

# AI and Financial Crime Risk in Australia's Superannuation Sector: A Strategic Imperative

---

### **Introduction: The Double-Edged Sword of AI in Superannuation**

Artificial Intelligence (AI) is transforming industries across the globe, and Australia's \$4.2 trillion superannuation sector is no exception. The technology offers unprecedented opportunities for efficiency, member engagement, and fraud and scam detection. However, the same tools that enable super funds to streamline operations are increasingly being weaponised by cybercriminals who are increasingly aware of the seemingly 'untapped' wealth Australians have through their default compulsory superannuation system.

AUSTRAC's 2024 National Risk Assessment warns that superannuation fraud remains a stable money laundering (ML) threat, compounded by digital onboarding and automation trends (AUSTRAC, 2024).

In recent years, AI-powered identity theft, synthetic document creation, and deepfake technology have created vulnerabilities that challenge even the most sophisticated fraud prevention systems. For superannuation funds, the stakes could not be higher: stolen identities and fraudulent withdrawals don't just erode member savings, they undermine the integrity of the entire Australian retirement system.

According to AUSTRAC's 2022 Superannuation Threat Update, technological advances have increased the prevalence of using falsified documentation to access payments, for example Services Australia confirmations supporting financial hardship claims, falsified birth certificates/death certificates/medical certificates supporting early release payments etc.

AI-driven automation streamlines processes, reducing friction for members and funds alike. However, criminals leverage these same capabilities to perpetrate identity fraud, create synthetic documents, and deploy deepfake technology. These tactics erode trust and expose systemic vulnerabilities (Infocentric, 2025).

### **AI as a Tool for Cybercriminals**

#### **1. Stolen Identities at Machine Speed**

AI-driven phishing campaigns, capable of personalising attacks through natural language processing, have made it easier than ever for criminals to harvest personal data. With large datasets from breaches (including driver's licence numbers, Medicare information, and bank details), attackers can automate identity theft attempts, scaling beyond what was possible with manual methods.

## 2. Fake and Tampered Documents

Generative AI models can produce hyper-realistic identification documents that pass casual inspection. Tools can replicate official Australian documents such as passports, driver's licences, bank statements, utility bills and come complete with matching metadata and security features. Where once poor image quality betrayed a fake, AI now ensures pixel-perfect forgeries.

**3. Deepfake Impersonations:** Voice and facial recognition systems, increasingly used for member verification, are vulnerable to AI-generated deepfakes. 'Using different methods and tools, it is possible to combine, or morph, the faces of the person the passport actually belongs to and the person(s) wanting to obtain a passport illegally. This method may increase the chance that the photo in a forged document passes any identity checks including those using automated means (facial recognition systems)'. (Europol, 2022).

## Why Detection Is Harder

Legacy fraud detection systems rely on rule-based checks and anomaly spotting. Modern AI-generated fakes mimic statistical patterns of legitimate data, embedding authentic noise and compression artefacts to evade forensic scrutiny. Synthetic identities, or fabricated personas built from fragments of real data, further complicate detection (MIT Media Lab, 2021).

## Regulatory Awareness

Regulators have acknowledged these emerging risks:

**AUSTRAC** (Australian Transaction Reports and Analysis Centre) has warned of the growing use of AI and automation in money laundering. In its recent guidance, AUSTRAC highlighted the risks of identity fraud in financial services and urged entities to adopt stronger Know Your Customer (KYC) and transaction monitoring procedures.

**APRA** (Australian Prudential Regulation Authority) has increased its focus on operational resilience and cyber risk in the superannuation sector. Under CPS 234 – Information Security, APRA mandates that regulated entities maintain robust controls to protect sensitive data and respond effectively to security incidents. This includes the expectation that boards understand emerging risks, such as AI-powered fraud and to allocate resources accordingly.

**ASIC** (Australian Securities and Investment Commission) requested Superannuation Trustees in its letter 29 January 2025 to uplift scam management practices "or risk becoming a soft target" ... "Across the whole financial system, technological innovations and data breaches—including breaches involving identity documents—continue to heighten the risk of scams and fraud."

## Industry Changes and ML/TF Risk

Digitisation and AI-driven onboarding have streamlined member experiences but introduced vulnerabilities. Staging accounts are increasingly used by criminals to open accounts and later launder illicit funds. Fraudulent rollovers exploit weak identity verification, while synthetic identities bypass traditional KYC checks. AUSTRAC predicts pure cybercrime will pose an increasing ML threat over the next three years, accelerated by AI (AUSTRAC, 2024).

## Do Industry Changes Promote or Discourage ML/TF?

Technological innovation enhances operational efficiency but inadvertently promotes ML/TF unless counterbalanced by stringent controls. Automated onboarding and remote verification

reduce friction but weaken assurance. Conversely, AI can discourage ML/TF when deployed for anomaly detection and behavioural biometrics. The net effect depends on governance maturity and investment in AML/CTF resilience (FSC, 2025).

To mitigate ML/TF risk and AI-enabled fraud, super funds should adopt a proactive, multi-layered approach:

### **1. Deploy AI Against AI**

Use machine learning models trained to detect synthetic media, deepfakes, and AI-generated documents. These systems can identify subtle artefacts invisible to the human eye.

### **2. Implement Multi-Modal Verification**

Avoid reliance on a single verification channel. Combine biometric checks with independent data validation, behavioural analytics, and physical document inspection where possible.

Superannuation Funds should utilise proof-of-life biometrics software that uses a combination of techniques to ensure the person is real and not a photo or video being presented to the camera. It also detects where a member is being coached by someone else in the room. “Biological signals tries to detect deepfakes based on imperfections in the natural changes in skin colour that arise from the flow of blood through the face” (Infocentric, 2025)

### **3. Enhance KYC with Real-Time Government Data Matching**

Integrate systems with authoritative sources (e.g., Document Verification Service) to cross-check IDs against live government records.

### **4. Continuous Staff Training**

Fraud prevention teams should receive regular updates on AI threat trends, including hands-on training in recognising deepfakes and synthetic identities.

### **5. Regulatory Collaboration**

Work closely with and lobby to AUSTRAC, ASIC and APRA to share intelligence on emerging fraud methods and co-develop sector-wide response protocols, for example have all financial institutions able to access the scam-safe accord and the Australian Financial Crimes Exchange, particularly as APRA regulated super funds do not have the means to develop their own systems and every dollar spent needs to meet members best financial interest duty requirements of s52(2)(c) Superannuation Industry (Supervision) Act 1993 (Cth).

### **6. Incident Simulation and Stress Testing**

Conduct regular red-team exercises that simulate AI-enabled fraud attempts to identify weaknesses before criminals exploit them. (Infocentric, 2025; FSC, 2025).

## **The Strategic Imperative**

The superannuation industry operates on trust. With retirement savings locked away for decades, members expect security from theft and fraud. As AI evolves, complacency becomes the most dangerous vulnerability. Boards and executives must embed resilience into every layer of operations, recognising AI as both a threat and a tool for defence. “As generative AI (GenAI) rapidly permeates businesses, expanding the attack surface, these (data breach) expenses will soon become unsustainable, compelling business to reassess security measures and response strategies. To get ahead, businesses should invest in new AI-driven defences and develop the

skills needed to address the emerging risks and opportunities presented by GenAI.” (Ponemon Institute, 2022).

## Conclusion

AI’s role in superannuation is a paradox. It offers powerful capabilities to protect member funds, yet it arms criminals with the means to bypass traditional defences. The challenge for Australia’s superannuation sector is clear: embrace AI-driven countermeasures, work hand-in-hand with regulators, and embed resilience into every layer of operations.

In an AI-driven threat environment, complacency is the most dangerous vulnerability of all.

## References

APRA (2023) *CPS 234 – Information Security*

[https://www.apra.gov.au/sites/default/files/cps\\_234\\_july\\_2019\\_for\\_public\\_release.pdf](https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf)

ASIC (2025) <https://www.asic.gov.au/about-asic/news-centre/news-items/asic-calls-out-superannuation-trustees-for-weak-scam-and-fraud-practices/>

ASIC Scam prevention framework <https://download.asic.gov.au/media/3r2bnrif/20241220-submission-no-5-scams-prevention-framework-bill-2024.pdf>

AUSTRAC (2024) *National ML/TF Risk Assessment*

<https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf>

AUSTRAC (2022) *Australia’s superannuation sector threat update 2022*

<https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/australias-superannuation-sector-threat-update-2022>

Australian Government, Document Verification Service <https://www.idmatch.gov.au/>

Europol (2022) *Facing the challenge of deepfakes*

[https://www.europol.europa.eu/cms/sites/default/files/documents/Europol\\_Innovation\\_Lab\\_Facing\\_Reality\\_Law\\_Enforcement\\_And\\_The\\_Challenge\\_Of\\_Deepfakes.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf)

Financial Services Council (FSC), *The AI Advantage Report* <https://fsc.org.au/resources/2859-fsc-ai-advantage-report-unlocking-a-decisive-decade-for-superannuation-investment-management/file>

Infocentric, *AI and Sensitive Data in Superannuation* (2025)

<https://www.infocentric.com.au/2025/08/21/ai-and-sensitive-data-in-superannuation/>

MIT Media Lab (2021) *Detecting AI-generated synthetic media*

<https://www.media.mit.edu/projects/detect-fakes/overview/>

Ponemon Institute (2022) *The Cost of Cybercrime in Financial Services*

<https://www.financierworldwide.com/fw-news/2024/8/1/data-breaches-cost-fs-608m-in-2024-reveals-new-report>

Copyright © Elizabeth Swan.

Published by the Australian Compliance Institute with permission. This work may not be reproduced or republished without prior written permission from the copyright holder.