers Licence \$465 (currently discounted from \$545)
- ▶ US Fullz (Identity theft) \$16
- ▶ US Identity cards \$854 (currently discounted from \$1,088).

Account hacking



- ▶ \$668 Email (up from \$269 in June 23 quarter)
- ▶ \$310 Facebook, Instagram, Snapchat, Telegram, WhatsApp (up from \$119 in June 23 quarter)
- ▶ \$154 WeChat Hack (up from \$149 in June 23 quarter)
- ▶ \$11 LinkedIn Company Profile
- ▶ \$3 WiFi hacks
- ▶ \$1,089 Hacking (Phone / SMS / Email).

Carding ((Visa, MasterCard, American Express (AMEX))



- ▶ \$3,000 USD balance \$163 (down from \$180 in June 23 quarter)
- ▶ \$2,500 USD balance \$163
- ▶ \$5,000 balance \$78
- ▶ Australian CBA Credit Card Statement (with custom details) \$39.

Phone/data SIM copy services



- ▶ SIM card copy \$621 (currently discounted from \$932).

Distributed denial-of-service (DDoS) attack



- ▶ **DDoS attack:** Clearnet \$139 (up from \$89 in June 23 quarter)
- ▶ **DDoS attack:** ToR network \$249 (up from \$160 in June 23 quarter).

Money transfer costs



- ▶ Payment transfers \$900 - \$187
- ▶ Payment transfers \$1300 - \$249
- ▶ Payment transfers \$1700 - \$311
- ▶ Western Union Transfer \$5,000 - \$78.

Payment facilitation/transfers (paid into PayPal/Skrill accounts)



- ▶ PayPal - Buy 2 and get a Skrill Account with Approx \$4,500 balance - \$125.



Latest trends

There is increased negotiation activity on the dark web, with traders and buyers actively promoting communication to resolve issues and differences. Like any marketplace, trust is crucial to making a transaction on the dark web, because if a transaction doesn't go to plan, you cannot report it to the police.

Sellers inviting buyers to negotiate with them and reach a solution has become a standardised feature, rather than setting fixed prices with no room to move.



Pricing - No significant change, with the possible exception of passports which have dropped significantly.



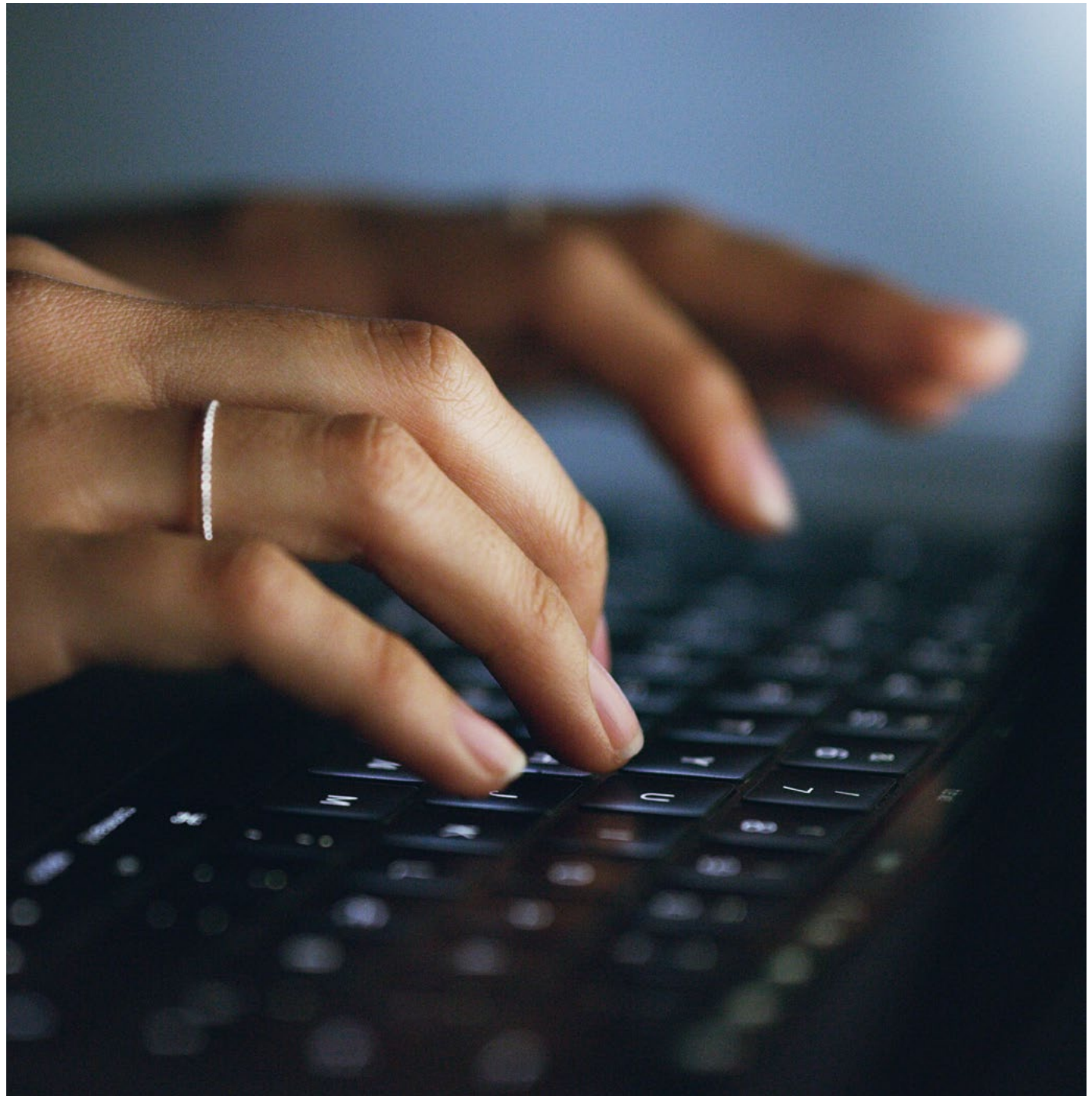
An increase in activity for **Identity documents** in countries such as Germany, Italy and France.



Law enforcement is active, with a number of the larger and popular marketplace sites having been shut down, however, several newer ones have sprung up in their place – many with the same vendors.



Security to access marketplaces is high – mainstream business could learn a lot from the approaches undertaken.



About BDO

BDO's forensic experts work with organisations to effectively identify and respond to suspicious activity. The multidisciplinary team includes certified accountants, certified fraud examiners and forensic accountants, forensic technology professionals, licensed investigators, financial analysts, and former members of law enforcement.



Michael Cassidy
National Leader, Forensic Services
michael.cassidy@bdo.com.au
+61 8 6382 4761



Stan Gallo
Partner, Forensic Services
stan.gallo@bdo.com.au
+61 7 3237 5995



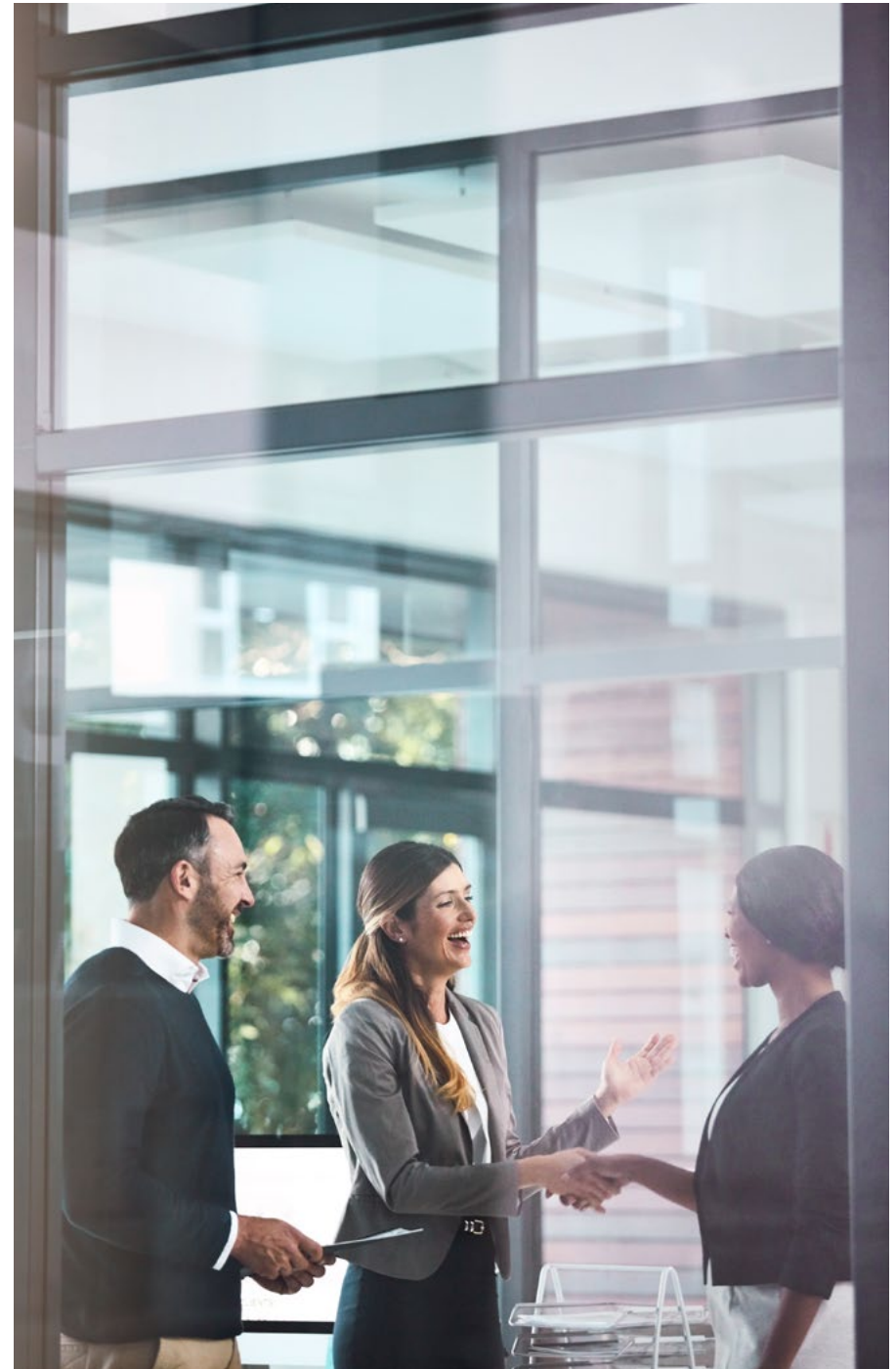
Karyn Lander
Director, Forensic Services
karyn.lander@bdo.com.au
+61 8 6382 4914



Michael Tarnawsky
Forensic Technology Specialist,
Forensic Services
michael.tarnawsky@bdo.com.au
+61 7 3237 5693



Conor McGarrity
Partner, Forensic Services
conor.mcgarrrity@bdo.com.au
+61 7 3237 5841



1300 138 991

www.bdo.com.au

NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA

AUDIT • TAX • ADVISORY

This publication has been carefully prepared, but is general commentary only. This publication is not legal or financial advice and should not be relied upon as such. The information in this publication is subject to change at any time and therefore we give no assurance or warranty that the information is current when read. The publication cannot be relied upon to cover any specific situation and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances.

BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not give any warranty as to the accuracy, reliability or completeness of information contained in this publication nor do they accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it, except in so far as any liability under statute cannot be excluded.

BDO Australia Ltd ABN 77 050 110 275, an Australian company limited by guarantee, is a member of BDO International Ltd, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© 2023 BDO Australia Ltd. All rights reserved.

30320