Digital Economy Council of Australia

Digital Economy Council of Australia

Submission to AUSTRAC's consultation on new AML/CTF Rules

Date 14 February 2025

Digital Economy Council of Australia

About the Digital Economy Council of Australia (DECA)

The Digital Economy Council of Australia (DECA) is the peak industry body representing Australian businesses and professionals driving innovation in the digital economy through the use of blockchain technology, tokenised assets, and digital assets. DECA advocates for responsible adoption and regulation of these technologies, working closely with government and industry to ensure Australia remains a global leader in innovation and economic growth.

For further information or any inquiries, please contact:

Amy-Rose Goodey, Managing Director
Digital Economy Council of Australia (DECA)
amy-rose@deca.org.au

Alec O'Sullivan, Policy Analyst
Digital Economy Council of Australia (DECA)
alec@deca.org.au

General

1. Do any aspects of the Exposure Draft Rules create unnecessary friction with existing approaches to risk mitigation in your business or sector? If so, what are they? Are there alternative approaches that could achieve the same regulatory outcomes?

Yes, several aspects of the Exposure Draft Rules create unnecessary friction with existing risk mitigation approaches for DECA members. Specifically:

1. Inflexibility for Digital Currency Exchanges (DCEs): The Travel Rule requirements risk creating significant compliance burdens due to the lack of interoperability across jurisdictions and the "sunrise challenge" where some jurisdictions have not yet implemented the Travel Rule (DECA, 2023; FATF, 2021). This could disrupt cross-border transactions and increase compliance costs unnecessarily.
2. Complexity in Customer Due Diligence (CDD): The proposed shift towards dynamic risk assessments for every customer relationship introduces operational challenges, particularly for smaller entities, as it requires monitoring beyond current capabilities (DECA, 2023).
3. Group Reporting Requirements: The automatic formation of reporting groups creates ambiguity for decentralised business models, leading to potential duplication of compliance efforts (Urquijo, 2022). A more flexible lead-entity nomination model could address this issue.
4. AUSTRAC's Travel Rule requirements should align with Financial Action Task Force (FATF) standards and the evolving EU MiCA framework to prevent regulatory misalignment, which has already resulted in compliance difficulties for Australian businesses operating internationally. The "sunrise problem" remains a major concern, where Australian businesses must comply with the Travel Rule while counterparties in other jurisdictions are not yet required to do so. Without a phased, globally coordinated approach, Australian businesses risk being unfairly penalised for operating in a fragmented regulatory landscape.

Alternative Approaches:

- Staged Implementation of the Travel Rule: Introduce a phased approach to allow international jurisdictions time to align, as proposed by Dan Rutter (2025).
- Risk-Based Simplification: Adopt a more tailored risk-based approach for small DCEs and niche service providers to avoid over-regulation while maintaining effective controls (Chitimira et al., 2024; DECA, 2023).
- Clarity and Guidance: AUSTRAC should provide clearer examples and guidance on how reporting groups should operate, especially for decentralised and non-corporate structures.

2. Are any rules not sufficiently flexible to be scalable to specific circumstances of small businesses, sole traders or sole practitioners? Are there alternative approaches that could achieve the same regulatory outcomes?

Yes, several rules in the Exposure Draft are not sufficiently flexible to be scalable for small businesses, sole traders, and sole practitioners, resulting in disproportionate compliance burdens.

Key Issues:

1. Customer Due Diligence (CDD): The dynamic risk assessment requirement is overly complex for smaller entities with limited resources. Monitoring requirements significantly increase costs and operational strain.
2. AML/CTF Program Complexity: Requirements for independent evaluations and comprehensive governance frameworks are impractical for sole traders and small operators, who lack the infrastructure of larger institutions (DECA, 2023).
3. Travel Rule Obligations: Applying uniform obligations on all DCEs, regardless of size, creates an uneven playing field and risks discouraging small business participation in the digital asset sector (DECA, 2023).

Alternative Approaches:

- Risk-Based Proportionality: Compliance obligations should be proportionate to the size and risk profile of each entity, reducing unnecessary burdens on smaller businesses (FATF, 2021).
- Simplified AML/CTF Programs: Tailored compliance frameworks for small entities should focus on key risks rather than full-scale programs.
- Extended Transition Periods and Practical Guidance: AUSTRAC should offer longer transition timelines and targeted support to help smaller entities implement new requirements effectively (DECA, 2023).

3. Are any rules not sufficiently flexible to be scalable to specific circumstances of large or multinational businesses? Are there alternative approaches that could achieve the same regulatory outcomes?

Yes, some rules in the Exposure Draft lack the necessary flexibility for large or multinational businesses, particularly in terms of scalability and cross-jurisdictional operations.

Key Issues:

1. Travel Rule Implementation: The absence of global harmonization creates compliance challenges for multinational businesses. The "sunrise problem" means Australian

entities may struggle to ensure compliance when counterparties in other jurisdictions are not subject to similar rules (DECA, 2023; FATF, 2021).
2. Group Reporting Requirements: Automatic formation of reporting groups without sufficient clarity on lead-entity designation complicates compliance for large organizations with complex structures, especially those with decentralized or multinational operations.
3. Inconsistent Data Sharing Rules: Multinational businesses may face conflicts between Australian obligations and foreign data protection laws, making it difficult to share customer information within the group (Urquijo, 2022).

Alternative Approaches:

- Flexible Lead-Entity Model: Allow multinational groups to nominate lead entities with appropriate compliance infrastructure to coordinate AML/CTF obligations.
- Global Coordination: Align Travel Rule obligations with international standards to reduce cross-border compliance conflicts (DECA, 2023).
- Cross-Jurisdictional Guidance: Provide detailed AUSTRAC guidance on managing conflicting legal requirements for multinational operations.

AML/CTF programs

4. What is a reasonable period of time for you to document updates made to your ML/TF risk assessment or AML/CTF policies?

A reasonable period for documenting updates to ML/TF risk assessments or AML/CTF policies would be three to six months, depending on the complexity of the business and the nature of the identified risks.

Key Considerations:

- Small to Medium Enterprises (SMEs) may require up to six months to ensure updates are comprehensive and align with their available resources.
- Large or Multinational Entities can adopt a shorter three-month window due to their existing compliance infrastructure and dedicated resources (Urquijo, 2022).
- Trigger-Based Updates: Immediate updates should be mandated following significant events such as adverse findings in independent evaluations or changes in regulatory obligations.

This approach balances operational feasibility with timely compliance, ensuring that businesses remain agile while maintaining regulatory standards.

Reporting groups

5. What are the structures in your industry by which businesses exercise control over one another (e.g. corporate structures, partnerships, joint ventures, franchises, trust arrangements, decentralised operations and platform-based operations etc.)?

In the blockchain and digital asset sector, businesses operate under diverse structures, reflecting the innovative and evolving nature of the industry.

Common Structures:

1. Corporate Structures: Traditional companies that provide blockchain services, including exchanges, custodians, and technology providers (DECA, 2023).
2. Joint Ventures and Partnerships: Common for collaborative blockchain projects and consortiums focused on developing shared infrastructure, such as blockchain protocols or DeFi platforms.
3. Decentralised Operations: Increasingly prevalent with Decentralised Autonomous Organizations (DAOs) and other blockchain-based entities that operate without central management or traditional ownership structures (DECA, 2023).
4. Platform-Based Models: Used by digital asset marketplaces and token platforms that facilitate peer-to-peer transactions or token issuance.
5. Trust Arrangements: Occasionally used for managing digital assets on behalf of clients in custodial services (Urquijo, 2022).

6. Where you or your sector use group structures that do not involve ownership or control, what are these structures? Are there any impediments to sharing customer and compliance information within such groups for AML/CTF purposes?

In the blockchain and digital asset sector, group structures that do not rely on ownership or control are common and present unique challenges for sharing customer and compliance information.

Group Structures Without Ownership or Control:

1. Decentralised Autonomous Organizations (DAOs): Operate on smart contract protocols with no central management, making it difficult to identify a lead entity responsible for compliance (DECA, 2023).
2. Platform-Based Ecosystems: Networks of independent service providers (e.g., wallet services, exchanges, token issuers) working within the same digital ecosystem but without formal ownership relationships.

3. Industry Consortia: Collaborative groups formed to develop shared blockchain standards or infrastructure, which often involve multiple parties without a controlling entity.

Impediments to Information Sharing:

- Privacy and Data Protection Laws: Cross-border operations often face conflicting data privacy regulations that limit information sharing (Urquijo, 2022).
- No Central Authority: The absence of a lead entity in decentralised or collaborative structures complicates decision-making on AML/CTF compliance responsibilities.
- Technological Interoperability: Different systems and protocols used by participants may hinder efficient data exchange (DECA, 2023).

A flexible compliance framework that allows group members to nominate a compliance lead and clear AUSTRAC guidance on data-sharing protocols could help address these challenges.

7. Are there obvious lead entities in each of these structures? If so, what are their common characteristics?

Yes, there are potential lead entities in some of these structures, although they may not always be obvious due to the decentralised and non-traditional nature of the blockchain and digital asset sector.

Common Lead Entities and Characteristics:

1. Corporate Entities in Joint Ventures or Consortia: Typically, the entity with the largest operational stake or highest compliance capacity serves as the lead. This entity often provides governance, financial oversight, and reporting functions.
2. Exchanges and Custodians: In platform-based ecosystems, digital asset exchanges or custodians frequently act as lead entities due to their extensive regulatory obligations and established compliance teams (DECA, 2023).
3. Project Originators or Technology Providers: In decentralised structures, the entity or organization responsible for launching or managing the underlying protocol may assume a quasi-lead role (DECA, 2023).
4. Industry Associations or Coordinating Bodies: In consortia or collaborative structures, an association may act as a coordinating body to manage compliance efforts.

Common Characteristics of Lead Entities:

- Operational Control or Oversight: Even in decentralised settings, lead entities typically oversee key operations or act as primary service providers.

- Regulatory Experience: Lead entities often have the most experience with AML/CTF requirements and the infrastructure to manage compliance.
- Technical Capability: The ability to develop and maintain compliance tools, particularly for monitoring and reporting, is critical for lead entities.

8. What is the best way to implement a nomination model for a lead entity for structures that do not involve ownership or control of one group member over another?

The best way to implement a nomination model for a lead entity in structures without ownership or control is to adopt a flexible, risk-based approach that ensures accountability while accommodating the diverse structures in the blockchain and digital asset sector.

Key Steps for an Effective Nomination Model:

1. Allow Group Members to Self-Nominate: Members should agree on the most suitable entity to act as the lead, considering factors such as operational capacity, regulatory experience, and technical capability.
2. Risk-Based Criteria: The lead entity should be selected based on its ability to manage AML/CTF risks across the group, with AUSTRAC providing guidance on minimum criteria for eligibility (Urquijo, 2022).
3. Formal Agreement: Group members should sign a written agreement outlining the responsibilities of the lead entity and the scope of information sharing for compliance purposes (DECA, 2023).
4. Ongoing Review: The nomination should be reviewed periodically to ensure the lead entity remains the most suitable based on changing business conditions and risk profiles (FATF, 2021).
5. Independent Oversight: Consider third-party oversight or independent evaluation to ensure fairness and effectiveness in the nomination process.

A nomination model with these elements will provide scalability and flexibility, reducing compliance burdens while ensuring robust AML/CTF governance.

9. Within reporting groups, what are the circumstances in which a reporting entity members of a reporting group would want a non-reporting entity to discharge an AML/CTF obligation? Would this extend to discharging reporting obligations (threshold transaction reports, suspicious matter reports etc.)? What benefits would this provide to you?

Within reporting groups, there are several circumstances in which a non-reporting entity may be best positioned to discharge certain AML/CTF obligations on behalf of reporting entities.

This typically arises in situations where the non-reporting entity has specialized expertise or operational control over relevant activities.

Circumstances for Non-Reporting Entities to Discharge Obligations:

1. Centralized Compliance Teams: In larger groups, a central compliance team housed within a non-reporting entity may handle AML/CTF obligations for all group members, particularly in monitoring transactions and filing reports.
2. Third-Party Service Providers: Non-reporting entities that offer outsourced compliance services may take responsibility for customer due diligence (CDD), transaction monitoring, or suspicious matter reporting, especially for smaller entities within the group (Urquijo, 2022).
3. Technology and Data Providers: In groups with platform-based models, the entity managing shared technology or databases may be best placed to ensure compliance with transaction monitoring and reporting requirements (DECA, 2023).

Extent of Obligations:

- Threshold Transaction Reports and Suspicious Matter Reports: While non-reporting entities can support reporting processes, it is crucial that ultimate accountability remains with the designated reporting entity to avoid liability concerns. The non-reporting entity can prepare and facilitate submission, but formal filing should be the responsibility of the reporting entity.

Benefits of This Approach:

- Operational Efficiency: Reduces duplication of compliance efforts across group members.
- Improved Risk Management: Centralizing expertise leads to more consistent application of AML/CTF measures.
- Cost Savings: Reduces the financial burden on smaller group members by leveraging existing resources.

This approach should be guided by clear governance frameworks and formal agreements to ensure transparency and accountability.

10. Are there circumstances where reporting groups formed automatically under law would want to combine with other reporting groups and/or reporting entities? Why?

Yes, there are several circumstances where reporting groups formed automatically under law might want to combine with other reporting groups or reporting entities. This often arises to

achieve greater operational efficiency, enhanced risk management, and regulatory compliance synergies.

Key Circumstances and Reasons:

1. Shared Compliance Resources: Groups with overlapping services or clients may combine to share compliance infrastructure, reducing costs and streamlining efforts in transaction monitoring, customer due diligence (CDD), and suspicious matter reporting.
2. Risk Mitigation: Combining reporting groups allows for a consolidated approach to managing AML/CTF risks, ensuring consistent application of policies across a broader network, especially in sectors with high cross-border exposure (DECA, 2023).
3. Cross-Industry Collaboration: Businesses in fintech, blockchain, and traditional financial services may merge reporting capabilities to improve their ability to detect and respond to evolving financial crime typologies (FATF, 2021).
4. Centralized Governance: Merging reporting groups helps reduce compliance fragmentation, particularly for multinational entities or industry consortia, by designating a single lead entity responsible for compliance oversight (Urquijo, 2022).
5. Scalability and Growth: As businesses grow or expand internationally, combining reporting groups can help scale operations more effectively, ensuring compliance frameworks keep pace with the business's complexity.

A flexible, well-defined framework for combining reporting groups, with appropriate governance and regulatory guidance, would help facilitate these integrations while maintaining compliance integrity.

Customer due diligence

11. Are there practical implementation challenges you anticipate you may face in meeting the CDD obligations set out in the Exposure Draft Rules? If yes, what are they and do you have alternate suggestions as to how the same regulatory outcome can be achieved?

Yes, several practical implementation challenges are anticipated in meeting the Customer Due Diligence (CDD) obligations set out in the Exposure Draft Rules. These challenges primarily relate to increased complexity, operational costs, and data privacy issues.

Key Challenges:

1. Dynamic Risk Assessments: Requiring ongoing, real-time risk assessments for every customer relationship introduces significant operational burdens, especially for smaller businesses with limited resources.

2. Enhanced CDD for High-Risk Entities: The additional requirements for politically exposed persons (PEPs), nested services, and source of funds verification could be difficult to implement without causing delays in service delivery (DECA, 2023).
3. Data Collection and Privacy Concerns: Collecting and verifying extensive personal information, particularly for international customers, creates conflicts with data protection laws in some jurisdictions, complicating compliance (Urquijo, 2022).
4. Delayed Verification and Service Disruption: Limitations on when delayed verification is allowed could disrupt operations, especially for digital asset providers offering fast-paced services.
5. Verification of Place of Birth: Reporting entities will struggle to meet this requirement for every customer as the most commonly used database for verifications (DVS) does not collect Place of Birth.

Alternate Suggestions:

1. Risk-Based Simplification: Tailor CDD obligations to the size and risk profile of the reporting entity, focusing enhanced measures only on higher-risk customers and transactions (FATF, 2021).
2. Use of Self-Sovereign Identity (SSI) Solutions: Encourage the use of digital identity verification systems like MyGovID to streamline CDD processes while minimizing sensitive data storage risks (DECA, 2023).
3. Extended Transition Periods: Allow a phased implementation timeline for CDD obligations to reduce immediate operational strain on reporting entities.
4. Verification of Place of Birth: Appropriate infrastructure needs to be in place - e.g. Registry of Birth, Deaths and Marriages to provide data to DVS. Alternatively, remove the requirement to verify Place of Birth.

This flexible, risk-based approach will help ensure the same regulatory outcomes without overburdening businesses.

12. Are there any additional circumstances (e.g. particular types of transactions that require the urgent provision of a designated service) in which your sector may need to delay aspects of initial CDD to prevent disruption of the ordinary course of business?

Yes, in the blockchain and digital asset sector, there are several scenarios where delaying aspects of initial Customer Due Diligence (CDD) may be necessary to prevent disruption of business operations:

Key Circumstances:

1. High-Volume, Low-Risk Transactions: For services involving micro-transactions or small-value transfers in decentralized finance (DeFi), immediate verification may not be practical and could unnecessarily disrupt the user experience.
2. Market Volatility in Trading: During periods of extreme market volatility, immediate CDD could delay transaction execution, leading to financial losses for customers in trading environments (DECA, 2023).
3. Token Launch Events or Airdrops: Token sales or large-scale distributions (airdrops) often involve high volumes of participants. Requiring full CDD upfront could significantly slow down the process and impact the project's success (DECA, 2023).
4. Cross-Border Payments: In international transactions, especially where counterparties are from jurisdictions with similar AML/CTF standards, initial CDD delays may be necessary to ensure the transaction is processed without unnecessary delays (FATF, 2021).

Suggested Approach:

- Allow Delayed Verification for low-risk and time-sensitive transactions, provided appropriate risk mitigation measures are in place (e.g., thresholds and ongoing monitoring).
- Adopt a Tiered CDD System where the level of CDD is proportionate to the transaction's risk and value.

These adjustments would ensure operational continuity without compromising regulatory objectives.

Compliance reports

13. Does the 12-month reporting period of January – December, with a report lodgement period of the following January – March present significant challenges to your business due to conflicts with other Commonwealth, State or Territory reporting or lodgement requirements? What are these challenges?

Yes, the 12-month reporting period of January to December, with a lodgement window from January to March, presents several challenges for businesses in the blockchain and digital asset sector.

Key Challenges:

1. Overlap with Financial Year-End Reporting: Many businesses operate on the Australian financial year (July to June), creating misalignment and additional administrative burdens when preparing multiple reports for different periods.

2. Resource Constraints in Q1: The January to March window coincides with tax preparation, annual audits, and other compliance obligations, putting significant pressure on finance and compliance teams (DECA, 2023).
3. Cross-Jurisdictional Entities: For multinational businesses, reporting periods often differ between jurisdictions, adding complexity and increasing the risk of errors or delays in compliance reporting (Urquijo, 2022).

Suggested Solutions:

- Align Reporting Periods with the Australian Financial Year to simplify reporting processes for entities already complying with other regulatory requirements.
- Extend the Lodgement Period to provide businesses with greater flexibility and reduce pressure during high-volume reporting periods.

This would enhance efficiency and help businesses maintain accurate and timely compliance without undue burden.

14. Is there a preferable reporting or lodgement period?

Yes, a preferable reporting and lodgement period would be aligned with the Australian financial year (July to June), with a lodgement window from August to October.

Reasons for This Preference:

1. Alignment with Existing Obligations: Most businesses already prepare financial and compliance reports for the financial year, reducing duplication and administrative burden.
2. Reduced Resource Pressure: Shifting the lodgement window to August–October avoids conflicts with tax reporting and year-end audits, providing businesses with more time and resources for compliance (DECA, 2023).
3. Consistency for Multinational Entities: Aligning with international reporting standards and periods would simplify compliance for cross-border businesses (Urquijo, 2022).

This approach would improve efficiency and accuracy while minimizing operational strain during peak reporting periods.

Value transfer

15. Do the proposed criteria for identifying the ordering institution and beneficiary institution in a value transfer chain describe common scenarios in your industry? What

gaps or uncertainty would remain that could not be resolved through example scenarios and other guidance?

The proposed criteria for identifying the ordering institution and beneficiary institution in a value transfer chain generally align with common scenarios in the blockchain and digital asset industry. However, several gaps and areas of uncertainty remain.

Common Scenarios Covered:

1. Centralised Exchanges (CEXs): The criteria effectively cover typical value transfer chains in centralized exchanges, where institutions act as clear ordering or beneficiary institutions.
2. International Transfers: The definition of financial institutions in cross-border transactions aligns with traditional models of remittance and cross-border payments (DECA, 2023).

Gaps and Uncertainty:

1. Decentralized Finance (DeFi) and Peer-to-Peer Transfers: The proposed criteria do not account for DeFi protocols and peer-to-peer transactions, where there may be no clear ordering or beneficiary institution (DECA, 2023).
2. Private Wallets: Transfers involving private wallets present a challenge, as identifying an ordering or beneficiary institution is often impossible (FATF, 2021).
3. Alternative Payment Models: Uncertainty arises around nested services and layered financial models, where multiple institutions may participate without a clear role differentiation.

Suggestions for Improvement:

- Specific Guidance for DeFi and Private Wallets: AUSTRAC should issue detailed scenarios and guidance tailored to digital assets and decentralized protocols.
- Clarification on Layered Models: Provide case studies and examples for complex value chains involving multiple parties.
- Risk-Based Approach for Private Wallets: Consider a modified approach for transactions involving private wallets, focusing on known risks rather than requiring full identification.

16. Do the proposed requirements for the collection, verification and passing on of travel rule information create any friction other international travel rule obligations you may be required to comply with?

Yes, the proposed requirements for the collection, verification, and passing on of Travel Rule information create significant friction with international Travel Rule obligations due to inconsistent standards and implementation timelines.

Key Areas of Friction:

1. Sunrise Challenge: Not all jurisdictions have implemented the Travel Rule, creating gaps where Australian entities must comply, but their international counterparties are not subject to the same obligations. This results in operational inefficiencies and compliance risks (DECA, 2023).
2. Interoperability Issues: Different jurisdictions have varying data requirements, making it challenging to ensure seamless data exchange across borders. For example, address information is required in some regions but not in others (FATF, 2021).
3. Data Privacy Conflicts: Compliance with the Travel Rule may breach data protection laws in certain jurisdictions, especially in the European Union, where GDPR places strict limits on personal data sharing (Urquijo, 2022).
4. Technical Integration and Costs: Implementing systems that meet diverse international standards requires significant investment, creating higher compliance costs for smaller businesses.

Suggested Solutions:

- Harmonize with Global Standards: Align AUSTRAC's requirements with FATF recommendations and other key jurisdictions to reduce friction.
- Phased Implementation: Adopt a staged approach, giving businesses time to adapt as other jurisdictions implement their Travel Rule obligations.
- Use of Secure, Interoperable Solutions: Promote secure data-sharing platforms like TRUST to address interoperability and privacy concerns (DECA, 2023).

17. Can you identify any challenges you may perceive in establishing whether you are dealing with another virtual asset service provider or financial institution, and whether they are regulated, in relation to transfer of value involving virtual assets?

Yes, several challenges exist when trying to establish whether a counterparty in a virtual asset transfer is a Virtual Asset Service Provider (VASP) or a regulated financial institution.

Key Challenges:

1. Lack of Global VASP Registry: There is no universal registry or standardized mechanism for identifying whether a counterparty is a licensed VASP, leading to uncertainty (DECA, 2023).

2. Inconsistent Licensing and Definitions: Different jurisdictions have varying definitions of what constitutes a VASP or financial institution. This inconsistency creates confusion and increases the risk of non-compliance (FATF, 2021).
3. Anonymous Counterparties in Decentralized Networks: Transfers involving private wallets or decentralized finance (DeFi) protocols often lack identifiable counterparties, making it difficult to determine their regulatory status.
4. Verification and Due Diligence Gaps: Even when a counterparty is identified as a VASP, verifying whether they comply with the Travel Rule and meet AML/CTF standards is challenging, especially in less-regulated jurisdictions (Urquijo, 2022).

Suggested Solutions:

- Establish a Global VASP Directory: Encourage international collaboration to develop a centralized registry of licensed VASPs.
- Standardized Cross-Jurisdictional Guidance: AUSTRAC should issue guidance on how to verify counterparties in regions with limited or inconsistent regulation.
- Risk-Based Approach for Private Wallets: Focus on transaction monitoring and red-flag indicators for transfers involving non-custodial wallets.

Keep open notices

18. Is the information required to be provided in a keep open notice sufficient for you to determine if the customer to whom the notice applies, is a customer of yours?

Yes, the information required in a keep open notice is generally sufficient to determine if the customer is known to the business, but there are a few areas where clarity and additional details would improve its effectiveness.

Current Sufficiency:

- Customer Identification Details: Key identifiers like name, date of birth, and address are adequate for most reporting entities to verify whether the customer is in their database.
- Transaction or Account Information: When included, this helps confirm the customer's relationship with the reporting entity, especially for high-risk customers or those with multiple accounts.

Areas for Improvement:

1. Unique Identifiers: Including unique reference numbers, such as customer IDs or account numbers, would enhance accuracy and reduce the risk of false positives (DECA, 2023).

2. Clarification on Timeframes: Providing a specific timeframe for the customer's activity related to the notice would help reporting entities narrow their search more effectively (Urquijo, 2022).
3. Data Accuracy: Ensure that all required information is accurate and current to prevent misidentification.

Recommendation:

To improve the process, AUSTRAC could offer clear templates for keep open notices that include additional optional fields, reducing ambiguity and enhancing compliance accuracy.

19. Are the explanations in the keep open notice and the keep open – extension notices easily understood by you?

Yes, the explanations in the keep open notice and keep open – extension notices are generally understandable, but there is room for improvement to ensure clarity and consistency.

Current Strengths:

- Concise Structure: The notices provide straightforward information about the requirement to keep the account open and the duration of the notice.
- Clear Purpose: The notices clearly indicate that the intent is to support ongoing law enforcement investigations without compromising the investigation.

Areas for Improvement:

1. Simplification of Legal Terminology: Some explanations use technical or legal language that could be simplified for ease of understanding, especially for smaller or non-specialized entities (Urquijo, 2022).
2. Guidance on Next Steps: More explicit instructions on how entities should manage customer interactions and account activity during the notice period would reduce confusion (DECA, 2023).
3. Consistency Across Notices: Ensure that the language and structure remain consistent between the initial notice and the extension notice to avoid misinterpretation.
4. Further clarity: Provide clarity on what determines validity of a keep open notice and how long the AUSTRAC CEO will take to determine whether a notice is invalid. Where a reporting entity provides designated services prior to AUSTRAC's determination, is this a breach?

Recommendation:

AUSTRAC could provide annotated examples or FAQs with the notices to help entities better understand their obligations and actions required.

References

Bednarz, Z. and Zalnieriute, M., 2023. *Money, Power, and AI: Automated Banks and Automated States*. Cambridge: Cambridge University Press.

DECA, 2023. *Blockchain Industry Standards and Compliance Framework*. Digital Economy Council of Australia.

DECA, 2023. *Submission to Attorney General Consultation: Modernising Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime*. Digital Economy Council of Australia.

Chitimira, H., Torerai, E., and Jana, V.L.M., 2024. *Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector*. *Potchefstroom Electronic Law Journal*.

Cooper, K.A., 2014. *An Examination of the Anti-Money Laundering Legislative Framework for the Prevention of Terrorist Finance with Particular Reference to the Regulation of Alternative Remittance Systems*. *White Rose eTheses Online*.

FATF, 2021. *Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*. Paris: Financial Action Task Force.

Gupta, D., Miryala, N.K., and Srivastava, A., 2023. *Leveraging Artificial Intelligence for Countering Financial Crimes*. *Journal ID*.

Hamada, M., Nikolinakos–Lardas, M., Cavallo, P., and Law, S., 2017. *ICLG: Anti-Money Laundering and Compliance*. Association of Corporate Counsel.

Urquijo, M., 2022. *A Framework for Reporting Groups and Compliance*. Edinburgh: University of Edinburgh.

Vandasová, D., 2023. *Assessment of AML/CFT Practices and Suspicious Activity Reporting in the European Union Member States*. Charles University.