

Anthony Quinn,  
Arctic Intelligence,  
36a Hickson Road,  
Sydney, NSW 2000.

13<sup>th</sup> May 2024

Attorney General's Department  
[economiccrime@ag.gov.au](mailto:economiccrime@ag.gov.au)

## **Reforming Australia's anti-money laundering and counter-terrorism financing regime**

Dear Sir/Madam,

On behalf of Arctic Intelligence, I would like to thank the Attorney-General's Department (AGD) once again for the opportunity to contribute to the public consultation on proposed reforms of Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime and participating in the planned roundtable discussions should the opportunity arise.

This submission builds upon the [previous submission](#) that was made nearly one-year ago on 1 June 2023 and whilst we appreciate the AGD has received a large number of submissions, the level of communication from the AGD about the timetable for further consultations was frankly non-existent and would appreciate (like the rest of the Australian AML/CTF practitioner community) much more transparency on the steps and timing of the process following this submission.

Further it is important to note that the AGD is running at least six-months behind its own timetable for this second-round of consultations and has been criticised publicly by the AML/CTF community and in Parliament by Greens Senator David Shoebridge who summed it up well, "*so it's a consultation, on a consultation, on a consultation*", which I believe underpins the general sentiment that the AGD should work with more haste and ensure that new AML/CTF laws are passed before the end of 2024.

This is especially important given the context as successive Australian Governments have repeatedly failed to introduce these reforms over a 16 year-period, when 99% of the other countries in the world have managed to do and as you rightly point out that is against a backdrop of billions of dollars every year in Australia being generated through illegal activities such as drug trafficking, tax evasion, people smuggling, cybercrime, arms trafficking and other illegal and corrupt practices – there is simply no more time to waste.

This submission has been broken down into the following sections, summarised into the areas where Arctic agrees and disagrees with the AGDs proposed position:

- Appendix 1 – Summary of our second-round consultation paper review and responses
- Appendix 2 – Comments on the broader reforms to simplify, clarify and modernise the regime (Paper 5)
- Appendix 3 – Real Estate Professionals (Paper 1)
- Appendix 4 – Professional Services Providers (Lawyers, Accountants, TCSPs) (Paper 2)
- Appendix 5 – Dealers in precious metals and precious stones (Paper 3)
- Appendix 6 – Digital Currency Exchange Providers (DCEPs), remittance service providers and FI's

If you would like further clarification or information on anything contained in my submission, please do not hesitate to contact me and I welcome the opportunity to participate in the round table discussions and subsequent consultation processes as these critical reforms are overhauled.

Yours sincerely,



Anthony Quinn - Founder/CEO - Arctic Intelligence and the Arctic Intelligence Team  
[Anthony.Quinn@arctic-intelligence.com](mailto:Anthony.Quinn@arctic-intelligence.com) / +61(0) 431 157006

## Appendix 1 – Summary of our second-round consultation paper review and responses

In this appendix, we have provided a reference section to the document outlining where we agree with the AGDs proposals with nothing to add, also where we agree but have further comments to add and where we disagree with our comments, so that it makes it easier to navigate to the main sections of interest.

## Appendix 2 (Paper 5) – Comments on the broader reforms to simplify, clarify and modernise the regime

Ref	Area	Topic	Arctic View
2.1	AML/CTF Programs	An overarching risk assessment obligation	Agree (with comments)
2.1.1	AML/CTF Programs	Establishing ML/TF risk assessment as a clearly mandated requirement	Agree (with comments)
2.1.2	AML/CTF Programs	Establishing the nature, size, and complexity of the organisation in EWRA	Agree (with comments)
2.1.3	AML/CTF Programs	Documenting the ML/TF risk assessment methodology	Agree (with comments)
2.1.4	AML/CTF Programs	Defining a baseline of risks that must be identified and assessed	Agree (with comments)
2.1.5	AML/CTF Programs	Reporting entities to only conduct risk assessments every 4 years	Disagree
2.1.6	AML/CTF Programs	Reporting entities to keep the risk assessment up to date based on triggers	Agree (with comments)
2.1.7	AML/CTF Programs	Board to approve the risk assessment and be informed of updates	Agree (with comments)
2.2	AML/CTF Programs	Proportionate risk measures	Agree (with comments)
2.3	AML/CTF Programs	Reporting entities to maintain internal controls	Agree (with comments)
2.4	AML/CTF Programs	Establishing a new “business group” concept and group-wide risk mgmnt.	Agree (no comments)
2.5	AML/CTF Programs	Simplified obligations for foreign branches and subsidiaries	Agree (with comments)
3.1	Customer DD	Applying a customer risk rating to each customer	Agree (with comments)
3.2	Customer DD	Refining requirements for ongoing CDD	Agree (with comments)
3.3	Customer DD	Confirming when enhanced CDD must apply	Agree (no comments)
3.4	Customer DD	Streamlining the application of simplified CDD	Agree (with comments)
3.5	Customer DD	Additional measures	Agree (with comments)
3.6	Customer DD	Defining a “business relationship” and “occasional transaction”	Agree (with comments)
4	-	Exception for assisting in an investigation of a serious offence	Agree (no comments)
5	-	CDD exemption for gambling service providers	Agree (with comments)
6	-	Tipping Off Offence	Agree (no comments)
7	-	Moving some exemption from the Rules to the Act	Agree (no comments)
8	-	Repealing the Financial Transaction Reports Act 1988	Agree (no comments)
9	Other Matters	There were several items raised in the 1 <sup>st</sup> round that remain unanswered	-
9.1	Other High-Value Dealers	Include other high-value goods dealers in the AML/CTF regime	AGD to provide detail
9.2	Independent Review Requirement	Explicit guidance that AML/CTF Programs must be subject to independent review at least every two years (or annually for higher risk businesses)	AGD to provide detail

## Appendix 3 (Paper 1) – Real Estate Professionals

Ref	Area	Topic	Arctic View
3.1	Scope of AML/CTF laws	Exclusion of residential tenancies, property management and leasing of commercial real estate	Disagree
3.2	Implementation time	Lacking detail on the commencement date or assisted compliance period	AGD to provide detail
3.3	Explicit EWRA for real estate sector	Develop and maintain an AML/CTF program based on a risk-based approach	AGD to provide detail
3.4		Detailed AML/CTF program requirements	Agree (with comments)
3.5		Regulatory relief for pre-commencement customers	Disagree

## Appendix 4 (Paper 2) – Professional Services Providers (Lawyers, Accountants, TCSPs)

Ref	Area	Topic	Arctic View
4.1	Use of language	Use term DNFSBPs rather than PSPs (and other language differences)	Disagree
4.2	Scope of PSP	The scope of Professional Service Providers	Agree (no comments)
4.3	Scope of PSP	The scope of “designated services” provided by PSPs (DNFSBPs)	Disagree
4.4	Deadline to comply	Lacking detail on the commencement date or assisted compliance period	AGD to provide detail
4.5	Legal Privilege	Legal and professional privilege	Agree (no comments)
4.6	Deadline to comply	Extended timeline for reporting for legal professionals	Disagree
4.7	Transitioning laws in	Regulatory relief for pre-commencement customers	Disagree
4.8	Transitioning laws in	Transitioning existing customers into the regime	Disagree

## Appendix 5 (Paper 3) – Dealers in precious metals and precious stones

Ref	Area	Topic	Arctic View
5.1	Expand law to other high-value dealers	Dealers in precious metals and precious stones are not the only high value goods	Disagree
5.2	Scope of the laws	Reducing the threshold from \$10,000 to \$5,000	Disagree
5.3	Deadline to comply	Lacking detail on the commencement date or assisted compliance period	AGD to provide detail
5.4	Transitioning laws in	Regulatory relief for pre-commencement customers	Agree (no comments)
5.5	Transitioning laws in	Transitioning existing customers into the regime	Agree (no comments)

## Appendix 6 (Paper 4) – Digital Currency Exchange Providers (DCEPs), remittance service providers and financial institutions

Ref	Area	Topic	Arctic View
6.1	Scope of AML laws	Scope of designated services	Agree (no comments)
6.2	Amendments to law	Proposed amendment to Item 50A of Table 1 in section 6 of the Act	Agree (no comments)
6.3	Scope of AML laws	Proposed designated service 2, 3 and 4	Agree (no comments)
6.4	NFTs	Non-Fungible Tokens (NFTs)	Disagree
6.5	Digital assets	Amending the definition of 'digital currency' (call Virtual Assets)	Disagree
6.6	-	Ensuring the integrity of remittance providers and digital asset service providers	Agree (no comments)
6.7	Scope of AML laws	Streamlining value transfer service regulation (including proposed services 5 and 6)	Agree (no comments)
6.8	Scope of AML laws	Proposed definition of 'value transfer chain' (including proposed designated service 7)	Agree (no comments)
6.9	Travel Rule	Updates to the travel rule	Agree (no comments)
6.10	IFTI Rules	Reforms to IFTI reports	Agree (no comments)
6.11	BNI	Cross-border movement of bearer negotiable instruments (BNIs)	Agree (no comments)
6.12		Additional issues	Agree (no comments)
6.13	Deadline to comply	Lacking detail on the commencement date or assisted compliance period	AGD to provide detail

### Key:

Disagree

Agree (with comments)

Agree\* (no comments)

AGD to provide further detail.

## Appendix 2 – Broader reforms to simplify, clarify and modernise the regime ([paper 5](#))

This section provides our response in relation to the “Overview of AML/CTF program reforms”.

### 2. AML/CTF Programs

#### 2.1 An overarching risk assessment obligation – establishing a clearer requirement to conduct a risk assessment

##### 2.1.1 Establishing ML/TF risk assessment as a clearly mandated requirement

We **strongly agree** with the intention to establish a clear, rather than implied, requirement that reporting entities must conduct a risk assessment.

It should also be clear what risks reporting entities are expected to assess, for example, it should explicitly include money laundering, terrorism financing, sanctions, and proliferation financing risk.

We **strongly agree** that proliferation financing should be included as per FATF recommendations.

##### 2.1.2 Establishing the nature, size, and complexity of the organisation in EWRA

We also **strongly agree** that the risk assessment should include information pertaining to the nature, size, and complexity of its business.

This could be made explicit by requiring regulated entities to provide at least the following information:

No	Suggested Minimum Requirements for Nature, Size and Complexity Explanations
1	General information such as legal status, legal name, trading name, country, and date of incorporation
2	Description of the nature of the business including history of the company, the customers it services (and targets), the products and services offered, the channels it distributes them through (including the use of third-party intermediaries such as brokers, agents, or other intermediaries), the geographies, industries, and markets it operates in (and plans to operate in the next 12 months).  Also types of activities that the business prohibits (i.e., engaging with shell companies, offering products in countries determined to be too high risk, offering products to unregulated entities) and how it manages
3	Description on the size of the business in terms of the number of customers, number of branches/offices, number of employees and the size of business by financial metrics, revenue, profit growth etc.
4	Description on the complexity of the business including any recent or planned M&A activity, the relationship of the business to parent organisations (i.e., subsidiary of a foreign branch) and the role between the parent and subsidiaries from an ML/TF perspective.
5	Description of the Board Governance and Oversight framework including the relationship of the AML Compliance Officer to the Board, the level of skills, expertise, and qualifications of the AML Compliance Officer(s), a description of the explicit roles and responsibilities and the frequency and content of management information supplied by them to the Board in relation to ML/TF/PF matters.

The main point is that the laws and guidance should be more explicit about what is expected when regulated entities are requested to document the nature, size, and complexity of their business.

##### 2.1.3 Documenting the ML/TF risk assessment methodology

We also **strongly agree** and that reporting entities should be required to document the ML/TF/PF risk methodology, including the rationale behind decisions such as weighting risk groups, risk categories, risk factors and controls and any rationale for determining the risk ratings that have been applied.

However, simply requesting regulated entities to document their ML/TF/PF risk assessment methodology alone **does not go far enough** and we would suggest that what regulated entities should be required to include when documenting their risk assessment methodology should be explicitly stated to include (at least) the following explanations:

No	ML/TF/PF Risk Methodology Requirements
1	Explanation of the process that the Board and Senior Executive team undertook to determine the organisations risk appetite and risk tolerance as it pertains to ML/TF/PF risks and actions that are to be taken if the ML/TF/PF risk assessment demonstrates that residual risks are outside stated appetite and/or risk tolerance statements.
2	Explanation of the ML/TF/PF methodology the reporting entity has put in place, when and how it was developed, how long it has been in effect for and how frequently it is updated, and whether the ML/TF/PF risk assessment has been subject to external review by suitably qualified experts.
3	Explanation of the ML/TF risk assessment approach to identifying and assessing inherent risks, for example, what risk groups, risk categories, risk factors and risk indicators were considered (and why), whether all risks are weighted equally or whether there is some proportionality and what the rationale is.
4	Explanation of the ML/TF risk assessment approach to conducting control design and operational effectiveness testing, testing methods, size of testing samples, how control effectiveness was determined, and any weighting applied to key controls etc.
5	Explanation of how the ML/TF risks are aggregated across different legal entities, business lines, operating divisions, product lines and countries as appropriate.
6	Explanation the process for documenting enhancement opportunities to continuously improve the approach to ML/TF risk assessment.
7	Explanation of the time-based and event-based triggers that has in the past prompted a review and refresh of the ML/TF risk assessment.
8	Explanation of what process the organisation undertakes to gather qualitative (question-based) and quantitative (data-based) inputs to inform the ML/TF risk assessment process and to strike the right balance between subjective and objective approaches to ML/TF risk assessment.
9	Explanation of how the ML/TF risk assessment methodology aligns to international standards of risk management (i.e., ISO31000 or similar).
10	Explanation of how the ML/TF risk assessment inputs and outcomes are presented and discussed with the Board and Executive committee and how any follow-up actions to continuously improve this process are tracked and monitored.
11	<p>Explanation whether the organisation is adopting RegTech to conduct enterprise-wide ML/TF risk assessments or if not to provide an explanation and justification that excel spreadsheets are fit for purpose (which they are most certainly not for organisations of a certain size or complexity)</p> <p>AUSTRAC would not accept a major financial institution to perform ML/TF Transaction Monitoring using spreadsheets, to monitor clients, accounts, or transactions, yet they in my opinion have taken a very weak stance on this, accepting spreadsheets as a robust approach to EWRAs. As a result of this casual approach taken by the regulator in this regard, the largest six banks in Australia all still conduct EWRAs using spreadsheets. In other jurisdictions, regulators have gone the opposite way, writing to banks notifying them that spreadsheets are no longer acceptable – we have <a href="#">written extensively</a> (since 2018!) on these limitations. We believe that complex organisations (i.e. banks, credit unions, investment managers) that fail to consider adopting technology for this purpose, should be challenged by regulators since the value proposition and benefits are undeniable.</p>

#### 2.1.4 Defining a baseline of risks that must be identified and assessed

We also **strongly support** the AGD's "baseline" for identifying and assessing ML/TF/PF risks as they relate to customer types, types of designate services provided, methods of delivery, and jurisdictions they deal with. AGD states additional factors may be specified in the Rules, if required.

We believe that additional risks are required to be added to the "baseline" as this **far too simplistic** and should contain many other elements that are entirely missing and are essential to properly being able to identify and assess risks, which we have simplified below to allow the AGD (*who are not risk assessment experts by any stretch of the imagination*) to get a far deeper understanding of financial crime risk management approaches so that Australia's ML/TF framework can mature far beyond the overly simplistic "baseline" specified its been using for 17-years.



We've summarised some of the risk groups and risk categories that could and should be considered by regulated entities, many of those such as environmental risk (internal and external), employee risk, outsourcing risk, transaction risk are just a few risk elements for AGD/AUSTRAC to consider and we could add value in this conversation as we've built many risk models, some have up to 450 risk indicators.

In our experience, many organisations struggle translating the “helicopter” view guidance to practical “ground floor”, when designing ML/TF/PF risk frameworks and we would recommend AUSTRAC to develop “industry baseline risk models” outlining the minimum risk groups, risk categories and risk factors/indicators that they expect reporting entities to consider otherwise AUSTRAC will have little chance in effectively reviewing EWRA methodologies of 100,000+ businesses.

### Examples of ML/TF Risk Groups and Risk Categories that should be explicitly covered

<b>Environmental Risks</b> Assess the organisations vulnerability to: <ul style="list-style-type: none"> <li><b>Predicate Offences</b> – deceptive crimes, illicit trafficking, personal crimes, property crimes</li> <li><b>Money Laundering</b> – higher risks associated with – business operations, channels, customer transactions, customers, products and services</li> <li><b>Terrorism Financing</b> – higher customer risk and customer transaction risks</li> <li><b>Financial Sanctions</b> – higher customer risk and customer transaction risks</li> <li><b>Regulatory Compliance Risks</b> – governance and oversight, program alignment to risks, program non-compliance and reporting</li> </ul>	<b>Customer Risks</b> Assess the organisations vulnerability to: <ul style="list-style-type: none"> <li><b>Customer Types</b> – segmentation of customer base - individuals, private companies, public companies, offshore companies, trusts, partnerships including extent UBO's known.</li> <li><b>Customer PEP Status</b> – number of customers that are foreign or domestic PEPs and categories of PEPs</li> <li><b>Customer Location Risk</b> – segmentation of customers by location/geography</li> <li><b>Customer Business Risk</b> – segmentation of customers by industry sector/occupation</li> <li><b>Customer Source of Wealth</b> – segmentation of customers where this information is known, unknown or vague</li> </ul>	<b>Business Risks</b> Assess the organisations vulnerability to: <ul style="list-style-type: none"> <li><b>Business Location</b> – extent of business operations that are carried out overseas (and which countries and which operations)</li> <li><b>Outsourcing Risk</b> – extent to which third parties are used to perform AML controls on your organisations behalf, the nature of outsourced controls, the extent of controls over the outsourced controls!</li> <li><b>Employee Risks</b> – number of employees, proportion that are customer facing, proportion in key risk roles, proportion that have been background screened and extent of background screening, proportion having adverse screening results, functions performed etc.</li> </ul>
<b>Channel Risks</b> Assess the organisations vulnerability to: <ul style="list-style-type: none"> <li><b>Non-Face-to-Face Channels</b> – the extent to which customers are met face to face during on-boarding or when servicing their accounts</li> <li><b>Methods of interacting with customers</b> – what methods are used, somewhat anonymous (e.g., internet, social media, SMS) or less anonymous (e.g., branch, post office, video conferencing, telephone etc.)</li> <li><b>Use of third parties</b> – the extent to which third parties are used as channels (e.g., introducing brokers, sales agents, intermediaries) and the locations of any of these channels</li> </ul>	<b>Product &amp; Services Risks</b> Assess the organisations vulnerability to: <ul style="list-style-type: none"> <li><b>Products and Services</b> – extent to which different products and services are offered (250+ Financial Services Products)</li> <li><b>Attributes of products and services that make them more attractive to money launderers</b> – for example, transfer of funds into and out of accounts through multiple methods, by unrelated third-parties, using remote access methods, from/to foreign jurisdictions, value / transaction limits, allow overpayment or early repayment, acceptance of cash or cash equivalents, cooling off periods etc.</li> <li><b>Extensiveness of use</b> – what proportion of customers use the product or service, what proportion of revenues are attributable, whether any transaction monitoring controls or suspicious matters related to different types of products etc.</li> </ul>	<b>Country Risks</b> Assess the organisations vulnerability to: <ul style="list-style-type: none"> <li><b>Methodology</b> – there is no universal standard for country risk and is geo-political, but there are numerous recognised sources such as Targeted Financial Sanctions (UN), FATF AML Concerns, High Risk and Other Monitored Jurisdictions, Terrorism Vulnerability (US Department), Illicit Drug Vulnerability (US International Narcotics Strategy Control Report), Corruption Vulnerability (Transparency International Corruption Perceptions Index), Financial Secrecy (Index), Kimberly Process (Conflict Diamonds etc.) and FATF Members/Observer Lists (and extent of compliance)</li> <li><b>Frequency</b> – each of these are published at different times of the year and using different rating scales, so agreeing a process and frequency of updates (and reflection through the ML/TF risk assessment can be a challenge!</li> </ul>

#### 2.1.5 Reporting entities to only conduct risk assessments every 4 years

We also **strongly disagree** the AGD's proposal that reporting entities must review ML/TF/PF risk assessments at least every 4-years.

**This is a ridiculous proposal and highlights AGD's complete lack of understanding of AML.**

The Financial Action Task Force (FATF) recommendations are for ML/TF/PF risk assessments to be conducted “at least annually”, so if Australia is to adopt the AGDs position this would continue to make Australia an outlier and likely support any case for grey-listing Australia.

AGD also propose that this applies to “current and new reporting entities”, meaning the reporting entities that have been conducting ML/TF/PF risk assessments “at least annually” as per international standards could decide to revert to a four-year review instead and essentially has the very likely potential for **Australia's AML/CTF regime will go 17-years backwards.**

If the AGD were to closely examine some of the material AML/CTF compliance breaches in Australia the ML/TF risk assessment was in every case found to be lacking (detail/substance, accuracy, applicability, timeliness) and often due to poor risk assessment or infrequent independent reviews (see 8.2), these risks remain unassessed or unmitigated – until it is too late, and the damage is done.

In other regulatory jurisdictions, such as the UK, the Financial Conduct Authority (FCA), which is AUSTRAC's equivalent has frequently issued "Dear CEO" letters (a practice we would recommend AUSTRAC adopt), highlighting the common failings related to Business-Wide Risk Assessments (BWRAs) (another suggestion is for Australia to adopt the BWRA naming as that is more globally common). Below is a summary of the key failings the FCA noted in May 2024.

**Can the AGD even begin to imagine how many failings Australian businesses would have if they were allowed to conduct risk assessments every 4 years rather than refining and improving each year?**

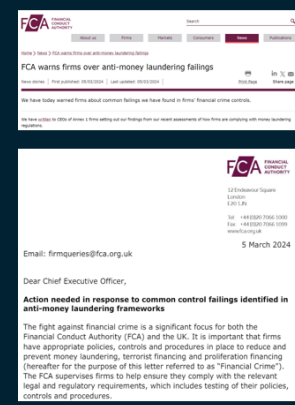
**Regulators have consistently found that the quality and substance of business-wide ML/TF risk assessments are falling far short of their expectations**

*Regulators like the UK's Financial Conduct Authority (FCA) issue warnings in the form of "Dear CEO" letters, notifying businesses of common failings in AML frameworks and actions they need to take*

**Common failings related to business-wide ML/TF Risk Assessments (BWRA):**

- ✓ Completely absent despite the legal requirement to conduct BWRAs
- ✓ Failure to document in writing the steps taken to identify and assess ML/TF and PF risks
- ✓ Failure to understand the ML/TF and PF risks that businesses are exposed to
- ✓ Failure to design and implement appropriate controls to mitigate those risks
- ✓ Poor quality BWRAs lacking sufficient detail and methodology used is often unclear
- ✓ Failure to clearly articulate relevant mitigating measures in place to counteract risk
- ✓ Failure to determine the effectiveness of controls to mitigate ML/TF and PF risks
- ✓ Failure to establish the residual risks that the business remains exposed to
- ✓ Lack of appropriate oversight from senior management
- ✓ Absence of a clear audit trail for financial crime related decision-making.

Source: <https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-action-response-common-control-failings-anti-money-laundering-frameworks.pdf>



## A lot can happen in 4 years...

The pace of change in a 4-year period for most businesses is immense – for example in the external operating environment in the last 4 years we have had a global pandemic (driving up operational risks as people work from home, a seismic shift towards digital payments and a massive rise in frauds and scams), global macro-economic slowdowns (and benefits fraud, tax evasion), massive tax evasion scandals including Australian businesses and individuals, a decline in international instability with Russia's war on Ukraine, Israel/Palestine conflict and other international posturing.

Further in relation to the internal operating environment, organisations would also go through material changes including (but not limited to) mergers and acquisitions (already highly present in the credit union / mutual banking sector in Australia), launching new products and services, acquiring new customer types, launching into new industry segments or countries, or deploying and sunsetting new technology systems etc. so the pace of change is much faster than every 4 years.

The risk is that ML/TF/PF risks will be very out of date and completely ineffective if only being conducted every 4 years. How can AUSTRAC expect to enforce Board oversight function if Boards are only reviewing their risks and mitigating plans every 4-years, that are either out of date or should have been actioned years prior?

## 2.1.6 Reporting entities to keep the risk assessment up to date based on triggers

We also **strongly support** the requirement that reporting entities must keep their risk assessment up to date based on “triggers” that could include “changes to a businesses’ risk profile or the adoption of new technologies to manage certain AML/CTF obligations.

We recommend that the AGD/AUSTRAC go much further into clearly defining the types of “triggers” that should prompt a review of the ML/TF risk assessment as if the triggers are “wishy-washy” (as described above) and the proposal is for a refresh on a time-bound basis (every 4 years – crazy talk!) then the trigger-bound expectations need to be **much stronger and clearly defined**.

We have prepared the following table outlining the level of guidance that should be explicitly advised to regulated entities regarding the expectations to conduct a trigger-based refresh:

External Events		Internal Events
Regulatory Events	Other Events	
Enforcement activity targeted at certain sectors or activities - is the same activity present?	Changes in the geo-political landscape making a country at higher risk than before.	External (or internal) independent review highlighting deficiencies in the ML/TF risk assessment.
Changes in AML/CTF regulations or rules - how do they impact your organisation?	Changes in various published country risk rankings (i.e., transparency international).	Review of ML/TF risk assessment prior to annual compliance reports being filed with the regulator.
Changes in guidance and risk typologies - has your ML/TF risk assessment considered this?	Increased media scrutiny on certain companies, industries, or activities.	Organisation is launching or has launched new products services, which pose new ML/TF risks.
Consultation papers about proposed regulatory changes - what would be the impact on your business if these laws are enacted?	Changes in the threat landscape as criminals find more innovative ways to launder criminal proceeds.	Organisation is targeting new customer segments, expanding into new geographic markets, or generally changing its business.
International guidance issued by the FATF, the Wolfsberg Group, the Egmont Group highlighting trends and risk-related guidance.	Emerging technologies that could pose new threats to your organisation, such as criminal use of Artificial Intelligence.	Merger and acquisitions activity (i.e., divestments, acquisitions) bringing together businesses with different risks and approaches.
Publishing of National Risk Assessments highlighting threats at national, industry, product, or activity level.	Collaboration through public and private partnerships could present opportunities to update ML/TF risks and controls.	Change in Board and/or Senior Management, with a greater focus on risk appetite and management.
Release of federal, state, or local crime statistics that are relevant to your industry and operations.	Investigations by journalists or law enforcement into organised criminal activity that is related to your organisation's operations.	Appointment of a new AML/CTF Compliance Officer/MLRO looking to make changes to the ML/TF risk assessment and AML Program.
Criminal or civil prosecutions or other enforcement action (i.e., enforceable undertaking, regulator appointed independent auditors).	Class actions being filed against organisations for failing to manage or disclose risks.	Appointment of risk, compliance, or legal advisors with experience in conducting and updating ML/TF risk assessments.

**We strongly recommend that the AGD reconsiders its proposal for risk assessments to be conducted every 4 years, to Annually and for other trigger-based events to be more explicitly define.**



### 2.1.7 Board to approve the risk assessment and be informed of updates

We **strongly agree** that Boards (or equivalent Senior Management, who have direct reporting lines into the Board) are required to formally approve and adopt the risk assessment, as well as being informed of updates.

As a Board Director, being presented with an ML/TF risk assessment every 4-years, should be considered by them as **woefully infrequent** and the exposure that they could potentially face if they are not identifying, assessing, mitigating, and managing risks in an appropriate and proportionate manner **that is far timelier (i.e., Annually)** could expose them and their organisations fundamentally.

We also believe that AUSTRAC should take action against individual Directors that are falling short of the expectations as Directors in this regard as in every corporate AML/CTF failure no action has been taken against Board Directors and until there is evidence of personal accountability or personal liability, then many Board's will continue to pay lip service to AML/CTF compliance but not put their (shareholder's) money where their mouth is.

## 2.2 Proportionate risk mitigation measures

We **strongly agree** that reporting entities must implement proportionate risk mitigation measures and develop, implement, and maintain enterprise-wide policies, systems and controls proportionate to the nature, size, and complexity of the business.

Whilst it is reasonable not to specify the detailed risk mitigation measures of each organisation, we believe that an expectation should be set for reporting entities to clearly demonstrate:

No	Mitigating Control Measures
1	Explanation of the process that has been undertaken to assess both the design and operational effectiveness of controls, including but not limited to, the methodology used, the control test questions that have been considered (as well as their responses) and the evidence that has been gathered to demonstrate an appropriate assessment on the effectiveness of the control environment.
2	A written report that outlines the inherent risks, the control effectiveness ratings (including rationale, control testing results) and the impact on the residual risk rating.

Whilst the AGD has noted from the first round of submissions that some regulated entities have certain risk mitigation measures in place, it is unlikely that many of those businesses, particularly in the proposed sectors to be regulated would have an understanding or appreciation of the full range of mitigating controls required to effectively manage its ML/TF risk, let alone have designed or implemented these controls across their business, so further guidance on control measures is important as we often encounter large businesses with either none, limited or immature understanding of the controls they should implement, so suggest Rules are required to be made more explicit.

## 2.3 Reporting entities maintain internal controls

We **strongly agree** with the proposal to include an express obligation to establish an internal control framework to manage AML/CTF obligations, support mitigating control frameworks and build compliance cultures.

We also **strongly agree** that the Board should be responsible for being "reasonably satisfied" with the organisations ML/TF risk management framework. However, the AGD use of the term "reasonably satisfied" applies a weak threshold and should be upgraded to "confident that the ML/TF risk management framework is appropriate and proportionate to the identified risks", as "reasonably satisfied" is very unlikely to build a compliance culture of accountability. For example, hypothetically speaking, the Board of a Sydney-based casino group could argue it was "reasonably satisfied" with its ML/TF risk management controls where major ML/TF failings could be just beneath the surface.

We also strongly agree with the other contents of this section.

## **2.4 Establishing a new “business group” concept and ensuring group-wide risk management**

We agree with the AGD’s proposal about replacing the DBG concept with a Simplified Business Group concept.

## **2.5 Simplified obligations for foreign branches and subsidiaries**

We agree with the AGD’s proposed changes to align more closely to FATF recommendations. Some of the issues we’ve identified with foreign branches and subsidiaries are either (a) that their approach to AML/CTF Programs is centrally mandated (and may not meet Australia’s requirements – a small risk with EWRA’s as Australia’s expectations are at a lower bar than many other jurisdictions – and about to get lower unless the 4-year period is significantly shortened to 12-months!) or (b) they simply do not understand Australia’s AML laws that they are subject to, so anything that can be done to solve these problems is welcomed.

## **3. Customer Due Diligence**

### **3.1 Applying a customer risk rating to each customer**

We **strongly agree** that Customer Risk Assessment (CRA) (*could this language be used in Australia to align us with the international community?*), should be assessed before a designated service is provided and be updated as part of both Initial CDD and Ongoing CDD.

We feel that reporting entities need to be provided with clear guidance on what typically constitutes a higher risk customer type (for example, location of customer, industry / occupation of customer, PEP status, nationality of customer, customer legal entity type, age of relationship to the reporting entity and many other factors), so that a similar standard can be applied across reporting entities in a similar manner.

Further we would recommend that reporting entities that have failed to assign a customer risk rating to any active customers (or any dormant customers that become active), should within six to twelve months of the laws being passed be required to retrospectively risk assess each customer until a customer risk rating exists **for every single customer**.

### **3.2 Refining requirements for ongoing CDD**

We agree with this section and only have one comment in relation to the definition of “unusual transactions or behaviour”, which we believe the definitions could be further expanded to include:

- The historical behaviour of the customer, relative to their current behaviour
- The behaviour of the customer relative to peer groups (i.e., peer group profiling for outliers).

Unless the AGD is crystal clear in their expectations, keeping it vague (i.e., what the reporting entity knows about the customer), it does not explicitly define the types of considerations to assess.

Further, in relation to the risk-based transactions to be monitored and the push-back that this leads to monitoring for “all crimes”, the AGD could be more specific on what it means by “serious money laundering predicate crimes” to include things specifically like fraud, cybercrime, ransomware, human trafficking, wildlife trafficking, environmental crimes (i.e. logging/de-forestation), tax evasion and sanctions evasion for example as leaving it just at serious ML predicate crimes could leave this open to interpretation (and materially scaling back transaction monitoring typologies that relate to these predicate crime types).

### **3.3 Confirming when enhanced CDD must apply**

Agree, no comments.

### **3.4 Streamlining the application of simplified CDD**

This makes sense, suffice to say that it materially increases the importance of conducting the Customer Risk assessment (CRA) and ensuring that this process is effective. A control AUSTRAC could apply would be to request that reporting entities quantify in the Annual Compliance Report the number of low risk rated customers (as a proportion of all customers) and those that have been subject to simplified CDD. Having an independent review requirement every two-years (see 8.2) could be a way of checking that reporting entities are not circumventing proper CRA's to apply simplified CDD in cases where they should not.

### **3.5 Additional Measures**

Record keeping for CDD comments make sense, particularly the audit trail requirement for Customer Risk Assessment (CRA) inputs and outcomes.

Pre-commencement customers prior to 2007 (>17-years ago) should absolutely be subject to the same standards of CDD as new customers today and is an oversight that has remained in place for far too long and a positive outcome to see this now being addressed. Providing reporting entities with a risk-based approach to this may not make sense as actioning could be put off further.

There are now many advanced technology solutions where reporting entities could easily and affordably "batch" up customer data and "wash" it through a KYC engine to complete KYC checks and CRA checks simultaneously and therefore does not have to be a manual process and six to twelve months would be reasonable.

Perhaps the AGD could consider an implementation timeframe by the size of the reporting entities customer base: (a) Less than 2,500 active customers (six months) (b) Between 2,500 and 100,000 (twelve months) and (c) 100,000 customers (twelve to eighteen months) (by dispensation request).

### **3.6 Defining a 'business relationship' and 'occasional transaction'**

This makes sense to define these terms in the Act and Rules to provide clarity on what reporting entities are expected to do.

## **4. Exception for assisting in an investigation of a serious offence**

### **4.1 Keep open notification process**

Agree, no comments.

## **5. CDD exemption for gambling service providers**

### **5.1 Lowering the threshold from \$10,000 to \$5,000**

Bringing Australia into line with FATF recommendations makes and \$5,000 is still a lot of money to be gambling with, without seeking any identification of who the person engaged in the gambling is!

## **6. Tipping Off Offence**

### **6.1 Changes to the tipping off offence to relate to disclosing SMR information**

Agree, no comments.

## **7. Moving some exemption from the Rules to the Act**

### **7.1 Revising the approach to exemptions to make those already granted to be enduring**

Agree, no comments.

## 8. Repealing the *Financial Transaction Reports Act 1988*

Agree, no comments.

### Consultation Questions

No	AGD's questions	Arctic Response
a	Under the outlined proposal, a business group head would ensure that the AML/CTF program applies to all branches and subsidiaries. Responsibility for some obligations (such as certain CDD requirements) could also be delegated to an entity within the group where appropriate. For example, a franchisor could take responsibility for overseeing the implementation of transaction monitoring in line with a group-wide risk assessment. Would this proposal assist in alleviating some of the initial costs for smaller entities?	<p>We believe this will reduce costs allowing for technology and / or advisory companies to work with franchisor operators at the Head Office level to provide services and support, as well as, underlying technology to provide AML/CTF Program related services like ML/TF risk assessments across an entire network of businesses in a "simplified business group".</p> <p>This flexibility would assist smaller entities reduce compliance costs through a centralised "hub and spoke" model of compliance.</p>
b	The streamlined AML/CTF program requirement outlined in this paper provides that the board or equivalent senior management of a reporting entity should ensure the entity's AML/CTF program is effectively identifying and mitigating risk. To what extent would this streamlined approach to oversight allow for a more flexible approach to changes in circumstance?	<p>We agree that this will make it easier for delegation to AML/CTF Compliance Officers on operational matters but also poses a potential risk that Board Directors will become even less interested/connected with the AML/CTF Program since more functions will be delegated and if reporting entities only need to engage them at a minimum every 4 years on risk assessment, many Boards will remain even more clueless on AML/CTF matters than many of them already are!</p> <p>Some progressive regulators (in Middle East and parts of Africa) are talking about moving to EWRA's every 4 months and Australia is talking about moving to every 4 years – makes absolutely zero sense.</p> <p><b>What was AGD's logic behind proposing 4 years?</b></p>
c	Many modern business groups use structures that differ from the traditional parent subsidiary company arrangement. What forms and structures of groups should be captured by the group-wide AML/CTF program framework?	<p>Networked arrangements:</p> <ul style="list-style-type: none"> <li>• Money Remittance Network Provider and Affiliates</li> <li>• Franchisor (HQ) and Franchise(s) (i.e. real estate)</li> <li>• Partnerships – Main HQ and regional partners etc (i.e. law firms and accountancy practices)</li> <li>• Pooled Resource Centres – for example Mutual Marketplace handles procurement for many Credit Unions as a centralised function; Cuscal provide transaction monitoring for many Credit Unions and others and could be extent to providing AML/CTF Program related services (i.e., supporting EWRA's, facilitating independent reviews, supporting annual compliance reporting as well as existing arrangements)</li> </ul> <p>Could this extend to Venture Capital / Private Equity investors many of whom have invested in "portfolio companies" that are in unrelated but regulated businesses where VCs sit on the Boards of regulated entities often unaware of the responsibilities of Board directors in relation to AML/CTF matters and they could insist on consistent financial crime risk management for all portfolio companies?</p>
d	To what extent do the proposed core obligations clarify the AML/CTF CDD framework?	It is clear and the diagram is a helpful reference guide.
e	What circumstances should support consideration of simplified due diligence measures?	<p>Only where the reporting entity has sound reasoning backed up by a comprehensive Customer Risk Assessment (CRA) to support low risk and simplified CDD.</p> <p>Examples of when Simplified CDD is considered appropriate would also be helpful.</p>
f	What guidance should AUSTRAC produce to assist reporting entities to meet the expectations of an outcomes-focused approach to CDD?	<p>Define the collection and verification standards for each of the approaches to CDD with examples. Only where the reporting entity has sound reasoning backed up by a comprehensive Customer Risk Assessment (CRA) to support low risk and simplified CDD. Examples of when Simplified CDD is considered appropriate would also be helpful.</p>

No	AGD's questions	Arctic Response
g	When do you think should be considered the conclusion of a 'business relationship'?	<ul style="list-style-type: none"> <li>• When all accounts are closed</li> <li>• When an occasional transaction for a non-customer is completed</li> <li>• When a customer has been off-boarded/exited following a decision that the customer is an unacceptable risk</li> </ul>
h	What timeframe would be suitable for reporting entities to give a risk rating to all pre-commencement customers?	Within six to twelve months of the laws being passed, smaller reporting entities with fewer customers closer to six months and larger reporting entities with more customers twelve months and by exception and on application very large entities up to 18 months.
i	Are there situations where SMR or section 49 related information may need to be disclosed for legitimate purposes but would still be prevented by the proposed framing of the offence?	Not that I can think of, however, is it possible for Australia to normalise the language to be more in line with international standards and call SMR Suspicious Activity Reports?
j	Are there any unintended consequences that could arise due to the proposed changes to the tipping off offence?	Not that I can think of.



## 9. Additional Considerations that the Attorney General's Department should consider

Both of the following points were made in our first submission, but they have both been ignored or overlooked and we would like to understand the reasons that the Attorney General's Department has chosen not to consider both points, since they are logical and based on obvious gaps in Australia's AML/CTF regime relative to other FATF-member countries.

At a minimum, we feel that the Attorney General's Department should be clear on proposals made during both rounds of submissions that it has decided not to introduce including the rationale behind this decision. **Please can you provide this information in future?**

### 9.1 Include other high-value goods dealers in the AML/CTF regime

One notable omission from the Attorney General's Consultation Paper into Tranche 2 reforms is the exclusion of high-value goods dealers, which was included in my previous submission, but the AGD has decided to continue to omit this sector from the AML/CTF reforms in Australia which in my opinion is a significant oversight for some unknown reason as to why this is not being considered.

This is surprising, particularly since the Attorney General Department's predecessor, the Home Affairs Department who in November 2016, issued its own consultation paper on a model for regulating high value dealers under the AML/CTF Act.

**Can the Attorney General's Department please explain why High Value Dealers have been omitted from both rounds of consultation papers?**

In this consultation paper, the Home Affairs Department stated:

"In Australia, items considered to pose ML/TF risks when purchased using large sums of cash include jewellery, antiques and collectibles, fine art, boats, yachts, and luxury motor vehicles. Building, bathroom, and kitchen supplies are also considered to be high-value goods that pose significant ML/TF risks because criminals often purchase real estate using illicit funds and renovate the property using crime-derived cash. HVDs that conduct a business in Australia involving the buying and selling of these items, and accept large sums of cash for these items, are being considered for AML/CTF regulation".

It is worth noting that the report goes on to outline the ML/TF vulnerabilities of high-value dealers:

*"Recent high profile asset confiscation cases in Australia demonstrate the breadth of criminal investment in HVDs and the scale of criminal wealth that can be laundered and invested in those goods. In 2014-15, the Australian Federal Police's (AFP) Criminal Assets Confiscation Taskforce restrained over AUD\$246 million worth of illicit assets that included a range of high-value goods. Real estate, motor vehicles and jewellery are the most commonly targeted high-value goods for money laundering, but other types of luxury goods or 'lifestyle assets', can also be used. The most significant ML/TF risks arise where these high-value goods are purchased using large sums of cash. Luxury cars can be purchased by criminals using illicit cash or a combination of credit and illicit cash. Where credit is obtained for the purchase, the loan is often repaid early using illicit cash. The cars are then resold. Any losses made by the criminal on the loan or as a result of a decrease in the cars' resale value are borne as the cost of laundering.*

*Precious stones and precious metals are particularly vulnerable to being used for ML/TF purposes. The purchase of jewellery can disguise the real amount of money laundered because a 'normal' market price can be hard to establish. This means the value of the jewellery can be misrepresented by either under or overvaluation to disguise the amount of criminal income laundered through its purchase. Transaction methods for jewellery can range from anonymous exchanges of stones or nuggets to government-regulated deals and international transactions conducted through the financial system. These goods can be readily purchased and transported, and later sold for cash, with their value increasing over time. Jewellery also carries an added ML/TF risk because individual items may be small, very high in value, and easily transportable, offering criminals the opportunity to transfer value within or between countries in a manner which minimises the chance of detection."*

The report then went on to explain the benefits of regulating high-value dealers under the AML/CTF regime:

*"The regulation of HVDs under the AML/CTF regime would deliver a number of benefits, including closing a regulatory and intelligence gap, enhancing national security, and enhancing the reputation of the Australian financial system. While transactions performed by HVDs that use electronic payment systems can be tracked by law enforcement, transactions that involve large sums of cash are virtually invisible. No information is collected and verified about the identity of the customer and the source of the customer's funds, and no information is reported to AUSTRAC that can be used by law enforcement agencies to follow the money trail for illicit funds.*

*This makes the use of HVDs attractive to criminals seeking to launder illicit funds through buying and selling high-value goods. If HVDs had obligations to collect, verify and report information, they could play a significant role in the detection and investigation of ML/TF offences.*

*This would allow for suspicious transactions to be reported to authorities earlier in the transaction chain than occurs currently, thereby activating the protections of the Act and providing earlier opportunities for law enforcement to detect and disrupt criminal activities and deprive criminals of the proceeds of crime. The AML/CTF regulation of HVDs would also enhance the sector's awareness of ML/TF risks and assist HVDs to identify 'red flags' that may be early indicators of criminality or potential misconduct. Red flags can relate to the customer, the nature of the transaction and/or the source of the customer's funds. Where there are a number of indicators, it is more likely that a HVD should have a suspicion that ML or TF is occurring."*

I have again illustrated this point at length as there are clearly concerns expressed by the Home Affairs Department into the ML/TF risks and vulnerabilities in the high-value goods sectors but for some unexplained reason the Attorney General's Department have entirely overlooked high-value goods dealers in the consultation process and appears that they must have formed a view that these risks have evaporated since 2016 or that high-value dealers are not worth regulating in Australia, which creates a weak link for organised criminals to exploit.

We would strongly recommend **again** that the Attorney General's Department reconsiders its position in respect of high-value goods dealers and includes them in the expanded AML/CTF laws as there has clearly been concern expressed by the Australian Government in the past and if the Australian Government is genuine in its claim that it is "committed to protecting the integrity of the Australian financial system and improving Australia's AML/CTF regime to ensure it is fit-for-purpose, responds to the evolving threat environment, and meets international standards set by the Financial Action Task Force (FATF)" as stated in the opening paragraph of this consultation paper, then it will act to regulate high-value goods dealers too.

In the previous submission, I summarised the ML/TF risks and vulnerabilities of the following high-value dealer sectors which we urge the Attorney General's Department to regulate:

- Antique and Art Dealers
- Auctioneers and Brokers
- Motorised Vehicle Dealers
- Luxury Goods Dealers

## **9.2 Explicit guidance that AML/CTF Programs must be subject to independent review at least every two years (or annually for higher risk businesses)**

In my opinion, another major deficiency in Australia's AML/CTF laws is the fact that there is no mandatory minimum requirement for when reporting entities must have their AML/CTF Programs subject to an independent review to assess the design and operational effectiveness of the AML/CTF Program and whether the regulated entity is in compliance with the AML/CTF legislation, rules, and guidance. Also, we do not agree with the approach to independent reviews advocated by AUSTRAC on their website under the section entitled "how often independent reviews must be done"; it is left entirely to the discretion of the reporting entity to decide when these should be conducted.

The AUSTRAC website states *“you must decide on how often reviews are done. How you decide depends on the size of your business, what kind of business you have, how complex your business is and your level of ML/TF risk”*. **This simply does not go far enough.**

We have met many businesses that have never had an independent review of their AML/CTF Program since the laws were enacted in 2006 (17 years ago), so this risk-based approach to independent reviews is not driving the right behaviours or outcomes needed for the 17,000 businesses regulated by AUSTRAC.

Often when there are material AML/CTF compliance failures these frequently relate to issues that have remained undetected or unaddressed for years (or even decades) because of independent reviews either not having been completed in a timely manner (if at all) or by independent reviewers not being sufficiently skilled or thorough in their reviews, particularly in the areas of control effectiveness testing.

We often hear about unqualified persons conducting superficial independent reviews, giving regulated businesses a false sense of comfort, and often failing to perform control testing at all, which in our opinion does not even constitute an independent review. Several years back, AUSTRAC established an Approved Persons list for practitioners that had demonstrated their skills, qualifications and/or experience in AML/CTF, much like the Skilled Person panels that exist in the UK and administered by the Financial Conduct Authority. In Australia, this process and concept was dropped, and it was not clear why, but seems like a sensible thing to consider reinstating as part of this review.

Our specific recommendations in respect of this can be summarised as follows:

- Include specifically in the laws that all businesses must have their AML/CTF Programs independently reviewed at least every two-years.
- Include high-risk industry sectors (i.e., casinos, crypto, money remitters and cash intensive sectors) where and independent review of the AML/CTF Programs is more appropriate on an annual basis.
- AUSTRAC advocates on their website and through their outreach programmes that independent reviews are an important mechanism to achieve compliance and they have a minimum expectation, which is not stated like this with the “you decide when” approach. Update their website to reflect a more prescriptive approach.
- Implement a timeframe of within 6-months for high-risk industry sectors (and those that have not had an independent review within the previous 3-years) and 12-18-months for all other businesses to have initiated and completed an independent review of their AML/CTF Programs
- A request that on completion of the Independent Review that these are provided to AUSTRAC and uploaded into a portal so that AUSTRAC can track who has and who has not completed the independent review within the specified timeframes and impose potential penalties, such as AUSTRAC appointing an independent reviewer on the reporting entities behalf if they have failed to initiate one themselves.
- AUSTRAC to reinstate the Approved Persons process but the definition last time was too restrictive as it approved legal practitioners (who could have zero AML/CTF knowledge or experience, as is currently the case with some lawyers conducting independent reviews) but did not as broadly as it could have included experience of AML/CTF practitioners who are working in the field but may not be qualified as a lawyer etc.
- AUSTRAC to spot check the independent reviews for completeness to examine the quality of the independent review and the approved person in conducting the review.
- AUSTRAC in the annual compliance report to explicitly ask, when the last independent review was completed, who by, for what periods, request that the report and any remedial actions are uploaded to AUSTRAC online and ask questions about whether any of the “trigger events” have occurred within the last 12-months. Where the trigger events have occurred, but no independent review has been conducted, AUSTRAC should write to regulated entities with a “please explain” letter.

## Appendix 3 – Comments on [Paper 1 – Real Estate Professionals](#)

### 3. General Comments

#### 3.1 AGD's proposal not to regulate residential tenancies, property management and leasing of commercial real estate

Recognising that these currently are outside of the scope of FATF recommendations does not mean that money launderers cannot use these activities to launder criminal proceeds and have included a couple of examples to illustrate this:

Real Estate Activity	Money Laundering Typologies and Description
Residential Tenancies	<p><b>Purchase of Properties:</b> Criminals can purchase residential properties using illicit funds, often under the guise of rental investments. These properties are then rented out, allowing money launderers to blend illegal funds with legitimate rental income.</p> <p><b>Over or Understating Rental Payments:</b> Money launderers might overstate rental payments to legitimize larger amounts of dirty money or understate them to evade taxes and scrutiny, mixing these payments with legal sources of income.</p>
Property Management	<p><b>Layering Through Multiple Transactions:</b> Property management companies might be used to layer illicit funds through multiple transactions and ownership transfers, disguising the origin of the funds.</p> <p><b>Maintenance and Renovation Overbilling:</b> Overbilling for property maintenance or renovations is a common technique where the additional charged amounts are used to inject illicit funds into the legitimate financial system.</p>
Leasing of Commercial Real Estate	<p><b>Complex Corporate Structures:</b> Using complex corporate structures like trusts, shell companies, and offshore entities can obscure ownership and the source of funds in large commercial real estate deals.</p> <p><b>High-Value Lease Agreements:</b> High-value or above-market lease agreements can be used to justify the transfer of large sums of money, which may be disproportionate to the actual value of the property or the rental market.</p>

#### 3.2 Lacking detail on the commencement date or assisted compliance period

The AGD has noted that real estate professionals would be given an extended period to allow them to meet their obligations but further clarity to the industry is required in the following areas:

- What is the window of time that the AGD expects to have finished drafting revised legislation and have enacted?
- What is the AGD's current position on the approach to the roll out of AML/CTF laws to new sectors?
  - Will the implementation be staggered, or will the assisted compliance period differ by impacted sector?
  - If staggered, which industry would be required to implement first and what is the proposed running order?
  - How long does the AGD expect is reasonable for each industry sectors assisted compliance period to be?

A couple of points to note here:

- Australia remains a laggard on the international stage and the AGD/Australian Government's lack of action over the last 17-years will mean additional pressure on industries to be compliant by the time of FATF's follow-up MER
- Countries like New Zealand implemented a staggered approach (six-months apart) with a 12-month assisted compliance period – however, New Zealand introduced their laws in 2009 and Australia does not appear to have the luxury of time for a staggered approach
- In order to plan accordingly, the sooner the AGD can be transparent on their thinking in this regard will mean there will be fewer surprises (like the crazy suggestion of 4-year EWRA cycles!)

### 3.3 Develop and maintain an AML/CTF program based on a risk-based approach

It is not explicitly stated that regulated real estate participants must conduct an ML/TF risk assessment of the frequency.

It does not explicitly state following the implementation of the AML/CTF Program what the AGD's expectations are in relation to the frequency of independent reviews (see 8.2) in relation to the real-estate sector.

### 3.4 Detailed AML/CTF program requirements

The paper outlines some of but not all of the AML/CTF Program requirements that might typically be expected to be managed. It then goes on to talk about "business groups" and the centralisation of the AML/CTF Program requirements but is entirely missing what the obligations are for "business group" owners or any independent real estate businesses providing the listed designated services that are not part of a "business group".

The AGD should explicitly define what the expectations are in the AML/CTF Program requirements for real-estate (and other tranche 2 sectors) following the expansion of the "designated services" to these sectors (i.e., ML/TF risk assessment, KYC (CRA, PEP name Screening, CDD, ECDD, OCDD refreshes), Employee Due Diligence, AML Risk Awareness Training, Transaction Monitoring, Regulatory Reporting, Record Keeping, Governance and Oversight etc. **It should be made explicit.**

We have included a diagram, which we use to depict the full extent of the obligations of an AML/CTF Program (fig. 1).

### 3.5 Regulatory relief for pre-commencement customers

**We do not agree with the proposal.**

Whilst it seems reasonable to offer newly regulated businesses regulatory relief for pre-commencement customers to essentially grandfather these provisions, this is just "kicking the can down the road" (as we are seeing in the reforms for Tranche 1 customers). It is also likely to make this harder to manage from the outset. One of the reasons this dispensation was granted (and made sense in 2006) was because there was a lack of viable technology to collect and verify customer information electronically. However, 18 years later major technology developments allow millions of customer records to be "washed" against databases with exceptions being reported and we do not believe that the same regulatory relief is warranted and makes more sense to "bite the bullet" and apply the same CDD standards to existing pre-commencement customers as new customers.

We recognise the need to give newly regulated entities the time to do this (6 to 12 months would be more than reasonable rather than de-scoping entirely).

If this is unacceptable (shouldn't be), then a fall-back position should be to define the triggers that would require a reporting entity to conduct CDD on existing customers as the definition of (a) unless and SMR obligation arises or (b) there is a change in risk profile, **is far too limited**. The AGD should develop other scenarios where CDD is required for existing customers, for example:

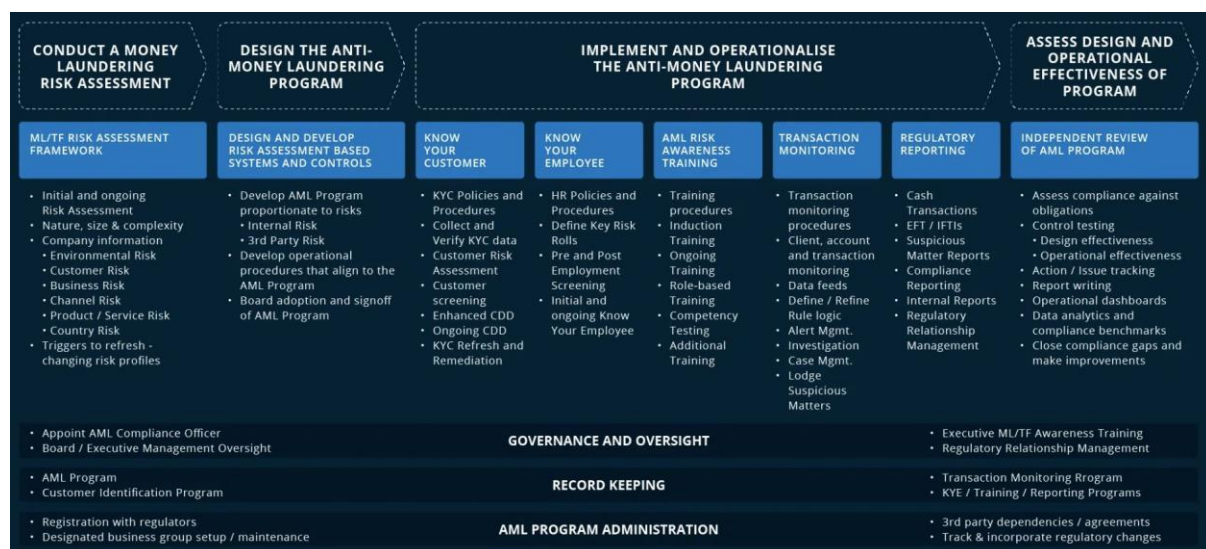
- Opening a new account / applying for a new product or service
- Changing the address of the account
- Changing the contact details on the account
- Appointing new directors or beneficial owners to the account
- Transaction monitoring alerts have occurred (even if does not change risk profile or warrant an SMR)



### 3.6 Consultation Questions

No	AGD's questions	Arctic Response
a	Does the proposed definition of real property and its intersection with the proposed designated services create any unintended outcomes with regard to real estate transactions?	Not in my view. However, we do disagree with the AGD's decision under pressure from the real estate sector to exclude residential tenancies, property management and commercial real-estate leasing as there are money laundering typologies associated with each.
b	To what extent do you think you would be able to leverage existing systems and controls to meet the proposed obligations?	<p>Whilst many Tranche 2 reporting entities in the first round of consultation expressed that they could leverage existing systems and controls to address the proposed obligations, given the lack of experience it could be a case that they "don't know what they don't know".</p> <p>This is not a criticism of those sectors and was like Tranche 1 back in 2006, which felt like <i>"in the land of the blind, the one-eyed man was king"</i>, very few people (including me) had any inkling of what was involved in implementing an effective AML/CTF Program. Fortunately, there are lots of practitioners now with lots of experience and technology around to make life easier that didn't exist back then.</p>
c	In what circumstances do you consider reliance among real estate professionals and other reporting entities for initial customer due diligence will be appropriate?	Where the reporting entity that is collecting customer due diligence can demonstrate that they have effective CDD controls in place to the party that is relying upon them. Also, makes sense to have an information sharing arrangement in place, a service level agreement and a "right to audit" in that agreement.
d	What additional information, guidance and materials would you require from AUSTRAC to help you comply with your new AML/CTF obligations?	Explicit guidance on ALL of the aspects of the AML/CTF Program for real estate companies that are and are not part of a business group. It is not entirely clear on things like employment screening, training, independent reviews, governance and oversight and other items from the paper.
e	What timeframe would you require to complete a risk rating for all pre-commencement customers (customers who you are in a business relationship with when the reforms commence)?	If the reporting entity is simply applying a flag to all existing pre-commencement customer accounts in the CRM that the Customer Risk Rating = Unassessed, this should be able to be done easily within six months.

**Fig 1 – A typical end-to-end AML/CTF Compliance Value Chain**



## Appendix 4 – Comments on Paper 2 – Professional Service Providers

### 4. General Comments

#### 4.1 Language is important

The use of terminology is important and whilst the rest of the world has one language Australia seems hellbent on creating its own lexicon of language that is different to the rest of the world when frankly it would be much, much simpler to adopt the international language of AML.

For example:

- Professional Service Providers (PSPs) when everyone else calls it Designated Non-Financial Services Businesses and Professions (DNFBPs)
- Enterprise-Wide Risk Assessments (EWRA) when everyone else calls it Business-Wide Risk Assessments (BWRA)
- Suspicious Matter Reports (SMRs) when everyone else calls it Suspicious Activity Reports (SARs)

There are probably many other terms that could be normalised to international standards.

#### 4.2 The scope of Professional Service Providers (DNFBPs!)

We agree with the scope of the professions to be including legal practitioners, accountants, consultants, trust and company service providers, financial advisors, and business brokers.

#### 4.3 The scope of “designated services” provided by professional services providers (DNFBPS)

We agree with most of the exclusions described and that the scope of ‘designated services’ should commence mostly in relation to transaction related activity.

However, advice requested of a lawyer or accountant or financial advisor etc. to circumvent AML/CTF laws, for example by seeking advice on how to setup a complex web of companies and trusts or to establish a business in an offshore tax haven should also be caught, even if no transaction has occurred to execute on the advice.

##### 4.3.1 Inclusion of residential tenancies, property management and commercial leasing

As noted in the real-estate section, there are money laundering risks associated with residential tenancies, property management and leasing of commercial real estate.

##### 4.3.2 Inclusion of deceased estates

We do not agree with the conclusion of exempting property received from deceased estates as soon as carved out this will be a legal loophole that could be exploited by money launderers. The table below summarise some of the typologies related to deceased estates that the AGD might want to consider if it has not already:

Typologies	Description
Ownership Concealment	Money launderers might attempt to conceal the true ownership of assets by transferring them to deceased individuals' estates. This could involve creating false documentation or using the identities of deceased persons to obscure the origin of illicit funds.
Complex Legal Processes	Dealing with deceased estates involves various legal processes, such as probate and asset distribution which can be lengthy and complex, providing opportunities for money launderers to exploit gaps or weaknesses in oversight.
Use of Shell Companies	Money launderers may establish shell companies or trusts within deceased estates to layer transactions and obscure the original source of funds. These entities can facilitate the movement of illicit funds through multiple jurisdictions, making funds difficult to trace.
Inadequate Due Diligence	Executors, trustees, and other parties involved in managing deceased estates may not conduct thorough due diligence on beneficiaries or transactions, leaving the estate vulnerable to exploitation by money launderers.

Typologies	Description
Real Estate Transactions	Deceased estates often include valuable assets such as real estate. Money launderers may exploit real estate transactions within these estates to introduce illicit funds or purchasing properties with illicit funds.
International Transactions	If the deceased had assets or beneficiaries located in different countries, it can add complexity to the estate administration process. International transactions and cross-border transfers provide additional opportunities for money laundering activities.

#### 4.3.3 Inclusion of escrow services

The AGD has sought views as to whether ‘escrow services’ (as opposed to those provided by financial institutions) should be excluded from the scope and wanted to note that there are money laundering risks associated with these services that facilitate secure transactions by holding funds or assets until certain conditions are met and can be vulnerable due to the potential for anonymity, the movement of large sums of money and the complexity of transactions.

The table below summarise some of the typologies related to escrow services that the AGD might want to consider if it has not already:

Typologies	Description
Layering	Money launderers may use multiple escrow transactions to layer funds, making it difficult to trace the original source of illicit funds. They may transfer funds between different escrow accounts or conduct a series of transactions to obscure the money's origin.
Third Party Payments	Escrow services often involve third-party payments, where funds are transferred from one party to another through the escrow account. Money launderers can exploit this process by using the escrow account to transfer illicit funds between multiple parties, making it appear as though the funds are legitimate.
Anonymous Transactions	In some cases, escrow services allow parties to remain anonymous or use pseudonyms during transactions. This anonymity can be exploited by money launderers who seek to conceal their identities and the source of their funds.
Complex Transactions	Escrow transactions can involve complex financial arrangements, such as multi-party transactions or transactions with international components. These complexities can make it easier for money launderers to disguise the true nature of their activities and move illicit funds across borders.
High Value Transactions	Escrow services often handle high-value transactions, such as real estate purchases or business acquisitions. Money launderers may target these transactions to launder large sums of money through the escrow account, taking advantage of the volume and size of the transactions to hide illicit funds.
Regulatory Arbitrage	In some jurisdictions, escrow services may operate with minimal regulatory oversight, creating opportunities for money launderers to exploit weaknesses in the regulatory framework. This lack of oversight can make it easier for illicit funds to be transferred through escrow accounts without detection.

#### 4.3.4 Inclusion of insolvency and business restructuring practitioners

The AGD has sought views as to whether ‘insolvency and business restructuring practitioners’ should be subject to AML/CTF laws and since these practitioners can take advantage of the complexity of financial transactions and the intimate knowledge of corporate structures and financial regulations, there are some money laundering risks associated, including:

Typologies	Description
Asset Stripping	Individuals involved in insolvency or business restructuring may strip assets from a financially distressed company before declaring bankruptcy or restructuring. These assets can then be sold or transferred to related parties, including shell companies or offshore entities, to conceal their origins and launder money.
Phoenix Companies	This involves the creation of new companies (often referred to as phoenix companies) to continue the operations of a failed business. Insolvency practitioners may be complicit in this scheme by facilitating the transfer of assets and liabilities from the insolvent company to the new entity. Money laundering occurs when illicit funds are injected into the new company or when funds from the old company are transferred to conceal their illicit origin.
Preferential Payments	Insolvency practitioners may make preferential payments to certain creditors or stakeholders during the liquidation or restructuring process. Money laundering can occur if these payments are made to conceal the origins of illicit funds or to benefit parties involved in criminal activity.
Insider Trading and Market Manipulation	In some cases, insolvency and restructuring professionals may have access to sensitive information about companies undergoing financial distress. They may use this information to engage in insider trading or market manipulation, allowing them to profit from illicit activities and launder money through legitimate financial markets.

#### 4.3.5 Other comments on proposed designated service examples

##### Proposed designated service 4

This should explicitly include private investments by individuals (i.e., individual angel investments) and by private equity/venture capital companies, who invest in technology companies that are often themselves regulated under AML/CTF laws (i.e., FinTechs), but many VC investors, who often take Boards seats associated with their investments are often unaware of the oversight obligations of a Board Director of an AML/CTF regulated entity.

##### Proposed designated service 5

The AGD is considering exempting testamentary trusts, but these could have anonymous beneficiaries who are not immediately identifiable or publicly known. Money launderers could exploit this anonymity by using trusts to distribute illicit funds to beneficiaries without revealing their identities, thus obscuring the source of the funds.

##### Proposed designated service 6, 7 and 8

Agree, no comments.

#### 4.4 Lacking detail on the commencement date or assisted compliance period

As noted above in the real-estate section, the AGD has noted that professional service providers would also be given an extended period to allow them to meet their obligations but further clarity to the industry is required in the following areas:

- What is the window of time that the AGD expects to have finished drafting revised legislation and have enacted?
- What is the AGDs current position on the approach to the roll out of AML/CTF laws to new sectors?
  - Will the implementation be staggered, or will the assisted compliance period differ by impacted sector?
  - If staggered, which industry would be required to implement first and what is the proposed running order?
  - How long does the AGD expect is reasonable for each industry sectors assisted compliance period to be?

#### 4.5 Legal and professional privilege

Agree, no comments.

#### 4.6 Extended timeline for reporting for legal professionals

**We do not agree that lawyers are as special as they think they are.** It seems that the AGD (as lawyers) also prescribe to this view and since they are so special, should be granted special treatment, allowing them extra time to provide reports, compared to 17,000 existing regulated businesses in Australia.

We believe all industry sectors should be treated the same as it relates to adhering to the reporting deadlines (i.e., 3 business days for suspicion of money laundering).

#### 4.7 Regulatory relief for pre-commencement customers

**We do not agree with the proposal.** The same reasons apply as for the real-estate profession that granting regulatory relief for pre-commencement customers is just “kicking the can down the road”. To reiterate, one of the reasons this dispensation was granted and made sense in 2006 for Tranche 1 businesses, was because there was a lack of viable technology to collect and verify customer information electronically. However, **18 years later** major technology developments allow millions of customer records to be “washed” against databases with exceptions being reported and we don’t not believe that the same regulatory relief is warranted and makes more sense to “bite the bullet” and apply the same CDD standards to existing pre-commencement customers as new customers.

We recognise the need to give newly regulated entities the time to do this (6 to 12 months would be more than reasonable rather than de-scoping entirely).

#### 4.8 Transitioning existing customers into the regime

We recognise the need to give newly regulated entities the time to do this and believe 6 to 12 months would be more than reasonable, given the availability of KYC solutions where customer data can be “washed” against third party reliable and independent data sources including screening lists and a Customer Risk Assessment (CRA) performed at the same time.

A “batch” process could be run within 1 day for hundreds of thousands of customers, so six months to plan, execute, implement, and update systems to reflect the risk assessment should easily be able to be achieved for most smaller businesses.

#### 4.9 Consultation Questions

No	AGD’s questions	Arctic Response
a	Are there any terms contained in the proposed designated services for PSPs that require a statutory definition to clarify their ordinary meaning?	See point on language, where Australia is making up its own variant language (i.e., PSPs), when the rest of the world calls this something else, DNFSBPs, why be different unnecessarily?
b	Should proposed designated service 3 be confined in a way to exclude services provided by sectors beyond PSPs?	No, there are money laundering risks associated with deceased estates, escrow services and insolvency and business restructuring practitioners that should be considered.
c	Is the current list of prescribed disbursements in proposed designated service 3 appropriate?	Yes
d	Are there any additional payments that should be included in the list of prescribed disbursements under proposed designated service 3 due to proven or demonstrable low risk?	No
e	With reference to proposed designated service 3, how often do you provide services relating to digital assets, and how does this differ from the services provided by dedicated digital asset service providers?	N/A
f	What additional information, guidance and materials would you require from AUSTRAC to help you comply with your new AML/CTF obligations?	Guidance on ML/TF risks and education on what is required in an AML/CTF program.
g	Do you have feedback on any of the proposals relating to legal professional privilege?	Only that lawyers should be given 3 days, not 5 to report SMRs.
h	What timeframe would you require to complete a risk rating for all pre-commencement customers (customers who you are in a business relationship with when the reforms commence)?	6 to 12 months maximum.



## Appendix 5 – Comments on [Paper 3 – Dealers in precious metals and precious stones](#)

### 5. General Comments

#### 5.1 Dealers in precious metals and precious stones are not the only high value goods

As described in section 9 above, the AGD ignored previous feedback provided that high-value goods dealers extend far beyond dealers in precious metals and precious stones, and we believe that the AGD should expand the AML/CTF laws to - Antique and Art Dealers; Auctioneers and Brokers; Motorised Vehicle Dealers and Luxury Goods Dealers.

However, if this is not something the AGD is considering on regulating, a public explanation as to why the AGD does not consider the money laundering risks to be high, when its predecessor the Department of Foreign Affairs and Trade (DFAT) wrote a whole detailed paper explaining the money laundering risks in these sectors to the Australian economy and society, which has been entirely ignored. **Please explain.**

#### 5.2 Reducing the threshold from \$10,000 to \$5,000

We believe the threshold should be lower than \$10,000 and be \$5,000 (which would align with lowered gambling threshold). Even at \$5,000, a criminal could easily go and buy 100 small diamonds with the proceeds of crime put them in a toothpaste tube and smuggle them across international borders and exchange them for clean funds.

#### 5.3 Lacking detail on the commencement date or assisted compliance period

As above the AGD has yet to provide a post-legislation timeframe for when businesses operating in these sectors are expected to comply with AML/CTF laws.

#### 5.4 Regulatory relief for pre-commencement customers

We agree that this is appropriate for this sector and unlike other 'designated services' much harder to retrospectively implement.

#### 5.5 Transitioning existing customers into the regime

We recognise the need to give newly regulated entities the time to do this and believe 6 to 12 months would be more than reasonable, for the reasons outlined previously.

#### 5.6 Consultation Questions

No	AGD's questions	Arctic Response
a	Do the department's proposed definitions of 'precious stones' and 'precious metals' capture the relevant materials dealt with by dealers in precious metals and precious stones?	Yes
b	Does amending the definition of 'bullion' in the Act help industry comply with AML/CTF obligations relating to bullion dealing?	Yes
c	To what extent would you be able to leverage existing systems and controls to meet the proposed obligations?	-
d	What additional information, guidance and materials would you require from AUSTRAC to help you comply with your new AML/CTF obligations?	As above
e	What timeframe would you require to complete a risk rating for all pre-commencement customers (customers who you are in a business relationship with when the reforms commence)?	6 to 12 months.

## Appendix 6 – Comments on [Paper 4 – DCEPs, remittance service providers and FIs](#)

### 6. General Comments

#### 6.1 Scope of designated services

We agree with the AGD's proposal to include all five services to bring Australia into line with FATF recommendations.

#### 6.2 Proposed amendment to Item 50A of Table 1 in section 6 of the Act

Agree, no comments.

#### 6.3 Proposed designated service 2, 3 and 4

Agree, no comments.

#### 6.4 Non-Fungible Tokens (NFTs)

The AGD has sought views as to whether NFTs and Stablecoins should be subject to AML/CTF laws. There are some money laundering risks associated with NFTs linked to their digital nature and potential for anonymity for the AGD to consider if it has not already:

Typologies	Description
Pseudonymity and Anonymity	NFT transactions often occur pseudonymously, with participants identified by their digital wallets rather than their real identities. This can make it difficult to trace the origin and destination of funds, allowing money launderers to transfer illicit funds without revealing their identities.
Cross-Border Transactions	NFTs can be bought, sold, and traded across borders with relative ease, often through decentralised platforms and blockchain networks. This global reach and the lack of centralised oversight make it challenging for authorities to monitor and regulate NFT transactions, creating opportunities for money laundering across jurisdictions.
Complex Transaction Chains	NFT transactions can involve complex chains of transactions, with tokens changing hands multiple times before reaching their final destination. Money launderers may exploit this complexity to layer illicit funds through a series of transactions, making it difficult to track the origin of the funds.
Use of Privacy Coins	Some NFT platforms and blockchain networks support privacy coins or tokens that offer enhanced privacy and anonymity features. These privacy-enhancing technologies can be exploited by money launderers to conceal the source and destination of funds involved in NFT transactions.
Market Manipulation and Pump-and-Dump Schemes	Money launderers may engage in market manipulation tactics, such as pump-and-dump schemes, to artificially inflate the value of NFTs and launder illicit funds. By driving up the price of NFTs through coordinated buying and selling, they can introduce illicit funds into the market and subsequently cash out through legitimate channels.
Integration with Traditional Financial Systems	NFTs are increasingly being integrated with traditional financial systems, allowing users to purchase them using fiat currencies or other cryptocurrencies. This integration creates opportunities for money laundering by facilitating the conversion of illicit funds into NFTs and vice versa, making it challenging for authorities to detect and prevent illicit activities.

Ultimately, NFTs can provide a transfer of value. And as these increase in popularity these can transfer a lot of value. For example, the most expensive NFT to be bought and sold was for USD\$91m (see [here](#) for a list of the highest value NFT transactions).

Because of these reasons we feel that NFTs should be regulated for AML/CTF.

#### 6.5 Amending the definition of 'digital currency'

There is an international term that is more commonly used and that is Virtual Asset Service Providers (VASPs), so maybe that would be more appropriate for Australia to adopt as "digital asset" is yet another terminology outlier used by Australia which is different to the rest of the world.

## 6.6 Ensuring the integrity of remittance providers and digital asset service providers

We agree with the AGD's proposal for a 'fit and proper' test. As we have seen with the CEO of Binance and the measly jail sentence he received that there is clearly a need for this power to be given to AUSTRAC.

## 6.7 Streamlining value transfer service regulation (including proposed services 5 and 6)

Agree, no comments.

## 6.8 Proposed definition of 'value transfer chain' (including proposed designated service 7)

Agree, no comments.

## 6.9 Updates to the travel rule

Agree, no comments.

## 6.10 Reforms to IFTI reports

Agree, no comments.

## 6.11 Cross-border movement of bearer negotiable instruments (BNIs)

Agree, no comments.

## 6.12 Additional issues

Agree, no comments.

## 6.13 Lacking detail on the commencement date or assisted compliance period

As above the AGD has yet to provide a post-legislation timeframe for when businesses operating in these sectors are expected to comply with AML/CTF laws.

## 6.14 Consultation Questions

No	AGD's questions	Arctic Response
a	Do you consider that the current term and associated definition of 'digital currency' is appropriate? What alternative terms outside of 'digital asset' might be considered, and why?	No, Australia should use the same language as is used internationally, Virtual Asset Service Provider (VASP).
b	How should the scope of NFTs subject to AML/CTF regulation be clarified?	We believe that NFTs should be regulated too. The largest NFT value transfer to date has been USD91m.
c	Are there any services that may be covered by the term 'making arrangements for the exchange...' that should not be regulated for AML/CTF purposes?	No.
d	Is the proposed language around custody of digital assets or private keys clear?	Yes.
e	Does limiting proposed designated service 4 to businesses 'participating' in an issuer's offer or sale of a digital asset clarify the scope of included services?	Yes.
f	Are there any services currently provided by financial institutions that fall outside the definition of 'electronic funds transfer instruction', but would be captured by the 'value transfer' concept?	Not that I can think of.
g	Is the terminology of ordering, intermediary and beneficiary institutions clear for businesses working in the remittance and digital asset service provider sectors?	Yes.
h	Is the introduction of a limited designated service with appropriate exemptions the simplest way to clarify the transaction monitoring and risk mitigation and management expectations for intermediary institutions?	Yes, probably.

No	AGD's questions	Arctic Response
i	What flexibility should be permitted to address the sunrise issue or where a financial institution or digital asset service provider has doubts about an overseas counterparty's implementation of adequate data security and privacy protections? What risk mitigation measures should be required?	There should be a requirement for a contractual agreement, with mandatory requirements including, a right to audit and/or commission an independent review, service level agreements and penalty clauses in agreements to support risk mitigation activities.
j	Do you consider that the existing exemptions for the travel rule are appropriately balanced?	Yes.
k	Are there challenges for financial institutions reporting cross-border transfers of digital assets, including stablecoins, on behalf of customers?	No, do not think there is.
l	Should the travel rule apply when transferring value incidental to a foreign exchange or gambling service?	Yes.
m	What is the anticipated regulatory impact for smaller financial institutions and remittance providers in giving them primary responsibility to report IFTIs sent or received by their customers?  Could this impact be offset by continuing to allow intermediary institutions to submit IFTI reports on behalf of smaller reporting entities, but with requirements for appropriate safeguards to ensure the accuracy and completeness of reports?	There is a risk they will not have the resources and therefore may poorly execute on this requirement (that is the same risk for larger organisations too).  The offset could work too, just need to make sure roles and responsibilities are clearly defined and managed to avoid over and under reporting.
n	What should be the 'trigger' for reporting IFTIs?  At what point is a reporting entity reasonably certain that the value transfer message will not be cancelled or refused, and the value transferred?	Inbound and outbound, above a threshold limit.
o	What information should be required to be reported in a unified IFTI reporting template, covering both IFTI-Es and IFTI-DRA's?	Will leave for others to comment.
p	Are there challenges with digital asset service providers reporting IFTIs to AUSTRAC as proposed?	Will leave for others to comment.
q	Would the proposed amendments to the BNI definition in the Act reduce the volume of reportable BNIs and regulatory impost on business?	Will leave for others to comment.

## Closing Remarks

Thank you once again for the opportunity to provide feedback. Whilst the second round of consultation has taken six-months longer than the AGD committed to and with very little communication with industry during that time, we can see there has been a lot of things to consider and we remain hopeful that the AGD can progress faster through the second round to issue laws into Parliament before the end of 2024.

I wanted to reiterate the main areas of concern that need further consideration and reflection on from the AGD:

1. Reduce the proposed timeframe for EWRA's from 4-years to Annually (which is the global norm) and anything else will expose us to (a) unnecessary risk (b) likely to result in a negative response from the FATF and (c) undo 17-years of progress by regulated businesses who are doing this annually now.
2. Provide more prescriptive information and make it explicit about the "triggers" for refreshing the EWRA. The triggers that have been provided are not explicit enough. I have provided a table of trigger-based suggestions that should be considered and hopefully accepted as an open-ended trigger like "if your business is changed" is not all that helpful.
3. AGD has omitted to extend the AML/CTF laws to other higher risk sectors, in particular other high-value goods dealers that its predecessor DFAT indicated were being widely used to launder criminal proceeds. No comment has been provided as to why the AGD disagrees with DFAT's paper that there is no money laundering risks in these sectors. We would request that the AGD reconsiders its position on this issue. If it is not planning to expand AML/CTF laws to these sectors a public explanation as to why should be the least the AGD could do as there is much evidence around how money is laundered through these sectors (see section 9 and my previous submission)
4. Reinstatement of the "Approved Persons" process AUSTRAC used to have. In the UK, the Skilled Persons Review Panel is successful at allowing the regulator to have a regulated entity appoint a Skilled Person to conduct a review of the AML/CTF Program and to publish the number of Skilled Person reviews that are underway. This process in Australia is not as transparent or clear as it is in the UK and could be improved.
5. No mention has been made to the other major flaw of Australia's AML/CTF regime that was highlighted in my first-round consultation paper and this one, is the fact that there is no explicit requirement for regulated entities to subject their AML/CTF Programs to independent review at least every two years (as is the case in New Zealand and many other countries). I have opined as to why this is important and should be considered. Again, if AGD is not planning to adopt this suggestion, a public explanation as to why it does not consider this to be an issue.
6. AGD has not committed to either (a) an implementation rollout plan (i.e., big-bang or industry-by-industry) or (b) suggested timeframes for implementation and any assisted compliance period following the laws being passed. Industry needs to be explicitly aware of how long they will have to implement these laws.

Since there have been at least two proposals made by me that have been ignored it might be helpful for the AGD to provide a summary of issues raised, considered by the AGD and a decision made not to act on the proposal, so that it is transparent that they are not being ignored and are being considered and the public can understand the rationale behind why no action is being taken.

As Australia is clearly playing "catch-up" to the rest of the world on Tranche 2 and has yet to implement the deficiencies FATF highlighted in 2015 in the last full-MER, the AGD needs to act with haste and conclude this process as soon as practicable and with FATF's follow-up visit Australia needs to have enacted laws no later than the end of 2024, to stand a chance of commencing the implementation of AML/CTF laws for the new sectors and hopefully avoid being grey-listed by the FATF.