BDO

Tel: +61 8 6382 4600
Fax: +61 8 6382 4601
www.bdo.com.au

Level 9, Mia Yellagonga Tower 2
5 Spring Street
Perth WA 6000
PO Box 700 West Perth WA 6872
Australia

Via email: scamspolicy@treasury.gov.au

Scams Taskforce

Market Conduct and Digital Division
The Treasury
Langton Crescent
PARKES ACT 2600

29 January 2024

Dear Sir/Madam

CONSULTATION PAPER - SCAMS: MANDATORY INDUSTRY CODES

BDO refers to the invitation by The Treasury to provide comments and feedback in response to the consultation paper “Scams – Mandatory Industry Codes” **(Consultation Paper)**.

In summary:

- BDO welcomes the proposal of a dedicated Scams Code Framework to address scams.
- BDO recommends further consultation with designated sectors to ensure the Framework is effective in addressing the potential harm landscape.
- BDO recommends that the Framework includes ongoing feedback mechanisms, formal evaluation processes and reporting post implementation, to ensure it remains fit for purpose
- BDO proposes an expanded definition of ‘scam’ to broaden the scope of harms that could be regulated under the Framework.
- BDO recommends the development of guidance tools and templates to support all Australian businesses in identifying, preventing, detecting, and responding to scams. The standards of these tools should be monitored for continuous improvement opportunities.

As part of our submission, we have provided commentary on the proposed Three Principles underpinning the Scams Code Framework (pages 2 – 3) as well providing comments on some of the consultation questions in the Consultation Paper (pages 4 – 18). The commentary within this submission is based on the information provided in the Consultation Paper.

Should you have any questions or wish to discuss any of the comments made in our submission, please do not hesitate to contact our team on 07 3237 5841 or at conor.mcgarrity@bdo.com.au.

Yours sincerely

Michael Cassidy
National Leader, Forensic Services

Stan Gallo
Partner, Forensic Services

Conor McGarrity
Partner, Forensic Services

Three principles underpinning the Scams Code Framework

1. **Principle One: A whole-of-ecosystem approach to address scams:**

The effectiveness of a whole-of-ecosystem approach assumes some precondition factors exist. The success of the ecosystem approach will require ongoing support to ensure these factors are maintained. This should include:

- The full range of parties and sectors within the ecosystem is known, both by regulators and the parties themselves, and that these stakeholders also know the types of scams that could be perpetrated within the ecosystem (this would require ongoing monitoring, intelligence sharing and risk responses)
- Each of the parties in the ecosystem is a willing contributor, as the ecosystem is only as strong as its weakest link.

2. **Principle Two: The Framework must be flexible and responsive:**

The ability of perpetrators of tech-enabled crime to adapt is well documented. Key to an effective regulatory response will be the ability of the owners and participants of the Framework to:

- Identify new and emerging technologies and the opportunities they provide to scammers

- Continually monitor the threat channels and revise their prevention, detection, and response measures accordingly.

3. **Principle Three: The Framework will complement and leverage existing interrelated regimes, systems, and initiatives:**

As with any regulatory regime, its success will be dependent upon the simplification and lack of duplication in the ecosystem. Overlap in regulatory regimes can cause unnecessary compliance burdens and costs to the consumer.

The Consultation Paper acknowledges that the proposed Framework will complement and leverage existing interrelated regulatory regimes. In addition to the resources listed, other relevant regulatory focused resources that could be considered in designing the Framework include:

- Australian Standard 8001:2021 *Fraud and corruption control*
- Australian Standard 10002:2022 *Guidelines for complaint management in organisations*
- Commonwealth Ombudsman's, *Better practice complaint handling guide*.

The Consultation Paper also suggests potentially '*lifting effective voluntary scams initiatives into legislation by establishing them as either ecosystem-wide or sector-specific obligations within the Framework, where appropriate*.' There are considerations to both approaches, which we have outlined below.

Ecosystem-wide obligations

Legislating for 'effective voluntary scams initiatives' will require an up-front understanding and ongoing evaluation of anti-scam initiatives. This will require - at minimum - the following:

- A complete view of all current voluntary scam initiatives (prevention, detection, response) in operation
- A consistent method to evaluate their effectiveness
- An understanding of what works well and what needs improvement to inform a maturity roadmap.

It will be important to ensure that less mature entities or sector types do not get left behind to ensure no 'weak points' in the ecosystem for scammers to exploit.

Sector-specific obligations

Obligations specific to certain sectors will depend on those sectors having an existing baseline understanding of their scam threat landscape and scam typologies. Some relevant considerations for a sector-specific approach include:

- The risk of creating 'one-size fits all' obligations for an entire sector where entities within that sector may face vastly different scam types
- Sector-specific obligations need to be flexible enough to cater for entities within that sector that are of differing sizes, risk maturity and level of interactivity with consumers
- The design of sector-specific obligations involves input from all sector stakeholders, where possible.

These sector-specific considerations will better inform the regulatory response and enforcement strategy in terms of proportionality (e.g., less risk-mature sector entities may require an educative response rather than punitive in the initial stages of implementation).

Responses to list of stakeholder questions

The proposed Framework

1. **Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?**

The effectiveness of the proposed Scams Code Framework in addressing the harm of scams can only be determined once the range of harms is fully understood. BDO recommends consultation with the designated sectors to better understand what the 'potential harm landscape' currently looks like so that the obligations outlined in the paper can be designed to address those harms.

2. **Is the structure of the Framework workable - can it be implemented in an efficient manner? Are there other options for how a Framework could be structured that would provide a more efficient outcome?**

Operation of the Framework is based on a principles-based approach, set out via obligations. For its implementation to be efficient, the Framework's objectives need to be able to be able to be met through 'the minimisation of inputs employed to deliver the intended outputs in terms of quality, quantity and timing'.[1] In practical terms, this means that critical elements of the Framework need to be settled, agreed upon and well understood by all relevant stakeholders, including:

- **Objective:** the overarching objective of the Framework is clear and well understood.
- **Performance:** success criteria, outcomes and measures have been developed and communicated.
- **Roles and responsibilities**: visibility and specificity to reduce overlap and promote speed.
- **Reporting channels:** clarity for vertical reporting within sectors and across the Framework.
- **Feedback mechanisms:** intelligence is captured, analysed, and shared both within sectors and laterally across the Framework, and used to develop new codes, standards, and guides for participants.
- **Consumer's voice:** ongoing feedback loops from consumers of the sector products to understand user views on performance of the Framework.

BDO suggests that clarity in these elements will support more efficient and consistent outcomes from the Framework.

3. **Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?**

No comment

4. **Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?**

No comment

5. **Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?**

The Framework will be enhanced where it is informed by intelligence from designated sectors and entities, and from direct consumer input. This includes intelligence from future sectors where the Framework may become operational. The current Framework does not appear to incorporate future intelligence as part of its design, which may limit the Framework's ability to evolve through the capture and leveraging of scam intelligence from designated and future sectors.

6. **What future sectors should be designated and brought under the Framework?**

No comment

7. **What impacts should the Government consider in deciding a final structure of the Framework?**

The Framework involves bringing together sectors and regulators to provide an integrated (yet untested) approach to scam prevention, detection, and response. The final structure of the Framework needs to consider the potential impacts of any unforeseen regulatory burden on business and will require ongoing feedback mechanisms to be put in place. It will also need to consider any impact the

[1] This definition is provided in the Standard on Assurance Engagements ASAE 3500 *Performance Engagements* issued by the Auditing and Assurance Standards Board and the standard applied by the ANAO in its performance audits.

operation of the Framework has on services delivered to the consumer and the risk that the regulatory impost outweighs the benefits (e.g., where the service provided to the user is disrupted to a greater extent than the threat of the potential scam). This may require ongoing calibration of the Framework – in particular, the sector-specific codes and standards - as it is implemented, as well as a formal evaluation post-implementation (for example, after two years).

The definitions

8. **Is maintaining alignment between the definition of 'scam' and 'fraud' appropriate, and are there any unintended consequences of this approach that the Government should consider?**

BDO considers that maintaining alignment between 'scam' and 'fraud' is appropriate as both activities have, at their core, deliberate deception to benefit the perpetrator.

To ensure this alignment, it is essential to note the key differences between the definitions of scam and fraud, being that fraudsters exploit illegal access, whereas scammers employ psychological manipulation. From a financial perspective, scams often involve the theft of funds where the victim may have been tricked into providing access to their details to the scammer, whereas fraud usually involves financial theft without the victim's permission or knowledge.

9. **Does a dishonest invitation, request, notification, or offer appropriately cover the types of conduct that scammers engage in?**

BDO suggests that the current definition does not encompass all forms of conduct associated with scamming. For example, impersonation, coercion, and manipulation are missing from the list. Some scams do not involve an explicit invitation, request, notification, or offer. For example, identity theft or skimming credit card data might fall outside this definition.

It may be helpful to consider the broader ways in which scams happen, such as through "deceptive communication" or "misleading inducement" to offer a complete understanding of the types of conducts associated with scams.

10. **Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?**

BDO considers that the proposed definition of a scam lacks some harms that should be regulated under the Framework. One such example being scamming activity resulting in financial losses for individuals and businesses (the proposed definition includes the financial benefit from the scammer's perspective but does not include it from the victim's perspective). During the September 2023 quarter, the total lost by scam victims was over AU$105 million[3].

11. **What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?**

No comment

12. **Will the proposed definitions for designated sectors result in any unintended consequences for businesses that could not, or should not, be required to meet the obligations set out within the Framework and sector-specific codes?**

BDO notes the following unintended consequences for businesses as reported in other areas that may need to be considered in designing the Framework:

- **Increased Burden on Reimbursement:** As seen in the UK, under the Payment System Regulator (PSR) new APP-fraud requirements, the introduction of a new scam definition may lead to challenges in determining who to reimburse for scam-related losses, especially for large entities, creating a burden in identifying and compensating victims, as well as potential abuse of the reimbursement system by scammers and fraudsters.
- **Impact on Financial Inclusion:** The introduction of new scam definitions and reimbursement models may have unintended consequences on financial inclusion (e.g., where definitions or reimbursement models are complex or not easily understood by culturally and linguistically diverse groups), potentially affecting vulnerable customers and their access to financial services[3].
- **Regulatory Compliance and Investigation Timeframes:** Companies may face increased regulatory compliance requirements and longer investigation times for determining scam-related claims, leading to additional administrative and financial burdens and potential challenges in resolving claims.
- **Adaptation of Scam Techniques:** The addition of a new scam definition may lead to scammers adapting their techniques to circumvent the new regulatory Framework, potentially leading to the emergence of new scam methods.

13. **Should the definitions of sectors captured by the Framework be set out in the primary law or in industry-specific codes?**

BDO considers there are benefits and disadvantages to both regimes. Regardless of the approach chosen, ongoing review and consultation with stakeholders will be crucial to ensure definitions remain effective and relevant in the ever-evolving world of scams.

Some examples of the disadvantages associated with definitions being set out in the primary law include:

- **Less flexibility:** Lacks the ability to adapt quickly to new or emerging sectors or technologies.
- **Potentially over-inclusive/exclusive:** May unintentionally capture unintended entities or exclude relevant ones.
- **Increased legislative complexity:** Adds to the length and complexity of the primary law.

Some examples of the disadvantages associated with definitions being set out in the industry-specific codes include:

- **Potential for inconsistency:** Different definitions across sectors could lead to uneven application and confusion.
- **Reduced transparency:** Definitions may be less visible and subject to less scrutiny than those in the primary law.
- **Risk of regulatory capture:** Industry representatives setting the definitions could lead to weaker protections for consumers.

BDO considers that the primary benefit of definitions in industry-specific codes over primary law is the extra flexibility it provides. Industry-specific definitions will be more easily modified and tailored to suit the full range of scam activity as it emerges over time, whereas definitions in primary law may be more difficult to modify and to obtain stakeholder agreement on. The inclusion of definitions in primary law remains available sometime after the Framework has taken effect and has been embedded by the designated sectors.

14. **What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?**

No comment

Overarching principles-based obligations

15. **Are there additional overarching obligations the Government should consider for the Framework?**

No comment

16. **Are the obligations set at the right level and are there areas that would benefit from greater specificity? e.g., required timeframes for taking a specific action or length of time for scam related record-keeping?**

No comment

17. **Do the overarching obligations affect or interact with existing business objectives or mandates around efficient and safe provision of services to consumers?**

The impact and interaction of the overarching obligations within the Framework on existing business objectives or mandates will vary on a case-by-case basis, depending on sector or specific operating context among individual businesses. Some examples of these interactions could include:

- **Enhanced consumer protection versus high compliance cost:** Implementing these obligations can lead to better scam detection, prevention, and response, creating a safer environment for consumers. However, the new obligations may represent an additional burden for businesses, requiring investment in resources, technology, and staff training to comply. This could impact operational efficiency and profitability in the short term. For example, the recent focus on cyber risk confirms that regulatory compliance is not a core function of many businesses and can mean extra resources may need to be diverted form 'business-as-usual' activities.
- **Reduced fraud losses versus disruption to legitimate activities:** Early detection and disruption of scams can enhance trust and reputation, minimise financial losses for consumers and businesses, improving overall efficiency and reducing costs associated with fraudulent activity. However, implementing overly sensitive scam detection mechanisms may have the opposite effect, disrupting legitimate transactions and potentially frustrating consumers.
- **Improved risk management versus competitive disadvantages:** The obligations encourage businesses to adopt proactive risk management practices around scam detection and

prevention, benefiting operational efficiency and resilience. If not implemented consistently across the industry, these obligations could put some businesses at a competitive disadvantage compared to others with less stringent practices.

- **Transparency and accountability versus fraud:** User-friendly reporting processes and complaint handling can increase transparency and accountability, improving customer satisfaction and reputation. However, if not correctly implemented the overarching obligations provide a gateway for fraudsters and scammers (e.g., where scamming methods are described in public information to would-be scammers but are not adequately controlled by some entities, leaving them vulnerable).

18. **Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?**

Like other fraud-related reporting mechanisms, there may be opportunities to minimise reporting burdens:

- **Centralised reporting:** Like the national cyber security hub, there may be efficiencies gained through establishing a centralised reporting mechanism where all stakeholders can share scam intelligence, incident data, and relevant information with a single responsible entity.
- **Information sharing and standardised reporting**: Exploring the use of secure information sharing platforms or databases where businesses can input data once, and authorised entities can access the information as needed. This information can be used for developing standardised reporting formats and protocols that are accepted by multiple entities to ensure consistency and facilitate the sharing of information without the need for businesses to tailor reports for different recipients.
- **Interoperable systems**: Encouraging the development of interoperable systems that allow businesses to share information seamlessly across different platforms used by regulators, industry bodies, and other relevant entities. This integration can reduce duplication of efforts and enhance the efficiency of reporting processes.
- **Collaborative industry initiatives**: Facilitating collaborative industry initiatives where businesses within the same sector collaborate to share relevant scam intelligence and incident data. This collective approach can reduce the individual reporting burden on businesses while ensuring comprehensive information sharing.
- **Clear protocols:** Defining clear protocols for reporting cross-sector scam activities. Businesses may encounter situations where scams span multiple industries, and having established procedures for cross-sectoral reporting can simplify the process for involved entities.
- **Automated Reporting:** Leveraging technology, such as automated reporting tools and systems, to streamline the reporting process. Automated reporting can help businesses submit required information efficiently, reducing manual efforts and minimising the reporting burden.

19. **What changes could businesses be expected to make to meet these obligations, and what would be the estimated regulatory cost associated with these changes?**

No comment

Anti-scams strategy obligations

20. **What additional resources would be required for establishing and maintaining an anti-scam strategy?**

- Developing and maintaining an anti-scam strategy may require businesses to invest in resources, secure technology infrastructure, and increase regulatory compliance activities. An investment in relationship-building within the scam ecosystem will be required to foster effective communication and collaboration with relevant stakeholders.

The specific resources required will vary depending on several factors, and could include:

- The scope and complexity of the information-sharing arrangements
- The number of stakeholders involved
- The type and sensitivity of the data being shared
- Existing technology infrastructure and resources.

The cost-benefit ratio of investment in scam activity versus core business operations may be less evident for some entities in the ecosystem, requiring careful consideration to ensure that the resourcing implications are well understood as part of the Framework design.

21. **Are there any other processes or reporting requirements the Government should consider?**

Experience with implementation of similar regulatory compliance regimes and Australian Standards suggests there are other reporting requirements that should be considered.

- **Incident Response Plan:** Mandating businesses to develop and maintain a comprehensive incident response plan tailored explicitly to mitigating the impact of scams would be helpful. This plan should outline detailed steps for immediate response, communication, and recovery in the event of a scam incident. Recent high-profile scams have involved the improper use of customer account details with one business – which was not in itself breached - used against another business. Response plans must consider this scenario and be able to address evolving scam techniques.
- **Training and Awareness Programs:** Paragraph 14 of the Commonwealth Fraud Control Policy[2] requires appropriate training for staff engaged in fraud control activities. A similar requirement could be implemented for a training program for employees involved in anti-scam activities. This program could cover scam detection techniques, reporting procedures, and cybersecurity awareness.
- **Consumer Education Initiatives:** The ACCC (Australian Competition and Consumer Commission) and National Anti-Scam Centre help raise awareness about scams, especially during the Scam awareness week. Encouraging businesses to engage actively in consumer education initiatives would help prevent scams. This could involve providing language-specific educational materials, hosting webinars, or conducting community-level in-person education sessions while collaborating with government agencies to raise awareness about common scams and preventive measures.

[2] https://www.ag.gov.au/integrity/publications/fraud-control-policy

- **Third-Party Audits:** As with similar compliance regimes (e.g., AML/CTF requirements), there could be a requirement for periodic third-party audits of businesses' anti-scam strategies and compliance with the Framework. This can provide an independent assessment of the effectiveness of measures in place, highlight deficiencies, and identify sector-wide opportunities for scam protection.
- **International Collaboration:** Encourage businesses to collaborate internationally in sharing information about global scams, particularly if they involve cross-border criminal activities. Facilitating partnerships with international agencies to strengthen the global fight against scams.
- **Incentives for Compliance:** Consider introducing incentive programs for businesses that demonstrate exemplary compliance with the Framework. This could include recognition, reduced regulatory burden, or other benefits to encourage a proactive and effective approach to anti-scam measures.
- **Public Reporting Portal:** Create a centralised, secure online portal for the public to report potential scams directly to relevant authorities in multiple languages. This could assist the reporting process for vulnerable consumers and provide valuable data for scam prevention efforts.
- **Regular Industry Summits:** Facilitate regular industry-wide summits or conferences where businesses, regulators, and other stakeholders can share insights, discuss emerging trends, and collectively address challenges in combating scams.

22. **Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to consumers that provides consumers an understanding of their rights?**

It could be beneficial to consumers if entities are required to prepare an annual anti-scam statement (statements) when the turnover exceeds a certain value or if they belong to a high scam risk sector to provide consumers with a better understanding of their rights.

These statements could set out the reporting entity's actions to assess and address scam risks in their operations. The Australian Government could publish these statements through a public register, similar to the operations of the Modern Slavery statement register.

Some of the information which could make up a company's anti-scam statement could include:

- Governance information
- Consumer rights and protections
- Education resources
- Reporting mechanisms
- Commitments to prompt actions.

23. **How often should businesses be required to review their anti-scam strategies, and should this be legislated?**

The frequency with which businesses review their anti-scam strategies should be risk-based and can vary depending on factors such as the dynamic nature of scam tactics, the industry in which the business operates, and the evolving regulatory landscape. However, legislation could stipulate a mandatory schedule for businesses to conduct reviews of their anti-scam strategies. This might include an annual or biennial requirement, providing a systematic approach to keeping strategies up to date.

Some additional relevant factors which can be considered when establishing a baseline requirement for review frequency can include:

- **Trigger Events:** Legislation could specify certain trigger events that necessitate an immediate review of the anti-scam strategy. For example, a significant increase in reported scams, a change in the business model, or the emergence of new scam tactics could trigger an unscheduled review.
- **Flexibility with Oversight:** Legislation can also allow for flexibility in review cycles but may mandate oversight mechanisms. For instance, regulators may have the authority to request an unscheduled review if there are concerns about the effectiveness of a business's anti-scam measures.

24. **Are there any reasons why the anti-scams strategy should not be signed off at the highest level of governance within a business? If not, what level should be appropriate?**

BDO considers that the anti-scams strategy should be signed off by top management as a visible demonstration of support. This requirement would align with the Australian Standard on Fraud and Corruption Control and is a strong affirmation to both the entity’s staff and clients that it takes its anti-scam responsibility to protect consumers seriously.

25. **What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?**

Regulators should be actively involved in overseeing and guiding businesses to ensure the effectiveness of their anti-scam strategies. A risk-based approach can help regulators prioritise engagement with high-risk businesses or sectors and adjust the level of support based on individual needs and risk profiles. This is important as anti-scam activity is not a core skillset and businesses, particularly those less mature, may need support in this regard.

Regulators can also offer guidance resources and support options, including self-assessment tools, best practice examples, and tailored consultations for businesses requiring additional assistance.

The regulators’ review and engagement functions with business might involve strategies to:

- **Develop and disseminate best practices:** Share knowledge and expertise on effective anti-scam strategies through guidance documents, case studies, and training programs.
- **Review and provide feedback on anti-scam strategies:** Offer constructive feedback on proposed or existing strategies to ensure compliance and effectiveness.
- **Monitor and enforce compliance:** Conduct audits and inspections to ensure businesses are implementing their anti-scam strategies effectively.
- **Facilitate industry collaboration:** Encourage information sharing and joint initiatives between businesses, regulators, and consumer protection groups.

Information sharing requirements

26. **What resources would be required for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework?**

The following resources would be beneficial for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework.

- **Human Resources:** Establish dedicated team responsible for liaising, coordinating, and facilitating information-sharing activities. This team may need members with expertise in cybersecurity, fraud detection, risk management, and legal compliance.
- **Technological Resources:** Invest in or develop a secure and encrypted information-sharing platform that facilitates the exchange of sensitive data among businesses, the NASC, and regulators. This could involve data encryption, secure communication channels, and data visualisation tools and take cross system requirements into account.
- **Legal and Regulatory Compliance:** Develop specific memorandum of understanding (MOU) with stakeholders outlining the scope, purpose, and responsibilities within the information-sharing arrangement. This will assist in ensuring compliance with privacy laws, data protection regulations, and any other relevant statutes.
- **Financial Resources:** Allocate funds for the training, development, maintenance, and enhancement of technology platforms that support information sharing and collaboration[3].

Additional considerations for information-sharing arrangements that contribute significantly to a robust anti-scam Framework include:

- Establish clear communication channels and protocols for timely and effective information exchange between partners.
- Define key performance indicators (KPIs) to track the effectiveness of information sharing and generate regular reports for internal and external stakeholders.
- Implement robust risk management procedures to address potential security breaches, data leaks, and misuse of shared information.
- Ensure that information-sharing adheres to data privacy regulations and respects individual rights.
- Establish clear protocols for safeguarding confidential information and preventing unauthorised access.
- Design information-sharing arrangements to be scalable and adapt to evolving scam trends and technologies.

27. **What safeguards and/or limitations (regulatory, technical, logistical, or administrative) should the Government consider regarding the sharing of information between businesses, the NASC or sector-specific regulators?**

[3] https://www.arnnet.com.au/article/1289772/aussie-businesses-forced-to-have-anti-scam-strategy-under-new-proposal.html

The Government should consider implementing the following safeguards and limitations regarding the sharing of information between businesses, the National Anti-Scam Centre (NASC), and sector-specific regulators under the anti-scam Framework.

- **Regulatory Safeguards**: Establish clear regulatory guidelines to ensure that information sharing complies with relevant laws and regulations, including data protection and privacy laws. This includes clear guidelines on the nature of information that can be shared, for what purposes, and under what conditions.
- **Technical Safeguards:** There needs to be creation/implementation of secure platforms with strong encryption, access controls, and audit trails to protect sensitive information from unauthorised access, breaches, and leaks. The access to this sensitive data should be on a need-to-know" principle to prevent unnecessary exposure and should be audited periodically.
- **Oversight and governance safeguards:** Establish accountability measures for entities involved in information sharing to hold businesses, the NASC, and sector-specific regulators accountable for adhering to agreed-upon safeguards and limitations.

Consideration should be given to whether the sharing of information between businesses should be opt-in or mandatory. If opt-in, safeguards must be in place to ensure information is restricted from businesses that have yet to opt-in.

28. **What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?**

There are existing information sharing arrangements relating to financial crime that should be considered:

- The Australian Transaction Reports and Analysis Centre (AUSTRAC) provides a centralised platform for private entities to submit details regarding suspicious matters and transactions.
- The Fintel Alliance initiative, set up by AUSTRAC to combat money laundering and other serious crimes, fosters sharing of information, financial intelligence and collaboration between its partner organisations (public and private) to investigate and disrupt criminal activities.

These mechanisms may be instructive to designing the Framework's information sharing arrangements.

29. **Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?**

The challenges of sharing and acting on intelligence include cultural, technological, and regulatory barriers. They can include, but are not limited to the following:

Technical Obstacles:

- **Incompatible data formats:** Information from various sources and data formats may be incompatible, making it difficult to integrate and analyse effectively.
- **Lack of secure data platforms:** Secure platforms for sharing sensitive information with appropriate access controls and audit trails may be lacking. These platforms could themselves become a target, especially where they hold sensitive data.

- **Data quality issues**: Inaccurate or incomplete data can lead to misleading conclusions and hamper efficient action.

Organisational obstacles:

- **Differing priorities and cultures:** Businesses and industry bodies may have different priorities and organisational cultures, leading to conflicting views on interpreting and acting on intelligence within 'effective' timeframes.
- **Internal silos and bureaucratic hurdles:** Information may get stuck within internal silos or face bureaucratic hurdles, delaying action or preventing it altogether.
- **Lack of trust and collaboration:** Lack of trust between organisations can hinder effective collaboration and information sharing.

Regulatory obstacles:

- **Data privacy regulations:** Concerns about data privacy and compliance with regulations like the *Privacy Act 1988* (Cth), which includes the Australian Privacy Principles (APPs), and sector-specific laws such as the *Security of Critical Infrastructure Act 2018* (Cth), which has implications for data security4.
- **Confidentiality agreements:** Existing confidentiality agreements with clients or partners may limit the disclosure of certain information.
- **Competition law concerns:** Sharing sensitive information between competitors may raise concerns about anti-trust laws such as the Competition and Consumer Act 2010[5].

Additional considerations for building trust and collaboration include, but are not limited to:

- **Fear of repercussions:** Businesses may be hesitant to act on intelligence for fear of negative consequences, such as reputational damage or legal action.
- **Lack of resources:** Implementing intelligence-based actions may require resources that are not readily available.
- **Decision-making biases:** Human biases can influence how individuals interpret and act on intelligence, potentially leading to suboptimal outcomes.

Consumer reports, complaints handling and dispute resolution

30. **What are the limitations or gaps that need to be considered in leveraging existing IDR requirements and EDR schemes for the purposes of this Framework?**

No comment

31. **If the remit for existing EDR schemes is expanded for complaints in relation to this Framework:**

    31.1. **What criteria should be considered in relation to apportioning responsibility across businesses in different sectors?**

[4] https://www.ag.gov.au/rights-and-protections/privacy

[5] https://www.accc.gov.au/business/competition-and-exemptions/competition-and-anti-competitive-behaviour

No comment

31.2. **How should the different EDR schemes operate to ensure consumers are not referred back and forth?**

No comment

31.3. **What impacts would this have on your business or sector?**

No comment

32. **Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework? Should there be equal across all sectors and how should they be set?**

No comment

33. **Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?**

While the Framework does not explicitly outline a clear pathway for compensation to consumers if regulated businesses breach obligations, some areas that may need to be considered include:

- The specific details of how this compensation would be determined, calculated, awarded and any associated target timeframes.
- Legal rights for claimants and regulated businesses and the role of courts or other decision-making bodies outside the court system.
- The responsibility of regulated businesses is to address breaches and compensate consumers, ensuring that businesses are held accountable for their actions.

The design of compensation pathways will be dependent upon the consumer complaints pathways in place in each of the sectors. This will involve consideration of preliminary consumer complaint review mechanisms (e.g., in-house, external sector specialist entity or external central entity).

Sector specific codes questions 34 - 42

No comment

Oversight, enforcement, and non-compliance

43. How would multi-regulatory oversight impact different industries within the scams ecosystem? Are there any risks or additional costs for businesses associated with having multi-regulatory oversight for enforcing the Framework?

The primary risk of a multi-regulatory oversight model arises where an industry or business within an industry my fall within the jurisdiction of more than one regulator. For example, a business may breach some of its principles-based obligations (ACCC oversight would be triggered) through lack of control over its digital platforms (ACMA oversight). To minimise any duplication or additional costs for business, the proposed Memoranda of Understanding between regulators may need to set out primary jurisdiction, and provide relevant examples of where this scenario may arise.

44. Are there any other factors the Government should consider ensuring a consistent enforcement approach?

The objective of consistent enforcement can be achieved with proper up-front consideration of lessons learned from other regulatory regimes:

- During the initial phase of implementation (e.g., first two years) regulators may need to adopt a 'guiding' rather than enforcement approach to help embed the Framework consistently.
- Regulators will need to demonstrate impartiality and integrity by being willing to explain their decisions and act on the feedback from stakeholders.
- The enforcement responses should be proportionate to the seriousness of the misconduct and should respond to the circumstances of the case.

45. Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?

No comment