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

Parliamentary Joint Committee on Intelligence and Security

I make this submission to the Parliamentary Joint Committee on Intelligence and Security in relation to its review of the Anti-Money Laundering and Counter Terrorism Financing Amendment Bill 2026.

The Bill is important. Money laundering, terrorism financing, organised crime, foreign interference, sanctions evasion, scam networks, cyber theft and the abuse of financial infrastructure are serious public harms. Australia needs a strong financial crime framework.

However, the seriousness of the threat does not answer the harder question. The harder question is whether the legal architecture proposed by the Bill is precise, proportionate, transparent, reviewable and capable of principled application.

The Committee should not ask only whether high risk mechanisms are dangerous. Some are. The Committee should ask who decides, on what evidence, under what safeguards, with what accountability, and with what effect on cash, public access, communities, lawful commerce, financial sovereignty and public trust.

The Committee's own public material states that the Bill would enable the AUSTRAC CEO 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. It also states that the inquiry is concerned with a rapidly changing financial crime landscape.

That description should guide the Committee's task. The financial crime landscape is changing, but not always in the way political debate suggests. The danger is not simply cash. The danger is a private, digital, opaque and increasingly automated financial architecture that allows value to move at speed, across borders, through institutions and platforms, often beyond practical recovery.

Cash should not be made the scapegoat for that architecture.

The Bill should be judged by good public purpose, not by national security branding

I support the objective of preventing money laundering, terrorism financing and serious financial crime. But national security language should not be allowed to suspend ordinary legislative discipline.

Parliament should apply a good public purpose test. In this context, good public purpose means a financial system that protects the community, preserves public access to lawful money, prevents serious crime, supports financial inclusion, maintains human scrutiny, protects national sovereignty and ensures that coercive powers are used only where necessary, proportionate and reviewable.

The Committee should also apply a floor and ceiling test. The Commonwealth should build a floor that all can stand on, including access to cash, banking, payment services and human assistance. It should also regulate a ceiling against disproportionate private power, regulatory capture, opaque financial structures, predatory digitisation and excessive discretion.

On those tests, the Bill requires strengthening.

The Committee should not accept a simple story in which more power automatically means more safety. Recent Australian experience shows that regulators can under enforce, over rely on private institutions, resist scrutiny and become too close to the sectors they regulate. The Senate Economics References Committee report into ASIC found that corporate law was under enforced in Australia, that ASIC took no further action on most public misconduct reports in 2021 to 2022, that only a small fraction of matters was investigated, and that ASIC investigation and enforcement decisions were opaque and difficult to scrutinise.

That finding is not about AUSTRAC directly. But it is relevant. It shows why Parliament should not grant broad regulatory discretion on trust alone. Powers must be designed for the real world, including institutional defensiveness, capture risk, political pressure, private sector influence and future misuse.

Cash is a strength, not a weakness

My major concern is that this Bill could be used, directly or indirectly, to further degrade cash.

That would be a serious mistake.

Cash is increasingly portrayed as a financial crime problem. The example often used is cash being converted into cryptocurrency through an ATM. But that example should be understood properly. The problem is not that cash exists. The problem is that cash is being converted through a high-risk mechanism into a digital asset pathway that may be difficult for ordinary people, banks, regulators and law enforcement to understand, control or reverse.

AUSTRAC itself describes crypto ATMs as allowing a customer to convert cash to cryptocurrency, which is then sent to a digital wallet without interacting with another person. It identifies risks including difficulty identifying the true ownership and control of the wallet, third party control of wallets, anonymous receipt of cryptocurrency, offshore access to value, and large volumes of transactions in short periods. But the same end risk can arise when digital bank funds are converted into cryptocurrency through an exchange, payment platform or other digital asset channel. In both cases, the critical point is not whether the value began as cash or as bank deposit money. The critical point is that value is converted into a crypto pathway where ownership, control, destination and recovery may become far less visible. The Bill should therefore target dangerous conversion mechanisms, not cash itself.

That does not prove that cash is the weakness. It proves that the conversion architecture is the weakness.

Cash is physical. Cash creates presence. Cash creates friction. Cash requires a person to appear somewhere, handle money, be observed and interact with a service channel. In a staffed bank branch, that interaction can reveal risk. A trained worker may notice distress, confusion, coercion, unusual urgency, a customer acting out of character, or a third party coaching the customer.

That kind of human scrutiny is not a weakness in the AML and CTF system. It is one of the remaining strengths.

By contrast, the private banking system has spent years pushing customers into remote, digital and automated channels while withdrawing branches, cash services and face to face assistance. Governments and regulators have largely watched this occur with inadequate resistance, accepting bank driven digitisation as inevitable while failing to protect the public functions that branches and cash services perform. That shift may

reduce costs for banks, but it removes human scrutiny and pushes vulnerable people into systems where identity can be hidden, stolen, manipulated or manufactured.

Online catfishing and scam conduct demonstrate the weakness of digital identity. A scammer can hide behind devices, false profiles, synthetic identities, stolen credentials, remote accounts, encrypted messages and psychological manipulation. Mrs Jones walking into her local bank branch cannot hide in the same way. She is physically present. She can be seen. She can be spoken to. She can be protected before the harm occurs.

The Committee should therefore reject any suggestion that cash degradation is an AML or CTF solution. Removing cash does not remove criminal intent. It may simply remove one of the few points where the financial system still has physical visibility.

The proper target is not cash. The proper target is dangerous conversion architecture, weak digital onboarding, opaque crypto pathways, remote manipulation, under regulated payment channels, branch withdrawal, debanking, poor bank conduct and private institutions externalising risk onto the public.

Cash protection or cash containment

The Committee should also consider the recent cash acceptance debate because it shows how cash can be eroded while being rhetorically protected.

The Commonwealth has presented the cash acceptance regulations as a protection for cash users. On one level, requiring some supermarkets and fuel retailers to accept cash is better than no protection at all. But the limited design of the mandate exposes the deeper problem.

Treasury described the mandate as applying to fuel and grocery retailers for in person transactions of 500 dollars or less between 7 am and 9 pm, with small businesses under 10 million dollars exempt and a review after three years. The ACCC guidance is even clearer. It states that most businesses can choose whether they accept cash, and that the cash acceptance rules apply only to some supermarkets and fuel retailers. The rules do not apply to any other industries.

That is not a general cash protection framework. It is a narrow retail exception.

The effect is that Parliament can say cash has been protected while most of the economy remains legally free to refuse it. Even the institutions most obviously associated with money, namely banks, are not placed under a general obligation by these rules to maintain staffed cash access, accept cash over the counter, or preserve physical cash services for the public.

That is a serious defect.

Nor are pharmacies, medical services, public transport, utilities, government shopfronts, hardware stores, post office services beyond existing bill payment arrangements, or many other essential everyday services captured by the scheme as general cash service providers. Senator David Pocock made a similar criticism in the Senate debate, saying the mandate declares only large supermarkets and petrol stations essential and that this does not cut it.

This matters directly to the present Bill. If cash is treated as a risk factor in AML and CTF policy while the broader law permits cash refusal across most of the economy, then the Bill may become another step in the managed degradation of cash. The public is told cash is protected because it can be used at some supermarkets and service stations during specified hours and below a specified transaction limit. Meanwhile, branches close, cash services shrink, digital payments expand, and the legal duty to accept or provide cash remains narrow.

That is cash containment dressed as cash protection.

A serious public cash framework would not stop at supermarkets and service stations. It would recognise cash as lawful public money and as a resilience, inclusion and financial integrity tool. It would require banks to maintain reasonable physical cash access. It would preserve staffed service points. It would ensure that people can pay for essential services, government services, medical needs, utilities, transport and basic household goods in cash. It would also distinguish between cash itself and particular high risk conversion mechanisms, such as crypto ATMs, that turn visible physical money into less transparent digital flows.

The Committee should therefore be careful that this Bill does not reinforce the same error. Cash should not be treated as the suspect mechanism. The suspect mechanism is the architecture that removes human scrutiny, forces people into digital channels, and then blames cash when digital conversion points are abused.

Branch closures weaken financial crime prevention

The degradation of cash cannot be separated from bank branch closures.

A financial crime framework that relies on digital surveillance after money has moved is inferior to one that preserves human scrutiny before money leaves. The Senate inquiry into bank closures in regional Australia recommended that the Australian Government recognise access to financial services as an essential service and guarantee reasonable access to cash and financial services for all Australians. It also recommended an expert panel to investigate a publicly owned bank, including options associated with the Australia Post branch network.

That work is directly relevant to this Bill.

If Parliament is serious about AML and CTF, it should not permit the same private banks that reduce branches, reduce cash services and push customers online to then portray cash and in person banking as the problem. That gets the risk backwards.

A staffed local branch is not merely a commercial service. It is a point of public protection. It is where unusual behaviour can be noticed, where a vulnerable customer can be assisted, where a scam can be interrupted, where identity can be physically checked, and where transaction risk can be assessed before irreversible harm occurs.

The Bill should therefore contain an express safeguard that the high-risk mechanism power must not be used directly or indirectly to justify further restriction of lawful cash access, branch closures, or removal of staffed cash services.

Digital value leaving Australia is a greater modern risk

The Committee should consider whether Australia needs a jurisdictional digital payments firewall for high risk inbound and outbound digital value flows.

The logic is straightforward. The point at which digital value leaves the Australian jurisdiction is often the last realistic point of control. Once funds move offshore into foreign accounts, foreign platforms, crypto wallets, stablecoin rails, mule networks or opaque digital asset structures, recovery may be difficult or impossible.

That means the law should focus more heavily on pre exit scrutiny, not merely after the fact reporting.

This is another reason cash should not be miscast as the central weakness. Cash is physical. It creates friction. It requires presence, movement, storage and observation. Digital value can leave the country at speed, at scale and through channels that may conceal the real actor.

If the concern is modern financial crime, the obvious risk is not Mrs Jones withdrawing cash at a local branch. The obvious risk is Mrs Jones being manipulated through a digital scam and induced to send funds offshore before any human being has intervened.

A jurisdictional digital payments firewall should not mean stopping every ordinary transaction. It should mean mandatory, risk-based scrutiny at the point where digital value enters or leaves Australia. Higher risk transfers should trigger stronger identity checks, payee verification, scam warnings, cooling off periods, human review, source of funds checks, destination checks, beneficial ownership checks and temporary holds where necessary.

That framework should apply to banks, remitters, digital asset exchanges, payment platforms and other reporting entities that enable cross jurisdiction digital value movement. Its purpose should be to prevent irreversible loss, money laundering,

sanctions evasion, terrorism financing, scam proceeds and foreign criminal extraction before value leaves the Australian jurisdiction.

If digital value can leave Australia in seconds, Australian law must be capable of scrutinising high risk exits before they occur.

The Bill must not become a tool of private bank convenience

The Committee should not assess AML and CTF risk as though private banks are neutral public utilities. They are private profit seeking institutions with shareholder obligations, global capital market exposure and strong incentives to reduce operating costs.

Those incentives may align with public safety in some cases. They may also encourage digitisation, branch withdrawal, labour reduction, debanking, over compliance, customer exclusion and transferring risk onto individuals and communities.

The major banks have already demonstrated that serious AML and CTF failures can occur inside mainstream banking infrastructure. AUSTRAC's proceeding against CBA concerned serious AML and CTF breaches relating particularly to Intelligent Deposit Machines. AUSTRAC said those machines were used to launder illicit proceeds of crime, and CBA admitted 53,750 contraventions of the AML and CTF Act.

AUSTRAC's proceeding against Westpac was even larger in scale. Westpac admitted more than 23 million contraventions of the AML and CTF Act, including failures to properly report over 19.5 million international funds transfer instructions amounting to over 11 billion dollars, failures concerning origin information, correspondent banking risk, record keeping and suspicious transactions associated with possible child exploitation.

Those examples matter because they show that risk does not sit only at the margins. It can sit inside the largest and most respectable institutions.

The Committee should therefore be cautious about any model that gives private banks practical power to define risk while public institutions merely bless their risk appetite. If a bank finds it cheaper to close branches, push customers online, debank higher cost customers, or treat cash as inconvenient, that is not necessarily public safety. It may be private cost reduction dressed as compliance.

If private banks are unwilling to maintain a national physical banking and cash network, then Parliament should stop pretending that private provision will deliver public purpose. Banking, cash access and payment services are not ordinary discretionary retail conveniences. They are essential public infrastructure. If private institutions withdraw from that infrastructure while continuing to profit from their privileged position in the monetary system, the Committee should recommend the reestablishment of a

publicly owned bank, supported by the Australia Post network and a national cash distribution function.

That recommendation should not be treated as ideological. It is a practical consequence of market failure. If the private banking system will not maintain staffed access, cash services and human scrutiny across the country, the Commonwealth must build or restore the public capability required to do so. A serious AML and CTF framework cannot depend on private banks that remove the very physical infrastructure needed to identify, interrupt and prevent harm before money is moved beyond recovery.

Financial security is national security

Terrorism is usually discussed as a physical threat. That is understandable, but incomplete.

Financial systems are often the enabling infrastructure beneath physical harm, organised crime, sanctions evasion, foreign influence, cyber theft, scam networks and extremist activity. Money moves people, supports organisations, conceals beneficial ownership, rewards criminal conduct, sustains propaganda and allows hostile or criminal actors to operate at scale.

The Committee should therefore avoid treating money laundering and terrorism financing as a narrow compliance field. It is a national security field.

This is especially important in relation to superannuation. Australia's compulsory superannuation system has created a vast pool of privately managed savings. APRA reported total superannuation assets of about 4.5 trillion dollars as at December 2025, including about 3.2 trillion dollars in APRA regulated funds.

Those savings are not ordinary discretionary investments. They are the deferred wages and retirement security of Australian workers, accumulated through compulsory public policy. A system of that scale should be treated as critical national financial infrastructure.

Large pools of compulsory savings, complex investment chains, custodians, nominees, offshore vehicles, private markets and related service providers should be central to the Committee's thinking. A credible AML and CTF regime must look beyond low-level visible transactions and examine the structures that allow wealth, control and risk to be hidden.

The proposed AUSTRAC power should not become a narrow tool used mainly against small or politically convenient actors while major financial institutions, superannuation structures, offshore ownership chains and professional enablers remain comparatively insulated.

Financial security is national security. A country that protects itself only against physical threats, while allowing its financial infrastructure to be exploited, has misunderstood the nature of modern threat.

Frontier AI changes the risk environment

The Committee should not assess this Bill against yesterday's threat model.

The financial crime environment is now being reshaped by frontier AI. High capability AI systems can assist vulnerability discovery, cyber intrusion, identity manipulation, social engineering, document generation, scam scripting, money mule recruitment and evasion of ordinary compliance controls.

APRA has warned that banks, insurers and superannuation trustees are adopting AI rapidly, while governance, risk management, assurance and operational resilience are not keeping pace with the scale, speed and complexity of AI. APRA has also identified high capability frontier AI models such as Anthropic Mythos as part of the emerging cyber threat environment.

APRA's media release stated that frontier AI models such as Anthropic's Claude Mythos could enhance the discovery of vulnerabilities by bad actors and are expected to increase the probability, speed and scale of cyber-attacks.

This matters for AML and CTF. A criminal or hostile actor does not need to defeat the whole financial system. It may be enough to exploit weak onboarding, compromise a service provider, generate convincing identity material, manipulate a vulnerable person, automate mule recruitment, identify software vulnerabilities or move funds through digital channels faster than human review can respond.

AI strengthens the case for human scrutiny, physical service points and resilient cash access. Digital identity can be hidden, stolen, fabricated or manipulated. Physical presence at a staffed bank branch remains one of the few points where a real person can be seen, questioned and assisted before irreversible harm occurs.

The correct response is not less cash and more automation. The correct response is stronger public capability, better human intervention, robust cyber resilience, scrutiny of digital conversion points, and accountability for institutions that externalise digital risk onto customers.

Foreign influence and sovereignty risk

AML and CTF law do not operate in a sealed domestic environment. It sits inside an international security, intelligence, sanctions and banking architecture.

That creates a sovereignty risk. Australian law should not become a quiet transmission belt for foreign government priorities, foreign intelligence claims, foreign sanctions pressure or the risk appetite of private banks seeking to preserve access to overseas financial systems.

This is not an argument against cooperation with allies, intelligence partners, FATF or foreign financial intelligence units. Cooperation is necessary. But cooperation is not subordination.

Whether pressure or information comes from the United States, Israel, Japan, China or any other state, the same principle should apply. Australian financial restrictions should be justified by Australian law, Australian evidence and Australian public purpose.

The fact that an issue is raised by a foreign government, foreign regulator, intelligence partner, correspondent bank, foreign sanctions regime or international body should not be enough to justify restricting an Australian product, service, delivery channel, charity, remittance pathway, community organisation or payment mechanism.

Where classified information prevents full public disclosure, the answer should not be secrecy without scrutiny. The answer should be structured scrutiny. An independent oversight body should be able to test whether the decision is based on independently assessed Australian evidence, whether the action is proportionate, whether less restrictive measures were available and whether the measure risks discriminatory or politically selective impact.

Capture risk, political management and the revolving door

The Committee should examine capture risk directly.

Capture is not always corruption. It may appear as deference, soft enforcement, over reliance on regulated entities, negotiated compliance, industry designed policy, private consultants embedded in public processes, partial reform, or officials who move between regulator, regulated entity, law firm, consultancy and compliance provider.

Capture can also appear as a reform that protects the appearance of public interest while leaving the deeper private architecture untouched. The recent cash acceptance framework is an example. It is described as a cash mandate, but in substance it applies only to some supermarkets and fuel retailers in defined circumstances, while most businesses remain free to refuse cash and banks are not given a general statutory duty to maintain staffed cash access. That is not full cash protection. It is a narrow exception that risks politically inoculating further cash erosion.

The PwC tax scandal shows the danger of private actors being allowed too close to public policy processes. A parliamentary committee report stated that PwC should

publish accurate and detailed information about the involvement of its partners and staff in the breach of confidential government information.

The Bragg chaired ASIC report also shows that regulators themselves can become defensive and resistant to scrutiny. It records concerns about ASIC's conduct prior to the inquiry, including whether ASIC sought to influence the terms of reference, and records that the Committee rejected a number of ASIC public interest immunity claims.

Those examples matter here because AML and CTF policy is highly technical. Parliament and the public depend heavily on expert advice. But if the expert class is drawn from, returns to, consults for, or is commercially dependent on the same financial institutions and compliance industries affected by the law, public purpose can be quietly displaced by industry convenience.

The revolving door is therefore not a side issue. It is part of the machinery through which private influence, regulatory caution and policy capture can occur.

The proposed high risk mechanism power would give AUSTRAC significant discretion over products, services and delivery channels. That discretion should not be exercised inside an opaque network of former officials, regulated entities, consultants, law firms, technology vendors and foreign aligned financial systems without strong safeguards.

The Committee should require transparent conflict declarations, recusal rules, post-employment restrictions, public reporting of relevant meetings and disclosure of whether submissions, advice or technical proposals have been prepared by persons who recently held senior government, regulator, intelligence, law enforcement or ministerial roles.

A credible AML and CTF regime should not only ask whether criminals can exploit financial channels. It should also ask whether the regulated industry can exploit public channels.

The Bragg ASIC report remains useful alongside this because it shows the broader institutional lesson. Its executive summary found that ASIC's enforcement decisions were opaque and difficult to scrutinise, and chapter 2 records concerns about ASIC's engagement with the inquiry, including public interest immunity claims and internal material concerning the inquiry process. That supports the argument that Parliament should not rely on appearances of protection or accountability. It should look at the machinery underneath.

Lessons from the prohibited hate group framework

The Committee should apply the same discipline to this Bill that should apply to any national security framework.

In my submission to the Committee concerning the listing of Hizb ut Tahrir as a prohibited hate group, I argued that the question was not whether the target organisation was bad. The question was whether the statutory threshold, legal architecture, proportionality and future credibility of the scheme were sound. That same principle applies here.

The question is not whether money laundering, terrorism financing or high-risk mechanisms are serious. They are. The question is whether the legal architecture is precise, proportionate, reviewable and capable of principled application.

That earlier submission also raised concern about frameworks that are too narrow in practical application and too broad in legal consequence. The same concern applies to this Bill. If AUSTRAC's power is used mainly against visible, politically easy or smaller actors, while major banks, professional enablers, offshore structures, superannuation architecture, correspondent banking risk and digital platforms escape equivalent scrutiny, the framework will not be credible.

A law presented as a response to modern financial crime must be capable of principled and even-handed application across materially comparable risks.

The Bill should distinguish cash from high-risk conversion mechanisms

A central defect in public debate is the failure to distinguish cash from mechanisms that convert cash into less transparent digital flows.

Cash at a staffed bank branch is not the same risk as cash inserted into a crypto ATM. A cash withdrawal at a local bank is not the same risk as a remote digital transfer to a foreign wallet. A pensioner paying with cash is not the same risk as a mule network moving value through digital accounts.

The Bill should require AUSTRAC to distinguish between lawful public money and particular high-risk mechanisms.

If AUSTRAC identifies a crypto ATM as high risk, the regulatory response should be directed at the crypto ATM, the digital wallet pathway, the provider, onboarding controls, transaction limits, scam warnings, customer due diligence, blockchain exposure, third party control and offshore movement. It should not become a general attack on cash.

The same principle applies to remittance channels, digital asset exchanges, international transfers, payment platforms and online accounts. The mechanism and risk pathway should be identified with precision.

Gambling, wagering and laundering architecture

The Committee should also expressly consider gambling and wagering as high-risk mechanisms.

Gambling is important because it demonstrates the danger of blaming cash rather than the architecture that enables laundering. Cash used by a person for lawful ordinary purposes is not the same thing as cash pushed through a gambling venue, gaming machine, wagering account, voucher, payout card, prepaid instrument, overseas account or online betting structure to obscure the source, ownership or destination of funds.

AUSTRAC has stated that gambling is routinely targeted, and that high transaction volumes, digital evolution and cash intensive channels create opportunity. It has also identified recurring systemic weaknesses across gambling and wagering operators, including high value and high frequency cash transactions, bill stuffing, minimal gameplay, prepaid cards, vouchers, payout cards, overseas accounts, multiple accounts, third party activity, synthetic identities, weak source of funds checks and high-risk customers continuing to transact despite warning signs.

That is directly relevant to this Bill. The problem is not cash as lawful public money. The problem is the mechanism that allows money to be placed, layered, converted, legitimised or moved without adequate scrutiny. Gambling can perform that function. So can crypto ATMs, digital asset exchanges, remittance channels, offshore payment platforms, opaque corporate structures and professional enablers.

The Committee should therefore ensure that any high-risk mechanism power is capable of being applied across materially comparable risks, including gambling and wagering. It should not become a power used mainly against visible or politically convenient channels while large, profitable or well-connected sectors receive softer treatment.

The same principle applies throughout the submission. Cash at a staffed bank branch is visible and interruptible. Cash converted through a laundering mechanism is different. Digital value moved through an online wagering account, foreign platform, mule account or crypto wallet may be faster, more obscure and harder to recover. The law should target the laundering mechanism, not scapegoat the existence of cash.

Public financial infrastructure is part of the solution

The Bill is too narrow if it treats AML and CTF as a matter of private sector compliance and regulator discretion only.

Australia needs stronger public financial infrastructure. That means lawful cash access, staffed service points, Australia Post banking capacity, public payment resilience, a

regulated public account to account payment option, and a clear national policy that financial access is an essential service.

The Senate bank closures inquiry has already recommended guaranteed reasonable access to cash and financial services and investigation of a publicly owned bank, including one associated with the Australia Post branch network.

Those recommendations should be treated as part of the AML and CTF conversation. Financial exclusion, debanking, branch withdrawal and forced digitisation do not make the system safer. They can push people into less visible channels, increase dependence on opaque digital systems and remove human scrutiny.

If the Commonwealth wants a safer financial system, it should build public capability rather than relying on private banks whose incentives are not identical to public purpose.

Recommendations

Recommendation 1

The Committee should recommend that the Bill be amended to include an express statutory cash protection safeguard. The AUSTRAC CEO's high risk mechanism power must not be used directly or indirectly to restrict lawful access to cash, reduce staffed bank branch services, narrow cash acceptance, justify branch closures, or treat cash itself as a suspect mechanism.

Recommendation 2

The Committee should recommend that AUSTRAC be required to distinguish between cash as lawful public money and particular high risk conversion mechanisms, including crypto ATMs, gambling and wagering channels, gaming machines, vouchers, prepaid instruments, payout cards, digital asset exchanges, stablecoin pathways, digital wallets and other mechanisms that convert visible physical money into less transparent digital flows.

Recommendation 3

The Committee should recommend that the proposed power be subject to a stronger public interest test, including necessity, proportionality, evidence of significant harm, consideration of less restrictive alternatives, impact on financial inclusion, impact on cash access and impact on lawful community activity.

Recommendation 4

The Committee should recommend that any restriction or prohibition be accompanied by a public statement of reasons, subject only to redactions that are genuinely necessary for law enforcement, intelligence or national security purposes.

Recommendation 5

The Committee should recommend that where full public disclosure is not possible, an independent oversight body must be able to review the evidence, test proportionality and report to Parliament in an appropriately protected form.

Recommendation 6

The Committee should recommend that AUSTRAC be required to publish an annual high risk mechanisms report covering use of the power, affected sectors, evidence relied upon, duration of restrictions, review outcomes, impacts on cash access, impacts on communities, impacts on financial inclusion and any unintended consequences.

Recommendation 7

The Committee should recommend that the Bill include a foreign influence and sovereignty safeguard. Any use of the power should disclose, to the greatest extent possible, whether the proposed restriction was prompted or materially supported by information, pressure or requests from a foreign government, foreign regulator, foreign intelligence partner, foreign sanctions regime, international body or private financial institution acting because of foreign compliance pressure.

Recommendation 8

The Committee should recommend a conflict and influence statement before any major restriction is made. That statement should identify material consultation with regulated entities, consultants, law firms, technology vendors, foreign agencies and former public officials, subject only to genuine security limitations.

Recommendation 9

The Committee should recommend stronger revolving door protections for senior AUSTRAC, Treasury, Home Affairs, intelligence, law enforcement and ministerial personnel who move into AML and CTF related private sector roles, and corresponding disclosure requirements for private sector appointees who move into public decision-making roles.

Recommendation 10

The Committee should recommend that AUSTRAC be required to report specifically on frontier AI related AML and CTF risks, including cyber compromise, identity fraud, synthetic identity, automated scams, deepfake enabled deception, money mule recruitment, digital onboarding abuse and AI assisted exploitation of financial infrastructure.

Recommendation 11

The Committee should recommend that the Government develop a jurisdictional digital payments firewall for high risk inbound and outbound digital value flows. That framework should require risk-based scrutiny before value leaves Australia, including payee verification, scam warnings, cooling off periods, human review, source of funds checks, destination checks, beneficial ownership checks and temporary holds where necessary.

Recommendation 12

The Committee should recommend that AML and CTF reform be linked to a broader public financial infrastructure strategy, including guaranteed access to cash, preservation of staffed service points, stronger Bank@Post arrangements and public payment infrastructure capable of supporting resilience, inclusion and financial integrity.

Recommendation 13

The Committee should recommend that the Government develop a genuine national framework for universal cash access applying beyond supermarkets and fuel retailers, including enforceable obligations on banks to maintain reasonable staffed cash services, physical cash access and over the counter cash assistance.

Recommendation 14

The Committee should recommend that major banks be required to maintain reasonable national access to staffed banking and cash services as part of their essential service obligations. If private banks are unwilling or unable to maintain that physical network, the Committee should recommend the reestablishment of a publicly owned bank, using the Australia Post network where appropriate, to provide universal basic banking, cash access, payment resilience and human service points as part of Australia’s financial crime prevention architecture

Conclusion

The Bill addresses a real problem, but it risks misidentifying the deeper one.

Money laundering, terrorism financing and serious financial crime are not simply the product of cash. In the modern financial system, the dominant risk architecture is digital, remote, cross border, privately controlled and increasingly automated. It is built around digitised financial infrastructure, remote identity, offshore value movement, crypto conversion pathways, gambling and wagering channels, private compliance incentives, weak human scrutiny, opaque ownership structures, professional enablement, frontier AI, branch withdrawal and regulatory systems vulnerable to capture.

Cash should not be scapegoated for those failures. Cash is lawful public money. In a staffed, accountable and accessible banking environment, cash creates presence, friction, visibility and human intervention. Those are strengths. The risk arises when value is pushed through mechanisms that convert, obscure, layer, accelerate or move it beyond practical scrutiny and recovery. That can occur when cash is converted into crypto. It can also occur when digital bank funds are converted into crypto, moved through wagering channels, sent offshore, routed through opaque accounts, or handled by professional structures that conceal ownership and control. The starting form of the money is not the central issue. The mechanism and loss of visibility are.

The recent cash acceptance framework shows the danger of partial protection. Cash is presented as protected, while the protection is confined to certain supermarkets and fuel retailers and most of the economy remains outside the mandate. That is not enough. A genuine national framework for universal cash access must extend beyond supermarkets and fuel retailers. It must include banks, staffed access, essential services, physical cash access, over the counter assistance, public payment resilience and public financial infrastructure.

The Committee should therefore resist any pathway by which this Bill becomes a back door attack on cash, branches or physical banking. If private banks are unwilling to maintain a national physical banking and cash network, Parliament should stop pretending that private provision will deliver public purpose. Banking, cash access and payment services are essential public infrastructure. If private institutions withdraw from that infrastructure while continuing to profit from their privileged position in the monetary system, the Committee should recommend the reestablishment of a publicly owned bank, supported where appropriate by the Australia Post network and a national cash distribution function.

The proper response to digital financial crime is not to force Australians further into digital systems whose risks are increasing. The proper response is stronger public

capability, better human scrutiny, tighter regulation of digital conversion points, serious scrutiny of gambling and wagering mechanisms, genuine oversight of regulatory discretion, stronger safeguards against capture and a financial system designed around Australian public purpose.

The principle should be clear. Financial security is national security, but national security must not become a blank cheque. If Australia is to restrict financial mechanisms in Australia, it should be because Australian law, Australian evidence and Australian public purpose justify it. Foreign pressure, private bank convenience, regulator caution, partial cash protection or technological fashion should never be enough.

References

1. Parliamentary Joint Committee on Intelligence and Security, Review of the Anti-Money Laundering and Counter Terrorism Financing Amendment Bill 2026.

2. Parliament of Australia, Anti Money Laundering and Counter Terrorism Financing Amendment Bill 2026, Bill homepage.

3. Department of Home Affairs, 2026 Reforms to the Anti Money Laundering and Counter Terrorism Financing Act 2006.

4. AUSTRAC, About the AML and CTF reforms.

5. AUSTRAC, Cryptocurrency ATM scams.

6. AUSTRAC, Powers proposed to tackle high risk products, services and channels.

7. AUSTRAC, Enhanced customer due diligence as a key tool in identifying scam and money laundering risk.

8. Australian Competition and Consumer Commission, Cash Acceptance Industry Codes.

9. Australian Competition and Consumer Commission, Payment methods.

10. Commonwealth Parliament, Senate Hansard, 31 March 2026, Competition and Consumer Industry Codes Cash Acceptance Regulations 2025 disallowance debate.

11. Senate Rural and Regional Affairs and Transport References Committee, Bank closures in regional Australia, final report.

12. AUSTRAC, AUSTRAC and CBA agree 700-million-dollar penalty.

13. AUSTRAC, AUSTRAC seeks civil penalty orders against CBA.

14. AUSTRAC, AUSTRAC and Westpac agree to proposed 1.3-billion-dollar penalty.

15. AUSTRAC, Westpac ordered to pay 1.3-billion-dollar penalty.

16. APRA, Letter to industry on Artificial Intelligence.

17. APRA, APRA calls for a step change in AI related risk management and governance.

18. APRA, Superannuation statistics for December 2025.

19. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Final Report.

20. Senate Economics References Committee, Australian Securities and Investments Commission investigation and enforcement, July 2024.

21. Australian Public Service Commission, Leaving the APS, post separation conflict of interest.

22. Parliamentary Joint Committee on Corporations and Financial Services, Ethics and Professional Accountability, Structural Challenges in the Audit, Assurance and Consultancy Industry.

23. Parliamentary Joint Committee on Intelligence and Security, Review of the listing of Hizb ut Tahrir as a prohibited hate group under the Criminal Code.

24. Michael Sanderson, Review of the listing of Hizb ut Tahrir as a prohibited hate group under the Criminal Code, submission to the Parliamentary Joint Committee on Intelligence and Security.

25. AUSTRAC, AUSTRAC CEO speech, Regulating the Game.

26. AUSTRAC, Indicators of suspicious activity for the online betting agencies sector.

27. AUSTRAC, Worked examples for the online wagering industry.