Australian Banking Association

# ABA Submission

## Inquiry into the capability of law enforcement to respond to money laundering and financial crime

Parliamentary Joint Committee on Law Enforcement

9 August 2024

Australian Banking Association

# Table of Contents

Australian Banking Association

# Inquiry into the capability of law enforcement to respond to money laundering and financial crime

## Introduction

The Australian Banking Association (ABA) welcomes the opportunity to provide the Parliamentary Joint Committee on Law Enforcement with a submission into the "*Inquiry into the capability of law enforcement to respond to money laundering and financial crime*" (**Inquiry**).

The ever-evolving landscape of money laundering and financial crime necessitates that law enforcement agencies (**LEAs**) leverage emerging technologies and broader intelligence and knowledge sharing opportunities to effectively respond to these threats. Financial Institutions (**FIs**) are committed to combating financial crime and have invested significantly in control environments and intelligence sharing to support LEA initiatives and disrupt illegal activities. However, deeper collaboration between the public and private sectors is increasingly crucial, especially with the impending inclusion of Tranche 2 entities and the enhanced focus in the proposed reforms on entities identifying and understanding their financial crime risk. Effective information sharing is critical in combating financial crime, and reducing regulatory barriers that inhibit such collaboration will enhance our collective ability to detect and prevent illegal activities. By working together, leveraging advanced technologies, and facilitating smoother information flow, we can collectively strengthen Australia's defences against financial crime.

The ABA's submission seeks to address all sections of the Inquiry's Terms of Reference.

## a. Scale and forms of financial crime in Australia

*the scale and forms of money laundering and financial crime in Australia, including their effect on the community and the economy, the types of criminal activities they fund, the methods employed by serious and organised crime, and emerging trends and threats;*

Money laundering and financial crime continue to be pervasive issues in Australia, significantly impacting the community with damaging economic, security, and social consequences. Financial crime is ultimately an indicator and enabler of predicate offences such as human and drug trafficking, child exploitation, environmental crime, bribery and corruption, and fraud and scams, among others. The recently published AUSTRAC National Risk Assessments (**NRAs**) offers an in depth look at the channels and sectors at the highest risk of exploitation. Financial institutions recognise the role that traditional channels such as banks play, investing heavily in specialised teams and systems to address financial crime risks. These teams span policy, compliance, governance, analytics, detection, investigation, and reporting, highlighting the substantial resources dedicated to combatting these threats. AUSTRAC regulated institutions submitted more than 192 million reports (IFTIs, TTRs and SMRs) in 2022-23, contributing to law enforcement investigations, recovery of tax revenue and AUSTRAC sector-based risk assessments.[1]

Financial institutions, LEAs and AUSTRAC have all observed that technological advancements have enabled more sophisticated methods of financial crime, posing significant challenges for

[1] AUSTRAC 2022-23 Annual Report

Australian Banking Association

detection and enforcement, particularly due to the globalised nature of crime. Some of these emerging trends and challenges are explored below.

**Scams – an ecosystem approach**

One such group taking advantage of this trend are scammers who are often part of a larger organised crime syndicate, using the illegal income earned by scams to invest in other criminal activity or support insurgencies.[2] In 2023, scams were responsible for losses of up to $2.7 billion[3] with the actual social and psychological impacts on victims going well beyond the financial impact. Whilst banks continue to invest in protections for customers, scammers continue to pivot to initiating contact with scam victims and disseminating scam content through social media/digital platforms.[4] Every sector of the scams ecosystem has a role to play in preventing scammers from exploiting any loopholes, including telecommunications companies, banks, digital platforms as well as law enforcement who have the power to investigate, disrupt and prosecute scam syndicates.

**Evolving payments landscape**

The way Australians make payments has transformed significantly since the passage of existing payments legislation and the AML/CTF regime, with the majority of transactions now being conducted through electronic methods. This shift has been driven by advancements in technology, the emergence of new market entrants, and evolving consumer preferences.

The dated regulatory architecture means that a number of payment system providers (PSPs) are not captured under the AML/CTF regime in Australia including PSPs that are domiciled overseas and don't have a geographical link, which limits visibility of the payment chain and business's ability to manage risk when they are not registered for AML/CTF purposes. AUSTRAC's NRA on Money Laundering acknowledged "[t]he design of some OPSP products and services may not fit within existing regulatory frameworks or are designed expressly to avoid regulation. It may be difficult for reporting entities to determine whether the OPSPs' product or service meets the definition of a 'designated service' under the AML/CTF Act, whether a provider is required to enrol with AUSTRAC and what reporting obligations they may have."[5]

To ensure that LEAs are able to better detect and disrupt financial crime, it is crucial to capture new and existing payment service providers (**PSPs**) that are not subject to Australia's AML/CTF regime.

**Money Mules**

The increasing digitisation of payments has provided unparalleled convenience, but it has also laid the foundation for a concerning shift towards the use of mule accounts to launder the illegal proceeds of crime. "Money Mules" provide a layer of legitimacy and anonymity by putting distance between the crime and the illegal funds, making it more difficult for LEAs to accurately trace money trails. New and faster payment types have added another layer of complexity whereby criminals are not just targeting bank accounts, but also less traditional payment mechanisms, such as virtual currencies, prepaid debit cards or money service businesses.[6] To disrupt these fast-moving transactions, the crime needs to be identified and disrupted earlier in the money mule lifecycle before it even reaches a payment method – when a criminal initiates contact with and solicits a

[2] https://www.aspistrategist.org.au/scams-are-now-a-national-security-issue/
[3] https://www.ausbanking.org.au/banks-continue-fight-against-scammers-as-new-report-shows-drop-in-losses/
[4] *ABA submission to the Joint Select Committee on Social Media and Australian Society.*
[5] AUSTRAC Money Laundering in Australia National Risk Assessment p 41.
[6] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/money-mules

Australian Banking Association

potential Money Mule victim. AUSTRAC's recently released guidance on 'Combating the exploitation of international students as money mules' assist government agencies and FIs to identify the signs of exploiting victims to be money mules.[7] The ABA encourages additional law enforcement community awareness initiatives, particularly for vulnerable cohorts of the community. Furthermore, greater information sharing avenues between the public and private sector (e.g. AFCX Intel Loop) could enhance the ability of organisations to detect and take down content using digital platforms or telecommunication providers to solicit individuals to be money mules.

## b. AML/CTF legislation in comparison with other jurisdictions and FATF Standards

*Australia's anti-money laundering and counter-terrorism financing (AML/CTF) legislation as well as comparison with other jurisdictions and the international standards set by the Financial Action Task Force;*

### AML/CTF Act

The ABA notes its 2024 submission to the Attorney-General's Department (**AGD**) on Reforming Australia's AML/CTF Regime, in which we emphasised the importance of a simplified and outcomes focused regime and highlighted key areas for reform.[8] The review presents a significant opportunity to address known pain points within the existing AML/CTF regime that impacts the capability of law enforcement to effectively respond to money laundering and financial crime.

> **Tipping off:** The current formulation of the tipping off offence acts, perversely, as a barrier to appropriate information sharing to detect and disrupt criminal activity. The expansion of the exceptions provision to the tipping off offence in 2021 provided some added flexibility, but not enough to remove major obstacles to information sharing. The ABA supports the removal of the 'inferential limb' of the current tipping off offence. The inferential limb in the current legislation poses significant challenges in practice, not limited to hindering FIs from ending relationships with customers or employees (i.e., because they may 'infer' a suspicion was formed) and from defending the positions they have taken with customers in private Court actions (i.e., because financial institutions cannot reference the 'tipping off' obligations or explain the basis for such a position, without creating an inference that an SMR may have been filed). A further example of difficulties caused by the inferential limb, is where a bank reports a suspicion that relates to an identifiable victim, who is a customer. For example, if a bank reports a suspicion about a victim of fraud or a victim of coercive control exercised through financial abuse detected in a bank's systems. The bank may be restricted in fully supporting a customer in this circumstance, because of not being able to disclose information from which a suspicion could be inferred.
>
> The ABA reiterates its June 2024 recommendation to AGD, suggesting the offence be re-drafted to align with approaches taken in the United Kingdom and Canada.[9] These jurisdictions focus on preventing actions that might compromise law enforcement investigations without broad restrictions on information sharing. The ABA recommends that

[7] https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/combating-exploitation-international-students-money-mules
[8] ABA Submission on 'Consultation on Reforming Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime', 21 June 2024.
[9] ABA Submission on 'Consultation on Reforming Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime', 21 June 2024.

Australian Banking Association

the tipping off offence should arise where it is reasonably foreseeable that the disclosure of the information would be likely to prejudice an investigation or potential investigation. Similar to the UK, we consider a new offence should reference causing prejudice to specific types of investigations, such as those conducted by agencies equivalent to the police, Revenue, and the UK National Crime Agency. Proposing that tipping off arises where it is 'likely to prejudice an investigation or *potential* investigation' could impose limitations that hinder FIs ability to manage ML/TF risks. It is difficult for FIs to assess the *likelihood* of a disclosure of SMR information *potentially* prejudicing law enforcement investigations, especially given the number of State and Commonwealth law enforcement bodies that often operate independently.

Private to private sharing of information is significantly inhibited by the existing tipping off regime. FIs have specialist intelligence units which could share intelligence in order to identify, manage and mitigate their own risks and those impacting the industry. Such sharing could result in the earlier identification of criminal activities or typologies. This would facilitate a more robust intelligence and risk environment which LEAs could harness to enhance capability. However, the tipping-off prohibition prevents the upside potential arising from such information sharing. Some other examples that demonstrate the unintended and undesirable impacts of the current tipping-off provisions include:

1. Bank A exits a customer due to serious financial crime concerns such as suspected involvement in significant money laundering. Customer onboards with Bank B (perhaps a second/third tier institution with less capable money laundering detection tooling). No ability for banks to share important financial crime intelligence to protect / harden the industry.

2. Bank A detects multiple transactions strongly indicative of money laundering being transferred to Bank B and submits an SMR. Bank A exits the customer but is unable to communicate to Bank B that their customer is suspected of transacting illegal funds.

3. Bank A identifies a customer strongly suspected of committing child sex exploitation crimes. Bank A submits an SMR and exits the customer. Bank A is unable to communicate to other institutions that this individual is suspected of engaging in this crime to prevent it occurring.

4. Small Business A wants to understand its financial crime risk more effectively by bringing in a third party consultancy to help assess risk. However, the third party is prevented from receiving SMR data to help understand its risk. This limits the effectiveness of the risk assessment and increases the costs to Small Business A by requiring investment in additional resources to analyse the SMR data (see Inquiry Terms of Reference (d) for more detail).

**Digital ID:** The misuse of identity is central to many crimes, including impersonation, fictitious identities, identity theft and money mules. Secure digital identities, such as cryptographic digital credentials, are crucial in combating organised crime in both the physical and digital worlds. In March 2020, the FATF issued guidance which highlighted the important role of digital ID in AML/CFT customer due diligence (**CDD**) processes, offering more security and greater assurance. To realise these benefits, the ABA continues to assert the importance of removing any doubt from the current (and future) AML/CTF regime that reliance upon a digital identity satisfies KYC obligations.

Australian Banking Association

The ABA notes the introduction of the Digital ID Framework and acknowledges AGD's reference to 'working with the Department of Finance in considering how changes to Australia's Digital Identity Framework might be leveraged by reporting entities to comply with certain CDD obligations under the AML/CTF regime, whilst also ensuring compliance with relevant FATF Recommendations'.[10] Harmonisation of the Digital ID framework presents an opportunity for a whole of government approach to customer identification. This may enhance LEA capability by reducing the potential misuse of identification information and criminal offences which follow. Private Digital ID platforms, such as ConnectID could also be considered to reduce potential misuse of the ID information.

**Other jurisdictions**

**Singapore:** The *Online Criminal Harms Act* (OCHA) commenced in February 2024. It gives law enforcement the power to issue directions and to stop/remove the communication of online materials, disable access to online materials and locations, restrict online accounts and online services, and stop the distribution or downloading of apps. This will enable law enforcement to deal more effectively with online criminal activities, including fraud, scams and money mule advertisements. Similarly explicit powers in Australia would equip law enforcement to better respond to criminal digital content.

**The Financial Action Task Force (FATF)**

**Digital Strategy:** The ABA notes the FATF's work on the 'AML/CFT Digital Strategy for Law Enforcement Authorities' (May 2022)[11] which explores how LEAs can use technology, including advanced analytics, to effectively investigate money laundering and financial crime and mitigate the risks of these crimes. The Strategy asserts the importance of LEAs aligning their strategies with the technology and digital tools available to both FIs and criminals. This includes harnessing opportunities to extract valuable intelligence from digital tools, such as Digital ID and private-private data sharing. Additionally, agencies need to possess the right technical skills to integrate these digital tools and must have adequate in-house technological and program management capabilities; or consider relying on trusted third-party partners for these services.

Another key focus of the Digital Strategy is the principle that collaboration with the private sector is essential to building trust. For example, joint initiatives relating to data sharing will foster a collaborative approach to targeting financial crime. As noted above, FIs have financial intelligence units which can facilitate such initiatives (via the Fintel Alliance or direct partnerships).

**Beneficial Ownership**: The FATF released guidance on beneficial ownership of legal persons (March 2023)[12] and legal arrangements (March 2024)[13]. This is an often-overlooked shortcoming of the Australian AML/CTF regime. In November 2022, Treasury consulted with industry on a proposed beneficial ownership register but unfortunately this proposed initiative has not progressed. A public beneficial ownership register aims to improve transparency of

[10] Reforming Australia's anti-money laundering and counter-terrorism financing regime, Paper 5: Broader reforms to simplify, clarify and modernise the regime p 15.
[11] https://www.fatf-gafi.org/en/publications/Digitaltransformation/Digital-transformation-law-enforcement.html
[12] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html
[13] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Transparency-Legal-Arrangements.html

Australian Banking Association

beneficial ownership in Australia and deter the use of complex structures designed to evade legal obligations. It seeks to support stronger law enforcement responses to tax and financial crime and facilitate the enforcement of sanctions. Whilst the proposal didn't go far enough, it's important to note that a beneficial ownership register would enhance the capabilities of both LEAs and FIs. For instance, it could streamline KYC and support screening of customers. Additionally, LEAs could more effectively determine the ownership of companies, trusts and assets involved in criminal enterprise. Finally, it would better align Australia with international approaches, including the FATF Standards.

## c. Proposed 'tranche two' reforms and implications for law enforcement

*proposed 'tranche two' reforms to extend the existing AML/CTF legislation to services provided by lawyers, accountants, trust and company service providers, real estate agents and dealers in precious metals and stones and implications for law enforcement;*

The ABA strongly supports the proposed expansion of Australia's AML/CTF Regime to 'Tranche 2' entities which has the potential to significantly increase the volume and enrich the value of the intelligence provided to LEAs. As AML/CTF obligations will be new to these sectors, initially there will likely be limited understanding and expertise, requiring time for the value of the intelligence to be utilised and the benefits realised. More broadly, we reiterate the time and resources required to bring new sectors up to speed on typologies and risks and the importance of education and engagement between the private and public sectors. Unless these new sectors are provided with the necessary tools for success, there is a risk of increased regulatory burden without any beneficial outcome. Comprehensive support from regulators and Commonwealth agencies is crucial for the successful implementation of tranche 2 reforms, ensuring intelligence outputs are fit for purpose.

The expansion of the AML/CTF regime to include tranche 2 entities will significantly increase the number of Reporting Entities (**REs**) requiring regulatory supervision, in turn requiring an expansion of AUSTRAC's supervisory capacity. The banking sector, whilst a key part of the ecosystem, should not be relied upon as a de facto supervisor of tranche 2 entities or a preferred source of quality intelligence Specifically, banks should not be expected to apply enhanced due diligence standards to newly defined 'high risk' tranche 2 entities merely because they are now included within the AML/CTF regime or to assess the quality of a tranche 2 RE's AML/CTF program. This would be both an unrealistic burden and, if such a stance is adopted, it could result in tranche 2 entities being considered non-compliant and potentially loosing access to banking services. Banks' existing transaction monitoring and risk assessment procedures should continue to apply.

Another example is the Legal Profession Uniform Law (as applied in Vic, NSW and WA) which presently requires that ADIs report irregularities associated with solicitor trust account. Irregularities may encompass suspicious matters which would also be captured in SMRs. This obligation essentially places some of the reporting obligations of law firms on banks and gives legal profession bodies (like the Law Society) quasi regulatory roles. This obligation will also cut across the AML/CTF obligations once tranche 2 reforms are enacted.

**Keep open notices**

With an increase in REs, there is likely to be an increase in the number of keep open notices issued under Chapter 75. This will inevitably place a greater operational burden on AUSTRAC,LEAs and REs to issue, review and manage these notices. The suggestion in the AML/CTF Reforms to remove

Australian Banking Association

AUSTRAC as an intermediary in the notice approval process is not supported by ABA members and will do little by itself to alleviate the burden for LEAs, as much as it will for AUSTRAC.

It is imperative that this process be resdesigned with efficiency and consistency in mind and incorporating safeguards against the issuance of high volumes of notices without substantial justification. LEAs should not be able to direct a bank to keep an account open for speculative purposes or convenience. The ABA recommends that any proposed AML/CTF amendments must include a framework that LEAs apply when issuing a keep open notice including that they should be approved by a senior level officer, relate to a relatively narrow set of offences (aligned with the definition in transaction monitoring) and include relevant information on the nature of the investigation to support the request. The administrative procedures for the issuing and expiry of keep open notices, together with those for revocation by AUSTRAC, must be straightforward.[14] To stem excessive or lower-quality notices being issued, AUSTRAC should track the quantity and quality of notices. This could take the form of a national register to ensure the principles of transparency, proportionality and appropriateness of use are adhered to. Where notices appear invalid, FIs should have a right to apply to have the notice revoked.

## d. Whether existing criminal offences and LEA powers and capabilities are appropriate, including for emerging technologies

*whether existing criminal offences and law enforcement powers and capabilities are appropriate to counter money laundering, including challenges and opportunities for law enforcement, such as those relating to emerging technologies;*

Despite continuous efforts by law enforcement, and governments to enhance defences against financial crime and money laundering through technological advancements, bad actors remain innovative, developing new strategies to outpace prevention and detection measures. To address these dynamic risks, LEAs must continuously adapt, ensuring they possess the requisite expertise and resources to improve detection capabilities and effectively respond to emerging technologies. Individual instances of financial crime may not be assessed as of sufficient priority to warrant allocation of resources, yet in aggregate represent a significant cost to the community and are often linked to other more obviously damaging forms of crime. Specialised teams such as the state cybercrime squads, and Joint Policing Cybercrime Coordination Centre (**JPC3**) had a high level of understanding and capability and the advantage of a dedicated focus. The ABA supports the allocation of additional human resources and technological supports to these specialised teams, as they are best equipped to handle financial crime investigations, rather than relying on local station officers.

**Obtaining data in a timely manner**

LEA's are often constrained by their inability to obtain data in a timely manner, with the need to serve notices for basic information and, particularly, the physical service of material in VIC. Given the speed at which financial crime activity is driven by new technology, measures to increase the speed of investigation and acquisition of data, including streamlined interaction with private sector initiatives such as the AFCX, must be developed.

[14] ABA Submission on 'Consultation on Reforming Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime', 21 June 2024.

Australian Banking Association

**Fostering innovation**

New technologies can improve the speed, quality and efficiency of measures to combat money laundering and terrorist financing. They can help financial institutions, LEAs and regulators to assess these risks in ways that are more accurate, timely and comprehensive. Less prohibitive tipping-off provisions coupled with secure intelligence sharing mechanisms would drive innovation in the financial crime sector. Given FIs are not inherently 'technology companies', they often have to leverage external vendors and technology platform providers for support. However, tipping-off provisions create significant challenges for fostering innovation in the financial crime sector. Information sharing requires a regulator to facilitate sharing via compulsory notices (or sanitisation of information). Emerging technologies such as ChatGPT and similar large language models (LLMs) offer unique opportunities to collaborate with FinTechs and other companies to utilise LLMs on SMR data to detect new and emerging risks, a process that could be initiated within days for testing purposes. Unfortunately, the tipping-off provisions hinder such initiatives. Consequently, tools must be developed internally, incurring substantial costs and requiring resource-intensive and time-consuming efforts that can span months or even longer. For smaller institutions, this approach may be cost prohibitive.

**Non-traditional technology platforms**

The regulation of non-traditional technology platforms, such as digital currency exchanges, Fintechs and social media, is in its infancy. This may translate to significant gaps in intelligence and opportunities to prevent financial crime if:

- Those sectors are not actively seeking to detect and report suspicious activity on their platforms,
- Those sectors have limited subject matter expertise, and/or
- The agencies dealing with them have a limited understanding of the platform and its underlying technology, making it difficult to know what information to ask for when undertaking an investigation.

This presents an opportunity for law enforcement to engage with private industry experts to support investigations and prosecutions. For example, if law enforcement is able to disseminate Know Your Customer (KYC) information relating to high risk/suspicious activity identified on those platforms to FI's, they may be able to fill intelligence or knowledge gaps and assist in providing a more comprehensive view of the person or entity and other financial activity of interest. Supporting LEAs by providing institutions with greater information about individuals, typologies, and risk indicators enables them to better identify and understand their financial crime risks, leading to more accurate SMRs reported to AUSTRAC and, by extension, LEAs.

## e. Effectiveness of collaboration, coordination and information sharing between LEA, agencies and the private sector

*the effectiveness of collaboration, coordination and information sharing between Commonwealth agencies, including law enforcement, and with authorities in other jurisdictions and the private sector;*

**Increased channels for public-private information sharing**

Australian Banking Association

The Fintel Alliance and law enforcement MOU partnerships with FIs (e.g., AFP) are both examples of successful collaboration between the public and private sectors. Intelligence shared in those forums has proven to be of great value to law enforcement and the regulator in understanding and disrupting financial crime threats. These partnerships are highly valued by the private sector as well, as the intelligence shared is used to uplift our control environments, in an effort to play our part in fighting financial crime.

However, outside of the Fintel Alliance's agreed programs of work, there are limited opportunities for FIs to report suspicious activity directly to law enforcement. Expanding these channels would enhance the capability of LEAs to detect and respond to financial crimes: firstly, by allowing for more timely interventions; and secondly, ensuring law enforcement resources can be flexibly adapted to evolving risks. Smaller institutions that are notmembers of the Fintel Alliance face additional challenges due to the lack of streamlined coordination and trusted contacts within LEAs. Without the status of an AUSTRAC entrusted person, private-to-private information sharing becomes a barrier, and these smaller institutions lack the same outreach capacity as those within the Fintel Alliance. To capture a more comprehensive view of threats, smaller institutions require increased channels to share intelligence.

Another successful collaboration is the Australian Financial Crimes Exchange (**AFCX**) anti-scam intelligence loop (**Intel Loop**) which provides the technological backbone for a whole-of-ecosystem approach to combatting scams. Although National Anti-Scam Centre (**NASC**) data indicates that overall scam losses in Australia are starting to decline,[15] we recognise that enhanced and continued cooperation among industries, government, and law enforcement is essential for making Australia a less appealing target for scammers. The Intel Loop facilitates near real time scam information sharing between participants, including the Federal Government's NASC, banks, telcos and digital platforms. Intelligence sharing channels like the Intel Loop allow the public and private sector to better coordinate intelligence and data-sharing activities to stamp-out financial and cyber-crime.

Nevertheless, tipping-off provisions and, especially privacy law constraints significantly inhibit the effectiveness of the Intel Loop. The restrictions on sharing customer information (even securely) within the private sector limit the ability of the private sector to leverage sector-wide capability and intelligence to disrupt financial crime. In April 2024, the Monetary Authority of Singapore launched a digital platform, COSMIC,[16] which significantly improves the ability of FIs to detect and thereby deter criminal activity by enabling FIs to securely share with one another, information on customers who exhibit multiple financial crime "red flags". LEAs could also leverage this data to identify broader industry trends and focus enforcement efforts. Current regulatory settings prevent Australia from adopting a similar approach as Singapore.

**Feedback loop**

Providing some form of feedback on submitted SMRs would provide REs with the opportunity to improve the content of SMRs leading to better investigation outcomes. Similarly, notices served on the private sector may not always outline what the predicate offence is and/or suspicion it relates to. If Commonwealth agencies were able to provide more specific details about what they were looking for, including potential offences, FI's would be able to provide more relevant information to support those queries via the SMR reporting channels. Additionally, the limited information provided by LEAs impacts the ability of FIs to appropriately manage and mitigate the risk for AML/CTF purposes. FIs recognise the challenge that law enforcement may be hesitant to provide information for fear of

[15] National Anti-Scam Centre, Targeting Scams Report 2023, issued in April 2024
[16] https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic

Australian Banking Association

customers being de-banked. However, the greater, and more granular, the guidance and information shared with institutions from government, the better they can understand and manage those risks.

**Inter-agency coordination**

The information sharing powers, including the prohibitions on disclosure of notices, of each Commonwealth agency varies. This can reduce the ability of participating agencies to rapidly identify money laundering activity and may hinder the effectiveness of investigations and/or the ability to absorb the true value of the intelligence.

Additionally, Commonwealth agencies have separate data repositories and case management systems. This may result in a duplication of limited resources across agencies, who do not speak with each other, nor do they have access to each other's data. From a private industry perspective, this may translate to receipt of notices from multiple agencies, also impacting private industry resourcing. There is an opportunity for better data and intelligence sharing across all agencies to smooth this out and determine roles and responsibilities and/or ownership of specific investigations/typologies.

Poor delineation of the roles and responsibilities between LEAs also exacerbates industry concern around the proposed 'likelihood test' for tipping off. It is very difficult, if not impossible, to determine the likelihood of prejudicing a potential investigation given the number of siloed agencies. For example, the AFP may assure banks that a disclosure will not prejudice their investigations (or that they have no investigations on foot). But that's not to say a disclosure could inadvertently prejudice another agency's investigation, such as a small State based LEA.

**International collaboration**

The globalisation of trade has created interconnected networks that enable crime and funds to transcends borders, making it challenging for any single country to address money laundering and terrorism financing independently. Whilst acknowledging the jurisdictional challenges inherent in a law enforcement context, we encourage Australian law enforcement to strengthen collaboration with their global counterparts, sharing information and working together to disrupt international crime syndicates.

**Community messaging**

Messaging around financial crime red flags when shared with the general public is not always undertaken with consultation across industry, which may lead to gaps and inconsistencies in information and threat management. For example, there are multiple reporting channels put to the Australian public and private sectors relating to Financial Crime: AUSTRAC, AFCX, Crimestoppers, Scamwatch, ReportCyber. However, these platforms do not necessarily 'talk' to each other. Reconciliation and/or sharing information across these data sources may also go far in supporting the wider community in both identification and prevention of scams and money laundering and the disruption of other associated offences.

There is also an opportunity to leverage public awareness to develop new intelligence on financial crime. Significant money laundering cases, proceeds of crime action and AUSTRAC action seem to capture the public's attention. With a receptive audience and a clear and engaging communication strategy, the Australian public can be harnessed to form a significant part of the effort to identify, report and disrupt financial crime. We therefore encourage law enforcement to share more successful disruption/prosecution cases.

Australian Banking Association

## f. Role and response of private sector, including awareness and assistance to LEA

*the role and response of businesses and other private sector organisations, including their level of awareness, assistance to law enforcement, and initiatives to counter this crime;*

The private sector plays a crucial role in the fight against financial crimes, leveraging their capability and resources to assist law enforcement, particularly through the sharing of information. However, subject matter expertise and maturity will differ dependent on the industry (see comments on tranche 2) which impacts the quality of reporting provided that may lead to triggering an investigation. While FIs maintain a sophisticated awareness of financial crime risks and have implemented robust controls to counter such activities, the reluctance of law enforcement to leverage information from other entities, such as social media/digital platforms, represents a missed opportunity. LEAs should expand direct engagement opportunities with the architects of these new and largely complex private sector organisations to better understand the technology behind these organisations and how it may support law enforcement. This will, in turn, enhance the value of the assistance provided to law enforcement initiatives by these organisations. Responding to money laundering and financial crime requires a whole-of-ecosystem approach to avoid criminals simply pivoting to target organisations with weaker AML/CTF systems or organisations subjected to less regulation or law enforcement action.

Public and private partnerships are one way of working through these challenges, however, there also needs to be consideration of legislative change implications including tipping off, privacy and Commonwealth agency information sharing powers to determine other instances where intelligence sharing is allowed or could be enhanced to assist law enforcement. Please refer to comments above.

## g. Operation of unexplained wealth and asset recovery legislation

*the operation of unexplained wealth and asset recovery legislation, the Criminal Assets Confiscation Taskforce, and the Confiscated Assets Account; and*

Ordinarily police may engage with banks during an investigation and indicate their intention to act against property. There has been a welcome shift towards early engagement. However, where banks identify potential unexplained wealth or proceeds in customer products, LEAs may not always be adequately equipped to receive this information directly and respond in a timely manner or at all. To increase the capacity of LEAs to respond and encourage deeper engagement with the private sector, we recommend additional resourcing.

There are times where the private sector may identify significant holdings believed to be linked to a predicate offence and/or money laundering. Where the AFP Criminal Asset Confiscation Taskforce (CACT) is engaged proactively, there may be challenges to meet evidentiary requirements to seize assets in a timely manner (including submitting notices to freeze accounts and/or assets). This may result in missed opportunities to recover the proceeds of crime because of the complexity and requirements involved in asset seizure.

Australian Banking Association

## h. Any related matters.

From a private sector perspective, banks invest heavily in their control environments and in reporting to AUSTRAC. Similarly, we recognise the importance of LEAs having the necessary resources to effectively utilise and act on the intelligence provided by banks and other REs. Ensuring appropriate investment in these agencies will enable them to support institutions (including incoming tranche 2 entities) more effectively in identifying, understanding, and managing their risks. This includes sharing guidance, typologies, and insights with institutions, as well as providing timely responses to their questions. To enhance the capacity of LEAs to foster deeper engagement with the private sector, we recommend considering additional resourcing for these agencies.

Policy contact:

### About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.