GRIFFITH UNIVERSITY

Submission to the Inquiry into Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024

To: Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

11 October 2024

Dear Sir/Madam,

RE: Submission to Inquiry into Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024 [Provisions]

We appreciate the invitation to participate in this consultation exercise. This submission was co-authored by the following researchers and practitioners:

- Professor Andreas Chai, Director, Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University
- Dr Andrew Childs, Lecturer, School of Criminology and Criminal Justice, Griffith University
- Dr Gordon Hook, Industry Fellow, Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University
- Professor Shireenjit Johl, Deputy Director, Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University
- Dr Ingrid Millar, Lecturer, Department of Accounting, Finance and Economics, Griffith Business School, Griffith University
- Associate Professor DaiFei (Troy) Yao, Associate Professor, Department of Accounting, Finance and Economics, Griffith Business School, Griffith University

1. Schedule 4: The Australian legal profession and legal professional privilege

The AML/CTF Bill contains measures to address concerns expressed by the Australian legal profession about the impact of an AML/CTF reporting and supervisory regime on the fundamental principle of legal professional privilege. The Bill aims to address those concerns while at the same time paying deference to the concerns of the profession.

This note reviews the measures proposed in the Bill and highlights weaknesses in those provisions against the strict requirements of the FATF standards.

Background

It is important to highlight, again, the context and materiality of the AML/CTF regime and its overall compliance with the FATF Recommendations. These Recommendations establish the minimum requirements to be met by Australia to be deemed technically complaint and effective in its performance to mitigate money laundering and terrorist financing/proliferation risks.

The high-level objective of any AML/CTF system is to ensure that financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism/proliferation, thereby strengthening financial sector integrity and contributing to safety and security.

Australia is an important regional financial centre. Weaknesses in Australia's AML/CTF system in turn weakens the regional financial system and poses a risk to the international financial system. Criminal actors target weak systems to exploit in order to conceal and disguise criminal proceeds from law enforcement authorities. In addition to the threats posed by a weak Australian AML/CTF system, Australia faces reputational damage by continuance of weak-to-non-existent money laundering and terrorist financing controls in a large sector of its economy – the tranche II entities.

The new FATF assessment methodology (2024) states that the assessment of the effectiveness of a country's AML/CTF system is equally as important as the assessment of a country's technical compliance with the FATF Recommendations. While effectiveness criteria and performance measures have been a part of the FATF standards since 2012, the new round of evaluations commencing in 2024 will place greater emphasis of effectiveness; in other words, the extent to which Australia's AML/CTF system is producing real and measurable outcomes in terms of reducing serious financial crime and financial crime risk.

To prevent the proceeds of crime and funds in support of terrorism from entering the financial and other sectors, or are detected and reported by these sectors, Immediate Outcome 4 in the FATF standards requires that:

> *Supervisors appropriately supervise, monitor and regulate DNFBPs for compliance with AML/CFT requirements, and DNFBPs adequately apply AML/CFT preventive measures commensurate with the risks, and report suspicious transactions.*

Legal Professional Privilege in Australia

The Law Council of Australia describes legal professional privilege on their website as follows[1]:

> *Client legal privilege (CLP), often referred to as "legal professional privilege", is a common law right that exists to protect the administration of justice and the right of individuals and other entities/organisations to obtain confidential advice about their legal circumstances. It protects legal advice given by a lawyer to his or her client (advice privilege) and communications pertaining to actual or contemplated litigation or court proceedings (litigation privilege). … The proper administration of justice requires that clients are able to communicate freely and frankly with their lawyer, without fear of disclosing any information relevant to the legal advice they are seeking. … It is in society's interest that people (including corporations) seek legal advice about their affairs and in seeking advice feel free to disclose all relevant facts. The complexity of these laws is coupled with increasing reliance on self-regulation by the community, for example the self-assessment system of taxation.*

As highlighted, the focus of the privilege is on protecting *advice* provided by a lawyer to a client and *communications* in the context of possible or actual litigation. The scope of advice and communications between the lawyer and client is not defined. For instance, how far is the concept of advice to be taken within the lawyer and client relationship? Is it meant to encompass facts conveyed by the client to the lawyer, or is advice limited to the statements made by the lawyer in regard to those facts?

In relation the Tranche II reforms, the Law Council made the following remarks in the context of possible reforms in 2008[2]:

> *…the Law Council opposes in principle reforms which go further and require legal practitioners to secretly inform [i.e., file suspicious matter reports] on their clients to regulatory agencies.*

Australia's Money Laundering Risk Assessment 2024 and the Legal Profession

The money laundering risks associated with Tranche II entities were recently assessed by Australia to be either 'high' or 'very high' as reflected in Australia's recent National Risk Assessment[1]. The same levels of risks were noted in an earlier 2014 national level threat assessment. Hence, the Australian government has been aware of these risks for almost a decade, if not longer.

The legal profession is required by the FATF to be a reporting and supervised entity for all purposes under the FATF standards as a DNFBP. Like-minded countries, including New Zealand and the United Kingdom, have included the legal profession within their suspicious transaction reporting regime for some time. In New Zealand, in particular, lawyers have been obligated to file suspicious transaction reports for almost 30 years since the enactment of the Financial Transactions Reporting Act, 1996. Their legal profession has been the subject of supervisory

[1] https://lawcouncil.au/policy-agenda/regulation-of-the-profession-and-ethics/client-legal-privilege.

[2] https://lawcouncil.au/policy-agenda/regulation-of-the-profession-and-ethics/anti-money-laundering/tranche-two-reforms-and-consultation.

oversight for AML/CFT compliance by the Department of Internal Affairs in conjunction with the New Zealand Law Society since 2018. The New Zealand profession does not consider that AML/CTF reporting and regulatory obligations to be an infringement of legal professional privilege.

Despite ongoing commitments by Australia to implement risk-mitigation measures in relation to the legal profession (as well as other Tranche II entities) Australia has failed to meet its domestic and international obligations and to address the risks to protect the integrity of its own economy from the negative effects of criminal proceeds. Recently, in mid-2024, Australia assessed the risk posed by the legal profession for money laundering and terrorist financing as "High," posing a "stable money laundering vulnerability" relating to (p. 81):

- The use of trust and other accounts to deposit, hold and disburse client funds;
- The facilitation of real estate, business and asset transactions including purchase, sale, transfer of ownership and financing arrangements; and
- The assistance is establishing and administering complex domestic and offshore legal structures (including trusts and companies, the use of straw directors and nominee shareholders).

The absence of customer due diligence (CDD) obligations under the AML/CTF Act exacerbates this risk, according to the report.

The NRA of 2024 specifically mentions legal professional privilege and states that "access to .... documents [held by lawyers] is limited and ... may attract claims of legal professional privilege." (p. 93). In Australia's 2015 FATF mutual evaluation report[2], it was highlighted that Designated Non-Financial Businesses and Professions (DNFBPs) including lawyers, are:

- not subject to requirements to file Suspicious Transaction Reports (STRs) with AUSTRAC;
- not required to implement internal controls including the full range of CDD, record keeping;
- not required to undertake internal risk assessments of clients/customers; products; and delivery channels and put in place risk-based measures for higher risk customers and clients; and
- not supervised by AUSTRAC or other agency for compliance with these FATF requirements.

In the most recent FATF follow-up report in April 2024[4], the same comments appear in relation to Australia, highlighting the on-going concerns the FATF and the global community has with respect to the weaknesses in Australia's AML/CTF system.

Legal Professional Privilege in the Draft Bill

The provisions in the new bill are designed to address the concerns of Australia's legal profession relating to legal professional privilege and provide as follows:

> *(2A) Despite subsection (2), the reporting entity may refuse to give the AUSTRAC CEO a report about the matter if the reporting entity reasonably believes that all of the information comprising the grounds on which the reporting entity holds the relevant suspicion is privileged from being given on the ground of legal professional privilege.*
>
> ***242 Legal professional privilege***
>
> *(1) Nothing in this Act affects the right of a person to refuse to give information (including by answering a question) or produce a document if:*
>
> *(a) the information would be privileged from being given on the ground of legal professional privilege; or*
>
> *(b) the document would be privileged from being produced on the ground of legal professional privilege.*
>
> *(2) The fact that a person has provided a description of information or documents that may be or are privileged from being given or produced on the ground of legal professional privilege does not, of itself, amount to a waiver of the privilege.*
>
> ***242A Guidelines in relation to legal professional privilege***
>
> *(1) The Minister may, by notifiable instrument, make guidelines in relation to making or dealing with claims or assertions of legal professional privilege in relation to information or documents required to be given under or for the purposes of this Act.*
>
> *(2) Without limiting subsection (1), the guidelines may deal with the following matters:*
>
> *(a) arrangements for making or dealing with claims or assertions of legal professional privilege in relation to the exercise of other powers under this Act, including the use of LPP forms;*
>
> *(b) facilitating the resolution of disputes in relation to legal professional privilege.*
>
> *(3) Before making guidelines under subsection (1), the Minister must consult with such persons (if any) as the Minister considers appropriate.*

If issued, the FATF will examine these provisions for the purposes of determining whether they comply with the requirements of the FATF Recommendations. Given that there is no definition or functional description in the Bill of what amounts to that scope of legal professional privilege, legal professionals may refuse to provide information or documents asserting privilege in any given situation. There does not appear to be a mechanism in the Bill for AUSTRAC to challenge that assertion in order to determine whether a refusal to file a report is within the limited scope of the privilege as outlined by the Law Council cited earlier (advice and/or communication within the context of litigation).

Moreover, the Minister's guidelines under proposed subsection 242A(1) will not be enforceable for the purposes of the FATF standards. Those standards outline what requirements are needed for instruments, such as guidelines, to be considered enforceable. In short, they must contain a range of effective penalties and sanctions for non-compliance. Absent those measures, the guidelines can be ignored.

Conclusion

It is likely that the draft provisions touching on legal professional privilege in the Bill will not yield effective risk mitigation outcomes within the context of the AML/CTF requirements in Australia.

Australia runs the risk that the regime affecting lawyers will fail both technically and on an effective performance basis within the FATF standards. Without enforceable requirements on lawyers to file suspicious matter reports with AUSTRAC and a regime of supervision to ensure compliance with those obligations, the Bill in its current form will not address Australia's international obligations with no measurable outcomes in relation to mitigating ML and TF risk in the legal profession.

2. Promoting Greater Information Sharing Arrangements between regulated entities, AUSTRAC and universities

For regulated entities to effectively mitigate financial crime risks, it is crucial that they have the capacity to identify and detect risks in the context of their business operations. Currently there is limited research on financial crime typologies and how they evolve as new technologies emerge. The proposed legislation will magnify this challenge as a new range of tranche II entities will be required to report to suspicious activities. Money laundering typologies can be highly sophisticated and by their nature difficult to detect. For this reason, it is vital to for these businesses to access publicly available insights and subject matter experts that can help organisations develop assessment and prevention strategies.

To address this challenge, we propose that amendments be made to enable University-based researchers based in Australia to work with tranche II entities to access relevant data for the purpose of identifying and preventing financial crime. University researchers from a range of disciplines, including criminology, accounting and ICT, are in an excellent position to conduct foundational research that can generate new knowledge about financial crimes such as money laundering, terrorist financing, and fraud. Increasing information sharing arrangements and collaboration opportunities will help to ensure a wide variety of regulated entities improve their approaches to monitoring and reporting suspicious behaviour, as well as conducting risk assessments.

Case Study: A proposal for a Financial Crime Data collaborative

The Academy of Excellence in Financial Crime Investigation and Compliance based at Griffith University is seeking to establish a National Data Collaborative for financial crime in partnership between multiple organisations across the public and private sector. This would utilise a secure air gapped data facility designed to meet Australian Government information security requirements. The facility has securely housed sensitive data for close to a decade and is currently pursuing accreditation as an Accredited Data Service provider under the Data Availability and Transparency Act. Linking data across multiple financial institutions and government entities can help highlight the need for a 'multibank' monitoring approach (FATF 2022). These collaborative arrangements have enormous potential in yielding insights into financial crime typologies and designing preventive measures to protect customers and communities. Internationally, similar arrangements have been developed in the Netherlands, the United States and Germany where universities have received de-identified data and developed relevant insights (FATF 2022).

The amendments we propose are in line with recent Financial Action Task Force (FATF) positions that have called on member countries to consider taking an active facilitation role in private sector information sharing initiatives, for example by updating laws or supervisory instruments as necessary; making use of regulatory sandboxes and pilot programmes; highlighting areas, typologies or data types that would benefit from sharing, noted by the FATF:

> *"Collaboration and information sharing helps financial institutions to build a clearer picture of criminal networks and suspicious transactions, and better understand, assess, and mitigate their money laundering (ML), terrorist financing (TF) and*

proliferation financing (PF) risks. It can also provide authorities with better quality intelligence to investigate and prosecute these crimes and ultimately help prevent crime from reaching our streets."[3]

As highlighted by FATF (2022), a good example of such a provision is the Section 314(b) of the USA PATRIOT ACT:

> *Section 314(b) of the USA PATRIOT ACT provides that two or more financial institutions and any association of financial institutions may share information with one another regarding individuals, entities, organisations, and countries suspected of possible terrorist or money laundering activities. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities shall not be liable to any person under any law or regulation of the US, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the disclosure.*

To promote greater information sharing, subsection 123(5) states that the tipping offence does not apply if disclosure is made to another reporting entity for the purposes of detecting, deterring or disrupting financial crime.

We propose an amendment to 123(5) should be amended that enables reporting entities to share information with universities for research purposes. The proposed amendment to 123(5) is as follows:

> *(e) Subsection (1) does not apply if:*
> - *(a) the disclosure is made to another reporting entity or university engaged in research related to crime prevention; and*
> - *(b) the disclosure is made for the purpose of detecting, deterring, or disrupting money laundering, the financing of terrorism, proliferation financing, or other serious crimes; and*
> - *(c) the conditions prescribed by the regulations are met.*

RECOMMENDATION: We encourage amendments to 123(5) to enable reporting entities and public entities to share information and collaborate with universities and promote research in crime prevention.

[3] FATF (2022), Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing, FATF, Paris, France, https://www.fatf-gafi.org/publications/digitaltransformation/documents/partnering-in-the-fightagainst-financial-crime.htm

3. AML /CTF Capacity Building through Ongoing Training

Training is critical for combating money laundering and terrorism financing because it equips employees with the knowledge and skills to fulfill their obligations under the AML/CTF Act and Rules. The current Bill on AML/CTF Act and Rules highlight the necessity of training programs to ensure employees understand these obligations, the potential consequences of non-compliance, the specific ML/TF risks their entity faces, and the internal processes and procedures to manage these risks. Without adequate training, employees may unknowingly facilitate money laundering or terrorist financing activities, exposing their organisation to legal, financial, and reputational damage.

The current AML /CTF Amendment Bill has broad provision on training of employees under Division 3 AML/CTF Policies 26F:

> *(e) providing training to persons who are employed or otherwise engaged by the reporting entity and who perform, or will perform, functions relevant to the reporting entity's obligations under this Act in relation to:*
>
> *(i) the risk of money laundering, financing of terrorism and proliferation financing that the reporting entity may reasonably face in providing its designated services; and*
>
> *(ii) the obligations imposed by this Act, the regulations and the AML/CTF Rules on the reporting entity.*

Further, the current AML/CTF Rules 2007: Chapter 8 and 9 mandates that a reporting entity's AML/CTF program must include an AML/CTF risk awareness training program. The Rule also requires that the training program be provided "at appropriate intervals, having regard to ML/TF risk it may reasonably face." The provision of "appropriate intervals" allows for flexibility, but also creates subjectivity and laxness or opportunity to disregard the benefits of having a systematic and appropriate ongoing training program at regular intervals, preferably annual.

Prior studies consistently demonstrate that frequent and well-structured training improves performance, strengthens compliance systems, and enhances organisational safeguards against financial crime. Pérez-Bustamante Ilander et al. (2016), studying Spanish SMEs, introduced the concept of "training intensity" and found that high levels of training not only enhanced employee skills but also improved overall organisational performance through better planning, execution, and program evaluation.[4] Another study showed organisations that invest in continuous training see improved employee skills and knowledge, which directly correlates with better performance outcomes (Slaviæ & Berber, 2014).[5] In the context of AML prevention, Said et al. (2013) found that while Malaysian banks recognised training's importance in identifying suspicious activities and AML policy compliance, it remained one of the least adopted measures.[6] Mele (2018) also highlighted that smaller institutions face resource limitations, but regular training can mitigate these issues by equipping staff to meet compliance demands

[4] Pérez-Bustamante Ilander, G. O., Marques, C. S. E., Jalali, M. S., & Ferreira, F. A. F. (2016). The impact of continuous training in small and medium enterprises: Lessons from an industrial case analysis. Journal of Business Economics and Management, 17(2), 234–250

[5] Slaviæ, A. & Berber, N., (2014). The Impact of Training on Organisational Outcomes in the CEE Region – Focus on Hungary, Serbia, Slovenia and Slovakia, Proceedings- 11th International Conference on Management, Enterprise and Benchmarking (MEB 2014).

[6] Said, J., Ghani, E. K., Omar, N., & Yusuf, S. N. S. (2013). Money laundering prevention measures among commercial banks in Malaysia. International Journal of Business and Social Science, 4(5), 227–234

effectively.[7] In the legal sector, Kebbell (2022) found that ongoing, relevant training is essential for managing complex tasks like beneficial ownership verification, especially when dealing with intricate corporate structures, trusts, or offshore entities.[8] Matras (2023) echoed this, noting that ambiguity in the definition of beneficial ownership in Poland limited the effectiveness of the beneficial ownership register, calling for more targeted training to address this gap.[9] Similarly, Zavoli and King (2020) identified training as a critical issue for UK real estate agents, with many reporting insufficient preparedness to meet AML obligations. They emphasised the need for frequent, tailored training—some suggested three to four times per year—to help agents recognise red flags and navigate the complexities of customer due diligence (CDD) and suspicious activity reporting.[10]

Additionally, Australia has been rated by FATF as non-compliant regarding recommendation 34 on Guidance and Feedback, insofar as Australia does not provide sufficient guidance and feedback to regulated entities in applying measures to combat money laundering and terrorism financing. These findings suggest regular effective training raises awareness of red flags, empowers employees to identify suspicious transactions and ability to uncover the "real" beneficial owners in complex arrangements, and provides guidance on reporting procedures, ultimately strengthening the entity's AML/CTF framework.

RECOMMENDATION: Enhancement to the AML/CTF Amendment Bill and AML/CTF rules as outlined below.

AML/CTF Amendment Bill Division 3 AML/CTF Policies 26F:

> *(e) providing training to persons who are employed or otherwise engaged by the reporting entity and who perform, or will perform, functions relevant to the reporting entity's obligations under this Act in relation to:*
>
> *i. the risk of money laundering, financing of terrorism and proliferation financing that the reporting entity may reasonably face in providing its designated services; and*
>
> *ii. the obligations imposed by this Act, the regulations and the AML/CTF Rules on the reporting entity.*

AML /CTF Rules Instrument 2007 Part 8.2.2:

The AML/CTF risk awareness training program must be designed so that the reporting entity gives its employees appropriate training at appropriate intervals, having regard to ML/TF risk it may reasonably face.

[7] Mele, A (2018). Stretching anti money laundering resources at smaller institutions. Journal of Financial Compliance. Henry Stewart Publications, vol. 2(1), pages 53-59.
[8] Kebbell, S. (2022). Anti-money laundering compliance and the legal profession. Taylor & Francis Group
[9] Matras, T. M. (2023). Functioning of the register of beneficial owners: findings from Poland. Journal of Money Laundering Control, (ahead-of-print).
[10] Zavoli, I., & King, C. (2020). New development: Estate agents' perspectives of anti-money laundering compliance—four key issues in the UK property market. Public Money & Management, 40(5), 415-419

We propose:

1) **The wording "providing training" in the AML/CTF Amendment Bill be revised to "providing ongoing training."** Adding the word "ongoing" emphasises the need for not only training but also regularity /frequency, reinforcing the continuous nature of AML/CTF education.

2) **Enhancing the AML/CTF Rules to provide clear guidance on training frequency** by aligning training requirements with organisational size, as per definitions and metrics provided by the Australian Bureau Statistics, FairWork Australia, Australian Securities Investment Commission (ASIC), and Australian Treasury, to remove subjectivity. We propose the following structured approach:

   a) **Large entities**[11]: **Require quarterly training** for all employees who perform, or will perform, functions relevant to the reporting entity's obligations under the Act. Given the higher volume of transactions and a larger, potentially high-risk customer base, large organisations face increased AML/CTF risks and should receive more frequent training to stay updated on emerging risks and regulatory changes.

   b) **Medium-Sized Entities**[12]: **Require semi-annual training** for all employees who perform, or will perform, functions relevant to the reporting entity's obligations under the Act. This frequency strikes a balance between ensuring that employees are regularly updated on AML/CTF matters while accounting for the lesser complexity of medium-sized organisations compared to larger firms.

   c) **Small Entities (including micro entities and sole proprietors)**[13]: at minimum **require annual training**, for all employees who perform, or will perform, functions relevant to the reporting entity's obligations under the Act. This frequency maintains compliance while recognising resource constraints. However, additional ad-hoc training should be provided when significant changes occur, such as new regulatory requirements, new services, or identified weaknesses in the compliance program.

   In addition to the structured approach based on organisational size, further criteria should be explicitly included to prompt more frequent training, above the minimum requirement, when needed. These factors include legislative and regulatory changes, introduction of new products or services, identified weaknesses in internal controls or compliance programs, significant operational changes within the organisation, new employees or employees moving into new roles.

[11] e.g. with more than 100 employees, with assets over $25 million, and annual revenue turnover over $50 million

[12] e.g. employees with 16 - 99 employees, with assets up to $25 million, and annual revenue turnover up to $10 million

[13] e.g. employees fewer than 16 employees and annual revenue turnover of less than $10 million

4. Independent Review and External Audit for Enhanced Oversight

Regular mandated independent reviews and discretionary external audits are essential components of Australia's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) framework in ensuring entities remain compliant with their legal obligations and effectively mitigate risks related to money laundering and terrorism financing. The framework reflects both FATF's 40 Recommendations and Australia's own regulatory approach, offering flexibility through a risk-based model, while ensuring that entities, particularly those exposed to higher risks, conduct independent reviews at appropriate intervals.

The **AML/CTF Amendment Bill (Division 3 AML/CTF Policies 26F)** and the current **AML Rule (8.6**) only requires independent reviews as part of the routine internal control mechanisms required under Part A of the AML/CTF Program. These are routine reviews initiated by the reporting entity and not prompted by AUSTRAC. The reviews can be conducted internally by a department independent of the compliance function, or by an external reviewer. The interval, choice of whether the reviewer provider is internal or external and the scope of independent reviews are somewhat at the discretion of the reporting entity, based on its risk profile.

While not explicitly mentioned in the AML/CTF Rules, provisions for external audits exist under **Sections 161 and 162** of the AML/CTF Act which grants the AUSTRAC CEO the authority to require a reporting entity to appoint an external auditor to conduct an audit under specific circumstances such as suspicion of inadequate risk management (Section 161) or suspicion of non-compliance (Section 162). This indicates that external audits are only initiated at the discretion of the AUSTRAC CEO based on specific concerns. With the impending regulation of additional entities - DNFBPs, the burden on AUSTRAC to monitor for non-compliance will increase significantly, potentially straining its capacity to oversee a broader range of regulated entities.

Taking this together, while **independent reviews** are designed to enhance the effectiveness of AML/CTF programs, in its current form, they also present drawbacks. Here are some key issues:

> **Lack of Independence:** While Rule 8.6 of the AML/CTF Rules states that Part A of an AML/CTF program must be subject to regular independent review, it allows for these reviews to be conducted by either internal or external parties. If an internal party conducts the review, their objectivity could be compromised due to their inherent connection to the entity being reviewed. This lack of true independence could undermine the effectiveness of the review and limit its ability to identify weaknesses or provide objective recommendations for improvement.
>
> **Variability in Quality and Scope:** Because there is no standardised methodology or scope for independent reviews, it creates ambiguity on extent and depth of review. This lack of uniformity can lead to significant variations in the quality and depth of reviews conducted across different entities especially when they are carried out internally and lack the experience. So, you could have some reviews being comprehensive and rigorous, while others may be superficial and fail to identify critical weaknesses.

Further, if entities view independent reviews as a mere box-ticking exercise rather than an opportunity for genuine self-assessment and improvement, the effectiveness of the AML/CTF framework will be compromised.

The 2024 FATF 4th Enhanced Follow-up Report (FUR) indicates that Australia has made progress since the 2015 mutual evaluation report (MER) in addressing the technical compliance deficiencies identified in FATF Technical Recommendation 18 found in the 2015 MER. The 2015 MER highlighted the issues such as lack of clarity regarding frequency of "regular" reviews and the independence of internal reviews. While the 2024 MER reassessment confirms that these deficiencies have now been addressed, we continue to recommend further improvements for reasons pointed out in the earlier paragraphs. Periodic external independent audit is a key preventive mechanism that strengthens AML/CTF internal controls of reporting entities. Such audits would contribute to the overall effectiveness of a regulated entity's compliance framework, and in turn contributing to higher ratings in FATF's Immediate Outcomes 3 and 4 which focuses on supervision and preventive measures (as shown below). Currently Australia rating is ME (moderate level of effectiveness).

> *IO3. "Supervisors appropriately supervise, monitor and regulate financial institutions and VASPs for compliance with AML/CFT requirements, and financial institutions and VASPs adequately apply AML/CFT preventive measures, and report suspicious transactions. The actions taken by supervisors and by financial institutions and VASPs are commensurate with the risks".*
>
> *IO4. "Supervisors appropriately supervise, monitor and regulate DNFBPs for compliance with AML/CFT requirements, and DNFBPs adequately apply AML/CFT preventive measures commensurate with the risks, and report suspicious transactions".*

RECOMMENDATION: Revision to Division 3 AML/CTF Policies 26F 4(f) as shown below:

> *"the conduct of independent evaluations of the reporting entity's AML/CTF program, including the frequency with which such evaluations must be conducted, which must:*
>
> *(i) be appropriate to the nature, size and complexity of the reporting entity's business; and*
>
> *(ii) be at least once every 3 years;"*

And be replaced with:

1) **Mandated independent external audits be introduced with a tiered frequency based on size of the regulated entity.** We propose extending the use of Australian Bureau Statistics, FairWork Australia, Australian Securities Investment Commission (ASIC), and Australian Treasury size definition, to all regulated AML/CTF entities in order to remove subjectivity.

- For **Large entities**, **annual independent audits** be required to ensure consistent evaluation of AML/CTF program, internal controls, complex systems and high-risk activities.
- **Medium entities** should undergo **independent audits every two years**, allowing sufficient time to address compliance while still maintaining strong oversight.
- **Small entities (including micro and sole proprietor)** should undergo **independent audits every three years**, allowing sufficient time to address compliance while still maintaining strong oversight and reducing the compliance burden.

This approach removes the discretionary nature of frequency and reviewer independence. Additionally, it aligns with the risk-based framework, ensuring that entities of all sizes are subject to audits proportionate to their risk and operational scale, balancing compliance demands with the regulatory burden for small businesses.

5. Response to 5B Meaning of Virtual Asset

Introduction

Clear definitions of *virtual assets* are integral to supporting innovation in the digital economy. Critically assessing how virtual assets are defined – and which are excluded – will help strike the right balance between effective regulation, new cybercrime threats, and the ability to foster growth in emerging technologies and digital environments. Subsection 5B explicitly excludes the following from being classified as a virtual asset: (1) Money, (2) A digital representation of value used exclusively within an electronic game, (3) Customer loyalty or reward points. It is crucial to examine the potential implications of these exclusions to prevent undermining the AML/CTF regime and avoid creating loopholes that cybercriminals could exploit for money laundering.

Not all 'fun and games': The Money Laundering Risks of Online Gaming Economies

The money laundering implications of online gaming economies were signposted over a decade ago[14], and yet, there are still no clear expectations of how online game developers should adhere to regulations regarding criminal activity. Assets like cryptocurrencies and NFTs are increasingly being incorporated into financial crime regulatory frameworks worldwide. However, in-game currencies and virtual items within online gaming ecosystems function much like virtual assets, often sharing similar characteristics but mostly lacking the same regulatory oversight. Online gaming economies have evolved in ways that have not been anticipated by AML/CTF frameworks.

The online gaming industry continues to expand with billions of dollars in transactions worldwide[15]. The financial flows through online gaming platforms are now so significant that, as recent as April 2024, the Consumer Financial Protection Bureau in the USA issued a report highlighting how some games (and their wider markets and infrastructure) now resemble traditional banking and payment systems[16]. Online gaming platforms generate their own digital economies in two primary ways:

- *Microtransactions*: This is a model where users make small payments, ranging from a few cents to several dollars, to purchase virtual goods within a game. These microtransactions allow players to buy in-game items such as cosmetic enhancements (e.g. character 'skins', weapon designs), power-ups, additional levels, or other digital content. Microtransactions have become a significant revenue stream for most major game developers and publishers[17].

[14] Richet, J. L. (2013). Laundering Money Online: a review of cybercriminal methods. ArXiv preprint arXiv:1310.2368

[15] https://www.statista.com/topics/1551/online-gaming/

[16] https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-video-games/

[17] https://www.statista.com/statistics/274761/electronic-arts-ea-extra-content-revenues/, https://www.thegamer.com/26-ea-revenue-game-sales/, https://www.tweaktown.com/news/84430/sony-made-over-2-billion-from-microtransactions-in-holiday-2021/index.html, https://www.asiabusinessoutlook.com/perspective/microtransactions-an-important-aspect-of-the-gaming-industry-and-business-nwid-2107.html#:~:text=In%20today%27s%20gaming%20world%2C%20in,%242B%20annually%2C%20and%20the

- Loot Boxes: Loot boxes are mystery packages that players can acquire using in-game credit or real money that offer a random assortment of items. Loot boxes differ from standard microtransactions in that they do not guarantee a specific item, and therefore, many regulators and consumer protection agencies around the world have cracked down on these gambling-like practices[18],[19].

The exclusion of digital representations of value used within online games warrants careful reconsideration. Academic research into the processes of money laundering with digital technologies has consistently shown that the use of large amounts of smaller value transactions to mask the true origins of funds is a key strategy for money launderers[20]. There are various methods by which money laundering can occur in video games [21] and online gaming is increasingly targeted by cybercriminals because of the lack of regulation in online gaming economies[22].

The proposed AML/CTF exclusion ignores how the lines between *in-game* and *real-world* economies are increasingly blurred when players engage in practices like skin trading, gold farming, and account trading. In these practices, players will accumulate in-game currencies or items, either by engaging in repetitive tasks, botting, or purchasing items through microtransactions and loot boxes. These accounts, in-game items, or in-game currencies are then able to be sold for fiat currency. As an interesting example of this, economic hardships led individuals in Venezuela to accumulate in-game currency in RuneScape and then sell this in-game gold for fiat currency[23]. These practices demonstrate the emerging avenues for money laundering.

These sales between game players for trades happen through either primary or secondary marketplaces:

1. *Primary marketplaces*: Game developers operate their own marketplaces or allow direct trading between player accounts. Valve Corporation, the developer of the popular *Counter-Strike* games, faced concerns over money laundering and fraud within its marketplace which subsequently led to policy changes. They stated at the time that *"nearly all of the key purchases that end up being traded or sold on the marketplace are believed to be fraud-sourced"*[24].

[18] Xiao, L. Y., Henderson, L. L., Nielsen, R. K. L. & Newall, P. W. S. (2022). Regulating gambling-like video game loot boxes: a Public Health Framework Comparing Industry Self-Regulation, Existing National Legal Approaches, and Other Potential Approaches. *Current Addiction Report, 9*, 163-178. https://link.springer.com/article/10.1007/s40429-022-00424-9

[19] https://agbrief.com/news/australia/20/09/2024/australia-tightens-regulations-on-loot-boxes-and-gambling-features-in-video-games/

[20] Tiwari, M., Gepp, A. & Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review, 32*(3), 271-303. https://pure.bond.edu.au/ws/files/35590645/AM_A_Review_of_Money_Laundering_Literature.pdf

[21] Higgs, S. & Flowerday, S. (2024). Towards definitive categories for online video game money laundering. *Journal of Money Laundering Control.* https://www.emerald.com/insight/content/doi/10.1108/JMLC-12-2023-0193/full/html

[22] Wronka, C. (2022). "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control, 25*(2). https://www.emerald.com/insight/content/doi/10.1108/JMLC-04-2021-0035/full/html

[23] https://www.polygon.com/features/2020/5/27/21265613/runescape-is-helping-venezuelans-survive

[24] https://www.vice.com/en/article/nearly-all-counter-strike-microtransactions-are-being-used-for-money-laundering/

2. *Third-party marketplaces*: These platforms operate without support or affiliation from game publishers. Websites like PlayerAuctions (https://www.playerauctions.com), EpicNPC (https://www.epicnpc.com), U7BUY (https://www.u7buy.com), and Gaming4EZ (https://www.gaming4ez.com) facilitate account trading, item auctioning, and the ability to transact fiat currency for in-game currencies. These platforms can be easily exploited for money laundering purposes due to a lack of oversight and regulation.

The financial flows through online games are considerably more complex than the proposed AML/CTF subsection suggests. These examples illustrate the various ways that value represented in online video games can, and historically has, been exploited for money laundering purposes. While some gaming operators, such as Linden Lab which operate the virtual world and game *Second Life*, have responded by enforcing anti-money laundering regulations[25], the global and digital nature of gaming economies along with the significant rise of games with microtransactions for items, poses significant future challenges for money laundering and cybercrime more generally. This highlights the need for comprehensive regulatory approaches that do not exclude digital representations of value used within electronic games.

The Money Laundering Risks of Customer Loyalty and Rewards Points

Customer loyalty programs have become ubiquitous across industries, and in Australia, around 90% of adults are enrolled in at least one loyalty scheme[26]. Although they were initially designed as closed-loop systems, these programs have evolved into quasi-payment instruments with broader functionalities which increases their susceptibility to cybercriminals and money laundering[27]. The cross-border nature of many loyalty programs, combined with a lack of stringent regulations on the accumulation, transfer, and redemption of points, makes them vulnerable to illicit activities like money laundering. Loyalty-program fraud is a recognised issue, with analyses revealing that travel and hospitality rewards programs are often found for-sale on dark web marketplaces[28]. Goldbarsht (2022)[29] also highlighted how frequent-flyer programs can be exploited for money laundering and noted how they share characteristics with convertible virtual currencies due to the ability to exchange miles for cash, goods, and services.

Moreover, there has been an increase in account takeover incidents within loyalty programs, which directly raises the risk of these platforms and accounts being used for money laundering. The Veriff Identity Fraud Report (2024)[30] demonstrated an increase in identity fraud rates from the payments industry, which included loyalty programs, rose from 4.07% in 2022 to 6.28% in 2023. There has also been several high-profile data breaches in relation to loyalty programs in Australia:

---

[25] https://www.itnews.com.au/news/virtual-world-second-life-to-enforce-anti-money-laundering-regs-527558
[26] https://www.statista.com/statistics/1400149/australia-what-brand-loyalty-means-to-consumers/
[27] Dostov, V. & Shust, P. (2014). Customer loyalty programs: money laundering and terrorism financing risks. *Journal of Money Laundering Control, 17*(4). https://www.emerald.com/insight/content/doi/10.1108/JMLC-06-2013-0021/full/html
[28] Ganan, C. H., Akyazi, U. & Tsvetkova, E. (2020). Beneath the radar: Exploring the economics of business fraud via underground markets. *2020 APWG Symposium on Electronic Crime Research (eCrime)*. https://ieeexplore.ieee.org/abstract/document/9493263
[29] Goldbarsht, D. (2022). Virtual currencies as a quasi-payment tool: the case of frequent-flier programs and money laundering. *Journal of Money Laundering, 25*(1). https://www.emerald.com/insight/content/doi/10.1108/JMLC-11-2020-0127/full/html
[30] https://www.veriff.com/fraud/learn/five-key-takeaways-from-the-veriff-fraud-report-2024#

- In 2023, up to 1.5 million customers of *The Good Guys* had their data leaked in a data breach related to a loyalty programme[31]
- In 2023, Dymocks experienced a data breach related to its loyalty programme[32]
- In 2024, Qantas investigated reports of a data breach in its loyalty app[33]
- In 2024, A Shell data breach exposed Australian customers' personal information related to a customer loyalty program[34]

These breaches and risks not only jeopardise personal data, but also give malicious actors access to loyalty accounts with accumulated points or credits. Criminals can exploit these compromised accounts to transfer or redeem points for goods and services, which can then be sold or laundered for real-world money which effectively turns loyalty points into a medium for money laundering.

Excluding loyalty programs from the AML/CTF scheme overlooks a significant area where stored value rivals that of financial institutes but operates without equivalent oversight. As these programs continue to grow and potentially integrate with crypto and blockchain technologies (as indicated by ACCC's 2019 report into Customer loyalty schemes[35]) it is imperative to consider their inclusion in financial crime regulation to prevent exploitation in the evolving digital economy.

[31] https://www.itnews.com.au/news/the-good-guys-warns-of-customer-data-leak-591237
[32] https://www.dymocks.com.au/customer-notices/communications_20231004
[33] https://money.usnews.com/investing/news/articles/2024-04-30/australias-qantas-probing-reports-of-data-breach-at-frequent-flyers-app
[34] https://www.cyberdaily.au/security/10639-aussies-affected-in-alleged-shell-fuel-data-breach
[35] https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF

GRIFFITH UNIVERSITY
QUEENSLAND AUSTRALIA

CRICOS: 00233E | TEQSA: PRV12076

griffith.edu.au

MAKE IT MATTER