Australian Banking Association

Strengthening Australia's cyber security regulations and incentives: Australian Banking Association submission

The Australian Banking Association (ABA) welcomes the opportunity to provide feedback to the discussion paper, *Strengthening Australia's cyber security regulations and incentives*. ABA promotes and encourages policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership. One of the banking sector's highest priorities is to work in partnership with Government and other stakeholders to effectively mitigate cyber threats. The banking sector values a strong and constructive relationship with government security and intelligence agencies, there is a long history of sharing and collaborating to keep customers and citizens safe.

Why should the government take action

1. **What are the factors preventing the adoption of cyber security best practice in Australia?**
2. **Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?**

While consumers and businesses have awareness of the importance of cyber security, there may be barriers to the adoption of cyber security best practice in Australia – noting these are not challenges unique to Australia. Cyber security best practices need to be adopted by all persons in the economy as broadly as possible to minimise the potential for cyber security criminals to exploit weaknesses.

At high level the challenges arise from a lack of consistent and actionable information for corporates, businesses and consumers. For entities and consumers, the multiplicity of messages and advice which differ from each other can be a barrier to the person taking action. For those entities that seek to provide cyber security information to their customers and stakeholders, the information barriers can dilute the impact of cyber security education. As a result, entities may lack an understanding of the risks, and the human and technology investment required to keep pace with the evolving threat landscape.

As such, ABA sees an important role for government in coordinating messaging and cyber security uplift efforts across stakeholder groups and sectors, and setting clear expectations of what entities should do to protect themselves and their customers. As a first step, ABA believes there is more value in uplifting cyber security capabilities and understanding, and ensuring relevant regulatory requirements are clear and efficient, with any enforcement options (including consumer-led court enforcement) being appropriately targeted, fault based and calibrated to recognise that even the most secure systems and services are still vulnerable.

The current regulatory framework

3. **What are the strengths and limitations of Australia's current regulatory framework for cyber security?**
4. **How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?**

Australia's cyber security regulatory framework is undergoing significant change. Nonetheless this consultation paper also identifies a number of areas where the mechanism for regulating is not clear and/or where the Commonwealth government does not have jurisdiction. Further, the level of cyber security awareness remains low in some critical sectors which are likely to be significantly affected by new or amending legislation which the government is proposing to introduce (such as under the *Security of Critical Infrastructure Act 2018* (SOCI Act)).

Australian Banking Association

Consultation on the related SOCI Act reforms has already highlighted many of the challenges arising in relation to cyber security regulation. ABA acknowledges that there is a difficult but important balance to be struck between, on the one hand, economy wide, consistent cyber security regulatory requirements that improve the nation's cyber risk position and, on the other hand, more specific or targeted measures which need to respond to specific risks and/or levels of risk. Using sectors or entity types does not automatically ensure the right balance.

Subject to a baseline of consistency in regulatory requirements, sector specific requirements ought to be risk based and should leverage, rather than duplicate, existing regulatory requirements where it is consistent with a risk based approach to do so. Such sector specific requirements should ideally address the complexities which can result for entities which service or operate in multiple sectors.

Where sector specific requirements impose a higher standard than any economy wide requirements, the sector specific requirements should apply in satisfaction or exclusion of the economy-wide requirements.

ABA also acknowledges there can be benefit in aligning to appropriate, objective international standards where that is possible, for example, ISO 27001 or NIST.

ABA suggests that the Department of Home Affairs (Department) address these issues of cross sectoral and international consistency and efficiency as part of current and ongoing cyber security regulatory reform.

Governance standards for large businesses

5. **What is the best approach to strengthening corporate governance of cyber security risk? Why?**

ABA provides comments on three aspects of the proposal: scope and coverage, legal effect of proposed standards and implementation.

Scope and coverage: the governance standards need to clearly specify who is a 'large business', as there are a number of existing definitions for tax and other purposes. The standards also need to address the treatment of entities that may move into and out of a 'large business' threshold, potentially multiple times.

ABA understands from the Department that the proposed governance standards would not apply to an entity that is subject to more specific standards under the critical infrastructure reforms. ABA asks the government to ensure this distinction is clarified in any implementing governance standards.

Further clarity will also be required for entities that may be indirectly subject to SOCI Act requirements, and for entities that may move in and out of the SOCI Act regime. For example, if a large business is a supplier to a critical infrastructure entity, but may not be directly subject to the rules made under the SOCI Act, it ought to be made clear whether these entities would still be expected to comply with the governance standards.

Legal effect of governance standards: ABA seeks further information about the legal form that the governance standards would take and what legal standing (if any) the standards would have.

ABA asks for clarity on the interaction between the proposed standards and other regulatory regimes. For example, depending on the requirements imposed under the governance standards and how they are applied and enforced, it may be appropriate for adherence with the governance standards to be taken to establish compliance with directors duties in relation to cyber security. On the other hand and consistent with ABA's response to questions 3 and 4, meeting more stringent specific regulation, such as APRA CPS 234, should be taken to also comply with the governance standards.

ABA also suggest clarifying that a supplier's compliance with the governance standards does not override or automatically replace existing contractual obligations such as providing attestation of compliance with CPS 234 or ISO 27001, or compliance with more specific and stringent cyber, privacy and infosec obligations such as those under Consumer Data Right (CDR) or proposed under

digital identity legislation. Whether and how private contract refers to any governance standards should be a matter for contracting parties.

Implementation: ABA strongly believes that rule-making in itself will not be sufficient to result in a meaningful improvement in cyber security awareness. As such, any governance standards would need to be accompanied by an implementation program that will be broadly and clearly communicated, made widely available, and provide large businesses with clear and actionable information or advice. Information and advice should address:

- What good looks like at a minimum level
- How to implement the governance standards in the large business
- How adherence to the governance standards is disclosed, noting disclosure must keep pace with the changing threat landscape

Ideally, communication about this initiative would be made in partnership with existing industry bodies and associations, and likewise education and advice would be provided in partnership with existing channels. ABA notes the Australian Institute of Company Directors provides a cyber training program which was developed in partnership with Data61 which could form part of the implementation program.

Finally, the government may wish to consider ways to establish a framework or an approach for oversight of compliance with the governance standard, to ensure the standards drive meaningful improvement in cyber security.

6. **What cyber security support, if any, should be provided to directors of small and medium companies?**

At high level the issues of communication, and provision of concrete and actionable advice remain the same, with greater sensitivity to the regulatory burden on these smaller companies. However also refer to question 8 and the case for baseline cyber security requirements to extend to all entities that hold personal information.

The partnership channels for communication and education or advice may differ for small and medium companies. It may be more important to have a clear 'checklist' of basic good cyber practices, such as what questions to ask IT providers, how to select suppliers, the importance of contract reviews. ABA notes the Australian Cyber Security Centre has issued guidance for SMEs.

As above, it would be important to clarify these governance standards cannot replace specific regulation on infosec, privacy and cyber security. However complying with these more stringent specific regulation could be taken to comply with the proposed governance standards.

7. **Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?**

Refer questions 5 and 6.

Minimum standards for personal information

8. **Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?**

ABA generally welcomes clear and consistent standards that protect the personal information of Australians. Critical infrastructure reforms have shown that cyber security regulation would likely need to address some details of technical controls. However, any whole-of-economy code or regulation needs to balance the baseline of prescription with a principles-based or risk-based formula to ensure

future proofing, in a rapidly changing technology environment. Examples of this approach can be seen in APRA CPS 234 and the current Australian Privacy Principle 11.

One foundational question may be whether the *Privacy Act 1988* is the appropriate vehicle for introducing the necessary level of detail relating to cyber security technical controls.

If the Privacy Act is to be used, the outcomes of the current Privacy Act review would affect the question of the appropriateness of such a code and potentially the code's effectiveness. ABA submits that if such a code is to be considered, it should be done in the context of the review and reform of the Privacy Act with a view to minimising the scope for conflict and added complexity. In this regard ABA notes that the Privacy Safeguards of the Consumer Data Right (Competition and Consumer Act 2010, Part IVD, Division 5) have added complexity as well as greater protections for consumer data.

ABA also observes that it seems potentially inconsistent with the Government's objective of strengthening cyber security regulations and incentives to be, at the same time, proposing to relax the protections for consumer data under Open Banking in order to extend the regime to a wider group of participants.

ABA notes in the digital identity context, the Digital Transformation Agency is working with state and territories to consider the application of privacy obligations to participants in the digital identity system, and would urge the Department to do the same or consider an alternative mechanism that does not suffer as a consequence of some of the limitations inherent in the current Privacy Act such as the fact that it does not extend to all entities which hold personal information.

ABA understands some stakeholders have expressed concern about a 'one size fits all' approach under a possible cyber security code. ABA's views are:

- Applying the conceptual framework under the Privacy Act, which protects data having regard to the sensitivity of the data and the risk of harm, the code could provide further clarity as to the data or information that should be subject to the highest level of protection, based on the potential harm that can be caused if such data or information is stolen and misused. For example, digital identity information, banking data. Note 'protection' refers to the infosec profile that should apply and should not prevent data from being moving or being held offshore.
- Where such data moves around the economy, the necessary protections should continue to apply and 'follow' the data or information. This avoids anomalous outcomes where data can cease to be protected if it moves between entities in different sectors – and personal or other information that can reveal significant intel about an individual can become more vulnerable to theft and misuse.
- Where possible the code should refer to existing regulation (where regulation is sufficiently robust) or objective international best practice. The code should seek to extend the coverage of existing regulation where warranted, based on the second principle.

This approach would have the advantage of allowing entities to rely on their compliance with these existing infosec or privacy obligations as evidence of their compliance with the cyber security code. It would also impose regulatory burden that is proportionate to the business model or type of information or data that the business would hold/process.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

Refer question 8 and the question whether the Privacy Act is the appropriate vehicle for introducing the necessary level of detail relating to cyber security technical controls. ABA supports adopting objective, internationally consistent standards such as ISO 27001 or NIST, noting some critical infrastructure sectors have expressed a preference for such international standards to be applied as part of the critical infrastructure reforms.

If the Office of the Australian Information Commissioner will administer the Code, government will need to ensure OAIC has appropriate cyber security and technical expertise. ABA reiterates the

importance of ensuring consistency of coverage and oversight for all parties that hold personal information.

10. What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?

ABA supports adopting objective, internationally consistent standards such as ISO 27001 or NIST, noting some critical infrastructure sectors have expressed a preference for such international standards to be applied as part of the critical infrastructure reforms.

Also refer question 8. ABA proposes an approach that provides further clarity as to the data or information that should be subject to protection and regulation. This approach should be technology neutral and sector neutral. For example, any person or entity that collects and holds personal information or biometric data should be required to comply with appropriate standards for the protection of that information or data, whether the person or entity does so as a technology company, financial institution, an outsourced service provider or because of the company's customer service optimisation.

Standards for smart devices, labelling for smart devices

ABA provides the following high level comments for consideration.

The government should consider how this will be implemented in industries where Australia is not a significant market for smart devices and if the costs will be as 'limited' as encountered in other markets. There is also likely to be limited ability of retailers to confirm or demand compliance by their suppliers.

Labelling should be consistent with those used by other major markets to reduce the level of confusion and the costs of having to apply different standards in different countries.

Imposing requirements on international suppliers to commit to a level of support may be problematic and, in some industries, may impose costs as the expectation will be that devices are replaced prior to expiration. The burden of the cost will differ depending on the market. There may be circumstances where the cost and decision to 'upgrade' is borne by the consumer and at the same time the consumer risks their service being discontinued if they do not 'upgrade'.

Responsible disclosure policies

22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

ABA in-principle supports this proposal with the following comments.

Responsible disclosure policies are more relevant for entities in some sectors (such as software/IT sectors) or possibly entities that manage larger and more complex IT in-house. Entities that rely on third party suppliers may have little ability to take action on the receipt of a report. A number of entities in the economy may not have the expertise or resource/time to fully engage with reports of vulnerabilities. For these entities, query if there may be a case for considering the obligations on suppliers.

For entities that adopt a responsible disclosure policy, there should be legal assurance for businesses and security researchers who identify vulnerabilities to create an environment that supports researchers, but also ensures businesses are not held to ransom through the withholding of information. In addition, any research needs to be conducted in an ethical and safe manner.

Setting specific timeframes for remediation of vulnerabilities needs to be considered carefully as doing so fail to take into account some specific mitigating circumstances which prevent the deployment of patches within prescribed timeframes, such as the need for customisation and/or testing and the

contracted service windows. The expectation that a vulnerability needs to be patched should also take in consideration where a device is 'end of life'.

Health checks for small businesses

23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

The impact of a health check proposal will depend on the effectiveness of incentives to undergo and implement the health check program. If these are not followed by substantive support and advice that can be applied to the individual needs of the SME, there is a risk that a health check program can create regulatory burden or the perception of regulatory burden for time-poor SMEs, without driving an improvement in cyber resilience.

Moreover, if an SME or a group of businesses suffers a cyber breach after undergoing a health check (because a health check would necessarily address general cyber matters rather than specifics), it could degrade the 'tick of approval' and raise questions about liability.

ABA suggests the government consider other ways of supporting an uplift in SME cyber security.

This should start with explaining 'why cyber security matters' and be followed by concrete and actionable advice to small businesses.

Trusted voices (small business associations and industry associations) could partner with government to provide broad reaching and/or more targeted education to their members. This would use existing communication channels for SMEs as well as allowing for more tailored advice for some sectors.

Communication and messaging would ideally be consistent across government and private sector. Targeted work should refer to an appropriate, common government standard or framework to ensure a baseline level of consistency in the advice that is provided to small businesses and assist with efficiencies. This could be adapted from a consistent national or international standard (such as NIST practice guides) and could consider a tool that helps SMEs to identify suppliers of cyber protections who have met a sufficiently rigorous baseline standard.

ABA notes there is already a large body of information – including government programs – that are targeting SME cyber security uplift. An example is the Department of Industry 'traffic light' health check. A first step could be consolidating, rationalising and coordinating existing programs as well as considering their effectiveness via post implementation reviews.

24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

Refer question 23. It is not clear whether the health check would be intended to provide consumers or businesses greater confidence in the SME's cyber security. As above, a cyber breach after an SME has participated in a health check could degrade the value of the 'tick of approval'. Such an incident can also raise questions about liability in case of a dispute.

For SMEs that supply other commercial entities or companies, ABA queries whether the health check program would provide significant value, to the extent there are already contractual obligations to comply with certain standards or provide attestations.

Also refer question 8-10. Where SMEs are subject to specific cyber security, infosec or privacy regulations, the health check should not replace these specific regulations. Therefore, in these circumstances, a health check may have little or no value for the SMEs.

25. Is there anything else we should consider in the design of a health check program?

To create rigour, the health check will need to be supported by an appropriate assurance framework, including how remediation is managed and if disclosure is required. If disclosure is to be required careful consideration would need to be given to the questions of to whom disclosure should be made and in what circumstances. Full public or discoverable disclosures could have the effect of increasing cyber risk for the disclosing entity.

If this is the case, the requirements under the health check and any assurance needs to be cost effective, i.e., the underlying technical requirements should not change regularly to require the acquisition of new software or hardware; or cost and/or time effective options should be explained (i.e., any time / cost trade-off in using cloud services).

Clear legal remedies for consumers

26. **What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?**
27. **Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?**

This proposal raises complex questions that cross multiple legal or regulatory regimes. ABA provides the following high level comments and would welcome further discussions with the Department.

- When would a consumer have a right of direct action? A right of action should be limited to cyber attacks or security incidents, not operational incidents. With this limit, the following scenarios should be considered and addressed in any legislation including existing legislation such as the Australian Consumer Law:
    - Impact on services due to change management by the entity or a supplier
    - Impact on services as a result of an outage or breach at a supplier governed by regulatory regime or other government decision
    - Where there are contractual arrangements for managing customer data
- What is the threshold for establishing liability? Clarity is needed on the standard that may apply. If the threshold is negligence, consumers and entities would also benefit from guidance about what may amount to negligence in the context of cyber security. Cyber attacks are unavoidable regardless of precautionary measures and ongoing investment in system resilience, and the impact of cyber attacks will differ. As such, consider whether consumers should be required to establish a loss of their personal information or data, as well as financial loss linked to the loss (and how may this be done), or whether the threshold for taking court action be evidence of a systemic failure to meet minimum cyber security standards and/or failure to protect personal information that results in serious harm.
- Interaction with specific regulation: consistent with ABA's response to questions 3 and 4, where sector specific requirements impose a higher standard than any economy wide requirements, the sector specific requirements should apply in satisfaction or exclusion of the economy-wide requirements. An entity's compliance with specific regulation (for example, CPS 234, infosec requirements under CDR) should be taken to be evidence that the entity has not breached a consumer guarantee for the relevant product or service.
- Deterring reporting under other regimes: If liability is linked to regulatory reports of cyber incidents, this could have a chilling effect on early and proactive engagement with regulators and impacted or potentially impacted data subjects.
- Impact on availability and cost of cyber insurance, the market for which is recognised as already 'hardening'. This can have consequential impacts on the cost of doing business and impact supply chain.

- Benefits for consumers: given some of these questions, there may be very limited benefit for consumers even if a direct right of action is introduced. Further, if not properly calibrated in recognition of the nature of cyber risk (e.g. 'not if but when and the role of states parties), any regulated right of action may have an adverse impact on the scope of innovation.
- Timing and staged approach: query whether a consumer right of direct action would have more benefit after the government has clarified and educated/supported businesses to improve their cyber resilience. When businesses have had opportunity to comply with clear rules and expectations, the introduction of a consumer right of action can provide additional incentive to review and maintain cyber standards.