Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026

1. Introduction

I make this submission in my personal capacity.

I support the objective of protecting Australia's financial system and wider community from money laundering, terrorism financing, serious organised crime, sanctions evasion and other illicit financial activity. These are legitimate and serious public-interest concerns.

However, anti-money laundering and counter-terrorism financing powers should be designed with precision. They should target demonstrable financial-crime risk without creating unnecessary collateral harm to legitimate privacy, cybersecurity, innovation, access to financial services, or lawful use of emerging technologies. The Committee's inquiry concerns the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026. The Committee's published summary states that the Bill would enable the Chief Executive Officer of AUSTRAC to restrict or prohibit reporting entities from using high-risk mechanisms to provide designated services; amend the meaning of financing of terrorism to reference new offences for financing a state sponsor of terrorism; and make technical amendments (Parliament of Australia, 2026a).

My submission focuses on safeguards for the proposed high-risk mechanism power and related technology-policy issues.

2. Core position

The Bill should proceed only with clear safeguards ensuring that any restriction or prohibition power is:

- necessary, not merely convenient;
- proportionate to a clearly identified financial-crime risk;
- technically precise;
- based on objective criteria;
- targeted at conduct, custody, control, transaction patterns and demonstrable misuse;
- accompanied by procedural fairness where possible;
- subject to review, reporting and oversight;
- careful not to treat privacy-preserving technology as inherently suspicious.

The correct regulatory question should not be, "Can this mechanism be misused?" Almost every financial, communications or cybersecurity tool can be misused. The better question is, "Does this mechanism, in its actual design and use, create a clearly demonstrated and material money laundering, terrorism financing or serious-crime risk that cannot be managed through less restrictive controls?"

3. High-risk mechanisms should be defined by objective risk factors

Any power to restrict or prohibit a "high-risk mechanism" should be supported by clear statutory or published criteria.

Relevant criteria may include:

- whether the mechanism materially reduces the ability of a reporting entity to conduct customer due diligence;
- whether it enables rapid movement of funds at scale without meaningful controls;
- whether it has a demonstrated pattern of serious criminal misuse;
- whether the reporting entity has custody or control over customer value;
- whether the mechanism prevents or frustrates transaction monitoring;
- whether less restrictive controls, such as enhanced due diligence, transaction limits, monitoring, reporting, or targeted conditions, would sufficiently mitigate the risk.

The power should not be used merely because a technology is new, difficult to understand, privacy-preserving, decentralised, encrypted or politically controversial. Risk should be assessed by evidence and operational reality, not by category-level suspicion.

4. Privacy-preserving technology should not be treated as inherently suspicious

Privacy is not the same thing as criminal concealment. Encryption, anonymity, pseudonymity, self-custody, privacy-preserving identity methods, cybersecurity controls and data-minimising technologies can serve legitimate purposes.

Individuals and businesses may use privacy-preserving technologies to protect themselves from fraud, stalking, doxxing, identity theft, commercial surveillance, data breaches, abusive relationships, targeted crime or political intimidation. Treating privacy itself as a risk factor would be a serious policy error.

The United Nations Special Rapporteur on freedom of opinion and expression has recognised that encryption and anonymity enable privacy and freedom of expression online and deserve strong protection (Special Rapporteur on freedom of opinion and expression, 2015). While AML/CTF systems legitimately require regulated entities to manage financial-crime risk, those systems should not collapse privacy-preserving design into suspicion.

5. Necessary, not merely convenient

A restriction or prohibition should be available only where it is necessary to address a legitimate objective and no less restrictive measure would reasonably manage the risk.

Australian Government guidance on human rights scrutiny states that a limitation on rights should pursue a legitimate objective, be necessary to achieve that objective, be rationally connected to that objective, and use means no more restrictive than required (Attorney-General's Department, n.d.).

That standard matters here. A high-risk mechanism restriction may affect access to services, business operations, lawful technology use, innovation, financial inclusion, privacy and competition. The mere fact that a prohibition would make enforcement easier should not be enough.

Before a restriction or prohibition is imposed, AUSTRAC should consider whether the risk can be addressed through:

- enhanced due diligence;
- transaction limits;
- additional reporting;
- targeted compliance conditions;
- improved monitoring;
- sector-specific guidance;
- customer-risk controls;
- time-limited restrictions;
- narrower restrictions on specific uses rather than whole technologies.

6. Procedural fairness and review

Where a restriction or prohibition affects a reporting entity, class of entities, technology provider or class of users, the framework should provide procedural safeguards to the greatest extent consistent with operational needs.

Those safeguards should include:

- written reasons, except where genuinely operationally sensitive;
- a public statement of the general risk basis, where possible;
- notice to affected entities before a final decision, unless urgency makes that impracticable;
- an opportunity to make submissions;
- access to merits review or independent review;
- time limits or periodic review of the restriction;
- publication of de-identified or aggregated information about the use of the power.

Where classified or sensitive intelligence is involved, affected parties should still receive the maximum possible unclassified summary of the case against the mechanism. Secret evidence should not become a substitute for accountable decision-making.

7. Avoiding overcollection and unnecessary surveillance

The Bill should not indirectly encourage reporting entities to collect more personal information than is reasonably necessary.

The Australian Privacy Principles provide that APP entities must only collect personal information that is reasonably necessary for their functions or activities, and agencies may collect personal information that is directly related to their functions or activities (OAIC, 2019). AML/CTF compliance should not become a general justification for excessive identity collection, indefinite data retention, unnecessary biometric collection or broad monitoring unrelated to actual financial-crime risk.

A strong AML/CTF regime should be risk-based and evidence-based. It should not normalise surveillance-by-default.

8. Small entities and implementation burden

Where the Bill affects smaller reporting entities, implementation should be accompanied by clear, practical guidance.

Many small entities do not have in-house legal, compliance, cybersecurity or financial-crime teams. Poorly explained obligations may lead to defensive overcompliance, unnecessary service refusal, excessive data collection or blanket de-risking of customers and technologies.

The Committee should recommend that AUSTRAC publish practical guidance explaining:

- what factors may make a mechanism high-risk;
- what mitigations may be accepted as alternatives to prohibition;
- what evidence AUSTRAC will consider;
- how affected entities can seek clarification;
- how restrictions will be reviewed;
- how privacy and data minimisation should be preserved.

9. Recommendations

I recommend that the Committee support the Bill only with safeguards ensuring that:

1. “High-risk mechanism” decisions are based on objective, published criteria where possible.
2. Restrictions or prohibitions are necessary, proportionate and rationally connected to a clearly identified financial-crime risk.
3. Privacy-preserving technology is not treated as inherently suspicious merely because it can be misused.
4. AUSTRAC considers less restrictive alternatives before imposing a prohibition.
5. Affected entities receive reasons, notice and an opportunity to respond where practicable.
6. Restrictions are time-limited or subject to periodic review.
7. Review rights are available, including where decisions materially affect businesses, users or technology providers.
8. AML/CTF compliance does not encourage unnecessary personal-data collection, biometric collection, indefinite retention or surveillance-by-default.
9. AUSTRAC publishes practical guidance for smaller entities and technically complex mechanisms.
10. The use of the restriction/prohibition power is reported publicly in de-identified or aggregated form.

10. Closing

Australia needs an AML/CTF framework capable of responding to evolving financial-crime threats. However, the framework should remain precise, risk-based and rights-compatible.

The strongest system is not one that treats every privacy-preserving or emerging technology as suspect. The strongest system is one that identifies real risk, applies proportionate controls, preserves lawful privacy and innovation, and gives affected people and entities meaningful procedural safeguards.

REFERENCES

Attorney-General's Department (n.d.) Permissible limitations. Available at: https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets/permissible-limitations

Office of the Australian Information Commissioner (2019) Chapter 3: APP 3 Collection of solicited personal information. Available at: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information

Parliament of Australia (2026a) Review of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AMLCTFBILL2026

Parliament of Australia (2026b) Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026. Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7448

Special Rapporteur on freedom of opinion and expression (2015) Report on encryption, anonymity and human rights, A/HRC/29/32. Available at: https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework