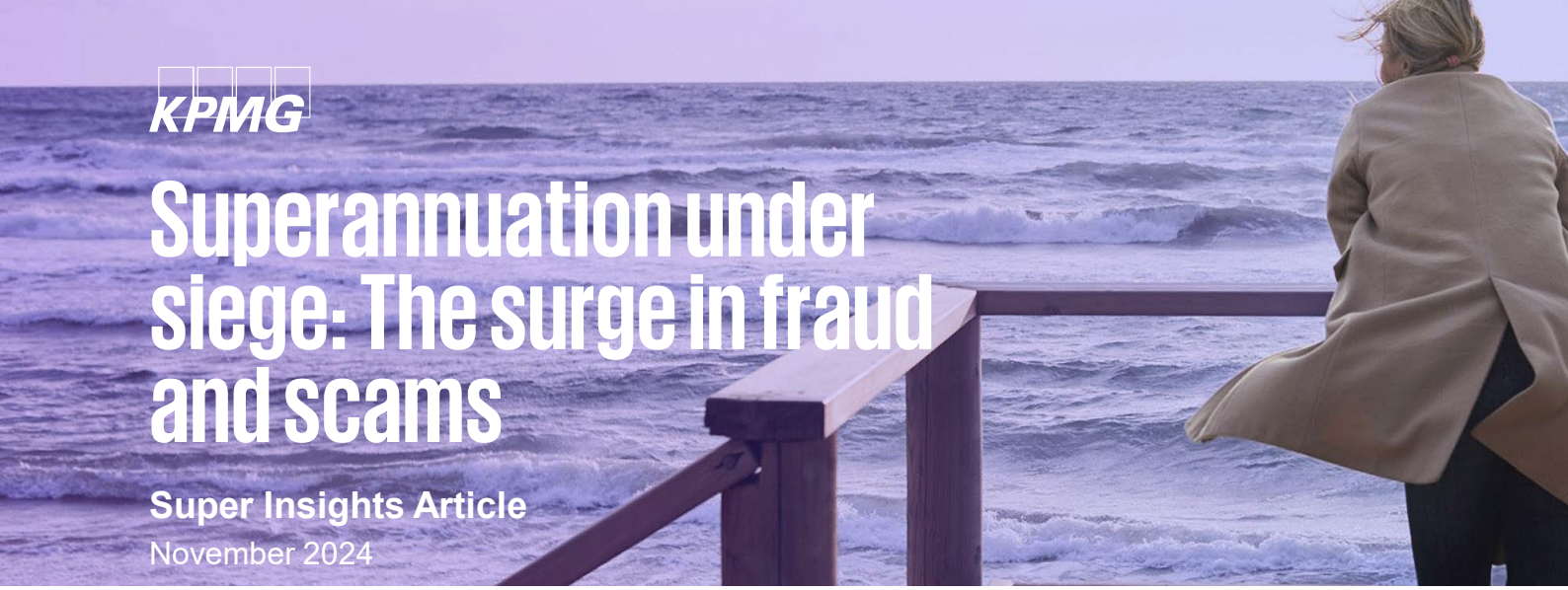

Superannuation under siege: The surge in fraud and scams

Super Insights Article
November 2024

The superannuation sector is currently grappling with an unprecedented surge in fraud and scams, as malicious actors increasingly target Australians' life savings. The Australian Securities and Investments Commission (ASIC) has sounded the alarm on this growing threat, highlighting that these attacks are no longer confined to individuals over the preservation age; working-age Australians are now also at risk.

The evolving threat

According to the Australian Competition and Consumer Commission's (ACCC) Targeting Scams Report published in April 2024, there were over 601,000 reported scams in 2023, marking an 18.5% increase from the previous year. These scams resulted in a staggering $2.74 billion loss to Australians, with investment scams alone accounting for $1.3 billion of this total. The stakes are particularly high for the superannuation sector, where low member engagement with retirement savings and the soaring total value of superannuation assets, which reached $3.9 trillion as of March 2024 according to the Association of Superannuation Funds of Australia, present an enticing opportunity for threat actors.

The rise of digital platforms for superannuation management has proven to be a double-edged sword for the industry. While these platforms offer convenience and ease of access, they also open up new avenues for exploitation by malicious actors. Identity takeovers and the misuse of Self-Managed Super Fund (SMSF) schemes have become favoured methods for criminals to access superannuation balances. After taking over an individual's identity, these actors can set up an SMSF without the individual's knowledge or lure members into transferring their superannuation into an SMSF with promises of "too good to be true" investment opportunities, only to siphon off these funds, leaving members with significant losses.

The integration of SMSF rollovers into the Australian Taxation Office's (ATO) SuperStream infrastructure is a positive move towards safeguarding retirement savings from unauthorised access. By sending notifications via email and/or text when the SMSF Verification Service (SVS) is utilised, some industry vulnerabilities are addressed. However, this measure alone does not guarantee protection against threat actors, particularly if a rollover has been executed before any unauthorised activity is detected. Therefore, it is crucial for superannuation funds and their trustees to remain vigilant and implement robust internal processes and controls to mitigate the risk of unauthorised access.

Increase in targeted attacks

Sue Bradford, KPMG Forensic Financial Services Lead Partner, has observed through the team's work across the market a marked increase in the targeting of financial services institutions by sophisticated threat actors. This surge in cybercrime activity is not only resulting in significant financial losses for customers and members, but it is also inflicting substantial reputational damage on these organisations.

In response to this growing threat, Sue underscores the critical need for financial services institutions to strengthen their financial crime, fraud and scams frameworks and embrace advanced technologies to mitigate emerging risks. "Organisations must adopt a proactive approach to fraud prevention and cybercrime

mitigation, ensuring they are prepared for the evolving landscape of financial threats," Sue advises. KPMG's approach focuses on helping clients navigate the complex and ever-evolving landscape of financial fraud and scams. Key areas of concern include:

- **Cybercrime targeting superannuation funds:** Increasingly, cybercriminals are targeting superannuation funds to gain access to large volumes of member data, which is then exploited for identity theft and fraudulent activity.
- **Phishing and investment scams:** The growing sophistication of phishing attacks and investment scams presents a significant risk, as attackers use deceptive tactics to trick members into disclosing sensitive personal information or transferring funds to fraudulent accounts.
- **The rise of deepfake technology:** The emergence of deepfake technology poses an additional challenge, as it enables the creation of highly convincing fake communications that appear to come from trusted sources. This innovation further complicates efforts to detect and prevent fraud.

In light of these evolving threats, regulatory bodies such as the Australian Securities and Investments Commission (ASIC) are increasing their focus on anti-scam practices within the financial services sector. ASIC's recent reports on the anti-scam measures of Australia's big four banks (Report 761) and other major financial institutions (Report 790) highlight the importance of robust scam prevention, detection, and response strategies.

Furthermore, the Australian Prudential Regulation Authority (APRA) has provided clear guidance on fraud risk management through its SPG 223 – Fraud Risk Management publication. This framework requires registrable superannuation entities (RSEs) to implement comprehensive systems for identifying, assessing, managing, mitigating, and monitoring material fraud risks that could impact their ability to fulfill obligations to beneficiaries. As financial services organisations face an increasingly complex threat landscape, Sue emphasises the importance of adopting a holistic, forward-thinking approach to fraud and financial crime risk management. By doing so, these institutions can better safeguard their members, protect their reputations, and ensure regulatory compliance in an environment of growing cyber risk.

How KPMG can help

KPMG's Forensic Fraud & Scam Risk Management team help clients achieve their fraud and scam prevention and mitigation objectives by:

- ensuring completeness of identification of fraud, scams and misconduct risk exposures, providing global insights gained from extensive experience in conducting high-profile fraud, corruption and misconduct investigations
- designing effective compliance programs and anti-fraud and scam controls
- optimising fraud and scam target operating models across Governance, People, Process, Technology and Member Experience
- implementation and advisory for fraud and scam detection technologies key to predicting, preventing, detecting and investigating fraud and scams.

Contact us

In an era where financial threats are of increasing concern and regulators are taking notice, KPMG can assist superannuation funds and trustees on their approach to fraud and scam risk management. Contact us to find out how we can help safeguard superannuation assets against the increasing risk of fraud and scams.

Sue Bradford
Partner, Forensic
+61 415 246 076
suebradford@kpmg.com.au

Harriet Tennent
Director, Forensic
+61 3 9288 5822
htennent1@kpmg.com.au

Robert MacKenzie
Associate Director, Forensic
+61 2 9273 5489
rmackenzie1@kpmg.com.au

Read our Superannuation Insights 2024

KPMG.com.au