

ANNEX A: INDUSTRY CHANGE & RISING AML RISK

The inherent vulnerability of the banking sector to Money Laundering (“ML”) and Terrorism Financing (“TF”) is well understood and widely documented. As Australia faces heightened scrutiny and potential Financial Action Task Force (“FATF”) Grey Listing, the banking industry is under increasing pressure to demonstrate not only compliance with global AML/CTF standards but leadership in prevention and resilience.

This article evaluates the changes reshaping ML/TF risk in the Australian banking environment, the implications—both positive and negative—of these changes, and the countervailing measures necessitated by the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 (“Amendment Act”). It draws on contemporary research, including AUSTRAC’s 2024 National Risk Assessments and international reporting, to form an informed judgement on the evolving risk landscape.

Regulatory Change

To align with FATF standards, the Amendment Act strengthens the risk-based, outcomes-focused obligations imposed on reporting entities. It requires a more granular assessment of ML/TF and proliferation financing risks based on each business’s size, nature and complexity. Enhanced requirements for customer due diligence (CDD), enhanced customer due diligence (ECDD), technology-enabled controls, governance, and ongoing monitoring set a higher compliance benchmark across all sectors.

These reforms discourage ML/TF activity by elevating detection capability and increasing the cost of exploitation for criminals.

However, more rigorous processes introduce operational friction, which may clash with customer expectations for speed and convenience.

Overall, the regulatory uplift materially strengthens Australia’s ability to detect, deter and disrupt ML/TF, but it also requires a significant operational and cultural shift across the industry—particularly for smaller institutions.

Customer Expectations and Demographic Shifts

Modern consumers expect seamless onboarding, instant payments and frictionless access to credit. While these expectations shape competitive strategies across mutuals and major banks alike, they also expand exposure to identity theft, synthetic identities, and cross-border anonymity.

AUSTRAC’s Money Laundering National Risk Assessment (2024) identifies cash as ‘the most commonly seized asset in criminal confiscation’, confirming its continued high-risk profile. Although the government has mandated the ongoing acceptance of cash for essential purposes, the visibility of reporting thresholds (e.g., \$10,000 TTRs, SMRs, as detailed on AUSTRAC’s website and strongly prioritised in The Act) can inadvertently encourage criminals to pivot into more anonymous or digital channels.

Increasingly digital customer interactions create both speed and complexity, enabling ML/TF typologies such as mule accounts, layered transfers, and anonymised payment flows.

ECDD requirements under the Amendment Act (Part 2, Divisions 2–4) mitigate this risk, improving transparency around beneficial ownership (s36 of The Act), PEPs (s39A of The Act), source of funds, and identity integrity.

The Amendment Act places a strong stance on reporting entities to undertake Customer Due Diligence (“CDD”) (s32-33 of The Act) and Enhanced Customer Due Diligence (“ECDD”) (s37 of The Act). As demographics change, jurisdictions become more fluid (with online access to products and services), structures can be complicated and beneficial ownership blurred (via Companies and Trusts etc), promotion of online account openings, along with existing Identity Theft crimes, the regulatory changes require entities to ensure they know who their customers are, the sources of wealth, beneficial ownerships, Politically Exposed Persons (“PEPs”), sanction evaders via shell companies, decreasing exposure to ML/TF activity.

Customer-centric innovation increases ML/TF exposure, but stringent CDD/ECDD obligations significantly counterbalance this risk when applied consistently and supported by trained staff. The net effect is risk-neutral to risk-reduced, depending on implementation maturity.

Environmental and Technological Change

Digital banking, FinTech partnerships, real-time payments and cross-border platforms have transformed the speed and complexity of financial flows - resulting in easily accessible funds exchanges and introducing anonymity. Simultaneously, emerging technologies—AI, machine learning, behavioural analytics—offer unprecedented detection potential. Advancing development of digital currencies and promoting peer-to-peer exchanges through block chains, continue to challenge traditional risk detection methods in the financial services industry.

Positive impacts:

- Improved anomaly detection
- Real-time alerting
- Automated pattern recognition
- Stronger identification of mule activity

Negative impacts:

- Criminals increasingly use AI, malware-as-a-service, and automated scripts to scale fraud, cybercrime, and ML techniques.
- Faster payments reduce the window for intervention and increase the efficiency of layering.
- Third-party platforms blur transaction visibility and accountability.

The Amendment Act’s expansion to Tranche 2 entities (effective 1 July 2026) strengthens oversight across non-financial entities —closing loopholes commonly exploited by ML/TF networks.

Technological evolution simultaneously empowers reporting entities and criminals. Net risk reduction is entirely dependent on governance, oversight, and responsible AI adoption. Technology without strong human supervision creates vulnerabilities rather than resilience.

The AML/CTF Act amendments, in conjunction with the COBA Scams Accord – in the mutual banking space – requires enhance transaction monitoring, to counteract the expected increased activity and layering of transactions.

Data Ecosystems and Privacy Risk

Open banking and mandatory data sharing improve transparency and cross-institution collaboration to detect, deter and disrupt. Reporting to AUSTRAC, and collaboration with AUSTRAC, ASIC and IDCare, enhances the collective intelligence available to detect ML/TF patterns.

However, data breaches remain one of the fastest-growing enablers of ML/TF (Optus, 2022, and Latitude, 2023), feeding identity theft, fraud, account takeovers and mule recruitment. Expanded datasets broaden the attack surface and heighten third-party risk.

Data sharing improves collective AML/CTF capability but also exposes entities to increased cyber risk. Robust data governance, breach resilience and third-party oversight are essential countervailing measures.

Geopolitical Instability

Geopolitical disruption—sanctions, conflict, poverty, economic downturns—directly shapes ML/TF behaviour. Criminal networks and terrorist groups adapt faster than regulatory systems.

Historical and contemporary examples illustrate this evolution:

- Triads and Macau junket operations in the 1990s
- Suncity and transnational organised crime networks
- POGO operations in the Philippines
- Scam compounds in Myanmar
- Global rise in cyber-enabled “pig-butchering” scams (Europol, 2025)

AUSTRAC’s 2024 Terrorism Financial National Risk Assessment and FATF’s Comprehensive Update on Terrorist Financing Risks (2025) highlight increasingly sophisticated cyber-extortion, sanction evasion and decentralised financial flows.

Geopolitical instability significantly increases ML/TF risk, pushing criminals toward more complex, cross-border, technology-enabled channels. This environment necessitates proactive adaptation—reactive compliance is no longer sufficient.

Countervailing Change

Across all areas, the industry must adopt coordinated countermeasures, including:

- Enhanced transaction monitoring and analytics (s83 of The Act)
- Stronger governance, accountability and staff capability
- Proactive detection frameworks (not relying on reactive attempts)
- Industry-wide initiatives such as the COBA Scams Accord i.e. national Confirmation of Payee
- AI tools with robust human oversight
- Strengthened data protection and third-party risk management
- Intelligence-sharing partnerships across sectors and jurisdictions

These countervailing measures are essential to maintain resilience, not optional.

Change is not inherently positive or negative—the risk outcome is determined by how the industry responds.

The Amendment Act elevates expectations and sets a stronger national standard for AML/CTF resilience. While evolving technologies, customer behaviours, and geopolitical pressures increase exposure to ML/TF, the regulatory uplift, collaborative frameworks, and cross-sector obligations provide a powerful counterbalance – forcing a cohesive cohort of reporting entities.

If the cohort embrace proactive governance, intentional monitoring and responsible technology adoption (of course, encouraged by increased penalties for entity non-compliance), these changes will discourage ML/TF activity, strengthen national security, and reduce Australia's vulnerability to FATF scrutiny. Failure to do so, however, risks widening the gap between criminal innovation and regulatory capability.

The path forward requires vigilance, collaboration and a commitment to continuous evolution—because ML/TF risks will continue to adapt, and Australia's response, not just the financial services sector, must adapt faster.

Bibliography:

- <https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/03/top-geopolitical-risks-2025-web.pdf>
- <https://www.austrac.gov.au/business/core-guidance/amlctf-programs/enhanced-customer-due-diligence-ecdd-program>
- <https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/source-funds-and-source-wealth>
- <https://www.austrac.gov.au/business/legislation/amlctf-act>
- <https://www.austrac.gov.au/optus-data-breach-working-our-reporting-entities>
- <https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf>
- <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>
- <https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html>
- <https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/anti-money-laundering-and-counter-terrorism-financing/anti-money-laundering-and-counter-terrorism-financing-amendment-act/changes-to-aml-ctf-program-requirements?TermStoreId=1cafda66-8aac-4a45-95fa-3e03872913b6&TermSetId=f8e5d72d-750a-4274-8b42-2c1fc70fdd2d&TermId=d3163466-c0db-4cc3-8b2c-8c418fb853c3>
- <https://www.legislation.gov.au/C2006A00169/latest/text>
- <https://minister.homeaffairs.gov.au/ClareONeil/Pages/latitude-financial.aspx>
- <https://ministers.treasury.gov.au/ministers/daniel-mulino-2025/media-releases/mandating-cash-acceptance-step-closer>
- <https://www.austrac.gov.au/business/core-guidance/amlctf-programs/enhanced-customer-due-diligence-ecdd-program>
- <https://www.europol.europa.eu/media-press/newsroom/news/launch-of-eu-serious-and-organised-crime-threat-assessment-2025>
- <https://windward.ai/knowledge-base/the-9-biggest-geopolitical-and-security-trends-this-year/>
- Australian Compliance Institute Workbook, *Module One: FNS80020 – Graduate Certificate In Anti-Money Laundering and Counter Terrorism Financing* (2025)
- Australian Compliance Institute Workbook, *Module Two: FNS80020 – Graduate Certificate In Anti-Money Laundering and Counter Terrorism Financing* (2025)
- Australian Compliance Institute Workbook, *Module Three: FNS80020 – Graduate Certificate In Anti-Money Laundering and Counter Terrorism Financing* (2025)

Copyright © Alishia Carswell.

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