2 September 2021

Digital Economy Resilience and Market Reform Team
Cyber, Digital and Technology Policy Division
Department of Home Affairs
Via email: techpolicy@homeaffairs.gov.au

RE: Strengthening Australia's cyber security regulations and incentives

The Australian Payments Network (**AusPayNet**) welcomes the opportunity to respond to the Department of Home Affairs' (**DHA**) '*Strengthening Australia's cyber security regulations and incentives*' discussion paper.

AusPayNet Membership and Role

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop regulations, procedures, policies and standards governing payments in Australia. Membership of AusPayNet is open to participants in, and operators of, Australian payments systems.

AusPayNet currently has over 140 members, including:

a) Financial Institutions (FIs), including the major banks and other Authorised Deposit-taking Institutions (ADIs), including credit unions and building societies;
b) the Reserve Bank of Australia (RBA); and
c) Operators or administrators of Australian payment systems.

AusPayNet's responsibilities include:

- controlling and managing risk in the Australian payments system;
- coordinating the operation of effective payment systems through facilitating industry collaboration, adherence to rules and system-wide standards; and
- developing industry policies and rules for the regulation of payment systems (also known as clearing systems) relating to cheques; direct entry (i.e. direct debit/credit); cards, and accepting devices (i.e. cards used for in-store purchases at Point of Sale (POS) terminals, ATMs, or mobile/online purchases); high-value payments (e.g. between FIs); and the distribution of cash in Australia.

Introduction & Scope

This submission has been developed in consultation with AusPayNet's members and seeks to present views on facilitating secure information sharing. We highlight tension within current legislation that either directly or indirectly prohibits information sharing, and point to how other jurisdictions have addressed similar issues. We have also provided some suggestions on how the regulatory environment may be improved for clarity, consistency and ease of compliance.

Importance of Private-Private Information Sharing for the Payments Industry

Within the Australian payments industry, cybersecurity failings can lead to various harms through breaches of privacy, scams, fraud, money laundering and terrorism funding. Participants need to share information to improve their preventative security measures and promptly take restorative actions. Without collective intelligence and coordination, individual participants are not sufficiently informed to deal with the increasingly sophisticated techniques used by malicious actors and whose actions are hidden among the intricate interconnectivity of global networks and infrastructure. One example includes the recent Accellion breach, which involved malicious actors obtaining unauthorised access to the servers of numerous financial, government and academic organisations. In Australia, both ASIC and Transport NSW were impacted. At the recent AFR Banking Summit held on 30 March 2021, APRA chairman Wayne Byres noted that whilst the Australian Banking sector had yet to be impacted by a significant cyberattack, the Accellion breach demonstrated "*the way a cyber breach can have a cascading impact through the wider system*.". Westpac chief executive Peter King also underscored the importance of information sharing to defeat hackers.[1]

Issues in the Regulatory Environment in Australia

AusPayNet has considered the list of discussion questions in Appendix A and found question 4 most relevant.

> Q4. Could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

Issue 1: Obligations in cross-sectoral legislation and sector-specific legislation at odds with benefits of information sharing

In the discussion paper, the Department noted its focus on three main cross-sectoral pieces of legislation (i.e. *Privacy Act 1988* (Cth)*, Corporations Act 2001* (Cth) and Australian Consumer Law[2]) and sought feedback on the clarity and enforcement of their requirements.

Compliance obligations within the relevant pieces of legislation are – in some instances – potentially at odds with the wider benefits attributable to information sharing. Companies recognise the need to be able to share information with other companies as part of verifying cyberattacks and safeguarding their cybersecurity interests. Currently however, some organisations may be dissuaded from doing so because they do not want to find themselves in contravention of other legislative requirements. One example is s180 *Corporations Act,* where the sharing of such information may not be believed by the director as being in the company's best interests. Companies are concerned with liability issues arising from leaks or misuse of the data they have shared.

Companies are also bound by other sector-specific legislation to not share information. Similarly, AUSTRAC is concerned that shared information is leaked and financial criminals could be alerted, which could disrupt ongoing law enforcement investigations or, if the suspects are found innocent, breach

---

1 Frost,J; Shapiro, J, March 2021, 'Cyber-attacks the 'biggest risk in banking', *Australian Financial Review*, accessed 1.9.21, https://www.afr.com/companies/financial-services/cyber-is-the-biggest-risk-in-banking-today-20210330-p57f5n

2 As set out in Schedule 2 of the *Competition and Consumer Act 2010* (Cth)

customers' privacy and reputation.[3] This concern has led to the prohibition on information sharing through s 123 in the *Anti-Money Laundering and Counter-Terrorism Financing Act* ('*AML/CTF*' Act). Under the s 123 "tipping off" provision:

> "(1) A reporting entity must not disclose to a person ***other than an AUSTRAC entrusted person***:
> (a) that the reporting entity has given, or is required to give, a report under subsection 41(2); or
> (b) ***any information from which it could reasonably be inferred*** that the reporting entity has given, or is required to give, that report."
> (emphasis added)

Companies sharing information with non-AUSTRAC parties could be committing a criminal offence, which carries penalties.

This and other legislation should be considered in more detail to consider enabling the sharing of different types of relevant information without breaching legislative obligations such as the Australian Privacy Principles. For example, the information shared to prevent cyberattacks could be anonymised but contain details of the attacks themselves to defend against them. In contrast, information shared to combat financial crime would require the personal information to find patterns and identify the criminals. The sharing could be within a secured environment.

<u>Best practices from other jurisdictions</u>

The competing interests contained in the relevant legislation can be reconciled with a policy that seeks to avoid total prohibitions on information sharing and instead lays out clear rules on when and how private-private information sharing can be conducted in a controlled manner. This will require provision for secure information sharing that could take the form of one of the options outlined below.

Policy change to enable information sharing with clear legal tests.

GDPR Article 6[4] on "Lawfulness of processing" specifies the conditions upon which information sharing is allowable in the EU. They include various legal tests of necessity, compliance with legal obligations, public or legitimate interests, and non-interference with customers' fundamental rights and freedoms. The provision allows for greater clarity in decision-making by setting clear parameters for the lawful reasons for which information can be shared.

AusPayNet sees value in streamlining and aligning with international standards, where possible. This has practical benefits in setting consistent expected behaviours and guiding corresponding business decisions.

---

3 AUSTRAC, 2021, *How to comply and report: guidance and resources on tipping off*, accessed 25.08.21, https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/reporting/suspicious-matter-reports-smrs/tipping

4 EU, 2021, *General Data Protection Regulation Article 6: Lawfulness of processing*, accessed 25.08.21, https://gdpr-info.eu/art-6-gdpr/

System to securely share information on external cyberattacks.

The 'Financial Services Information Sharing and Analysis Center' (FS-ISAC) in the US is another example for sharing information on external attacks. This platform was created in response to the US Homeland Security Presidential Decision Directives.[5] The cyber intelligence sharing platform is built on a tiered system of designations. The information shared is verified, anonymised and categorised according to the risks of misuse.[6] Access and timely broadcasts are then based on that risk. Participants are assured and encouraged to share their information and rely on others' information without liability issues. These clear expectations on how shared information will be managed can be a useful model to regulate private-private information sharing.

System to share information on suspicious patterns and work with enforcement agencies.

The Transaction Monitoring Netherlands (TMNL)[7] started by five banks is another example of sharing internal information on suspicious transactions. TMNL creates a national (chain) approach, which helps to identify unusual patterns in payments traffic that individual banks cannot identify. The banks work closely with government partners such as the Ministries of Finance and Justice and Security, the Fiscal Information and Investigation Service and the Financial Intelligence Unit. The aim is to leverage the return from the chain, from identification to detection, prosecution, and conviction of criminality. An amendment of the Dutch AML/CTF Act is foreseen to enable full-scale collective transaction monitoring and is due this month.[8]

Issue 2: Fragmented coverage and regulatory burdens due to various legislation dealing with sector-specific impacts.

In the discussion paper, the DHA noted the limited cross-sectoral coverage of the present legislative and regulatory environment. Currently, there is no cybersecurity-specific legislation. Instead, companies are complying with various legislation and regulations set up to manage sector-specific cybersecurity impacts. These include the *Privacy Act*, *AML/CTF* Act, and APRA's Prudential Standard CPS 234. Discussions on enacting more reporting requirements remain ongoing through the Ransomware Payments Bill in the House of Representatives.[9]

These developments create a potentially confusing and complex regulatory landscape involving different regulators, sharing/reporting requirements, and expectations on different reporting entities. It has been particularly challenging for small and medium-sized companies to understand and comply with them. The following is a summary of mandatory initiatives:

---

5 FS-ISAC, 2021, *Our History*, accessed 25.08.21, https://www.fsisac.com/who-we-are

6 FS-ISAC, 2021, *Traffic Light Protocol (TLP) Designations*, accessed 25.08.21, https://www.fsisac.com/tlp

7 TMNL, 2021, *Transaction Monitoring Netherlands: a unique step in the fight against money laundering* and the financing of terrorism, accessed 25.08.21, https://www.nvb.nl/english/transaction-monitoring-netherlands-a-unique-step-in-the-fight-against-money-laundering-and-the-financing-of-terrorism/

8 Ibid.

9 Parlinfo, Ransomware Payments Bill 2021: s8 on Notification of ransomware payments and s 9 on ACSC using provided information, accessed 25.08.21, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=LEGISLATION;id=legislation%2Fbills%2Fr6730_first-reps%2F0002;query=Id%3A%22legislation%2Fbills%2Fr6730_first-reps%2F0000%22;rec=0

Sharing/reporting initiatives	Ad hoc impacts	Reporting entities	Parties to be notified		
			Government	Companies	Consumers
Notifiable Data Breaches scheme under the *Privacy Act*	Personal information breaches	Companies with over $3M annual turnover	Yes (OAIC)	No	Yes
Fintel Alliance under the *AML/CTF* Act	Money laundering, terrorism financing and other serious crime	Designated services	Yes (AUSTRAC)	Case-by-case application	Case-by-case application
Notification to APRA according to CPS 234	Information security breaches	ADIs, funds and insurers	Yes (APRA)	No	No

The discussion paper suggested a model ('option 1' in Chapter 5) to clarify cyber security obligations under the *Privacy Act.* AusPayNet notes the existing obligation under Australian Privacy Principle 11 to keep personal information secure. The Privacy Act is under review, which could present an opportunity to improve the security of personal information. AusPayNet supports the review and has made comprehensive suggestions to that effect.[10]

Whilst this increased coverage would help for this specific purpose, there are some potential issues with using this approach for the purpose of cybersecurity. The Privacy Act's legislative objects limit it to issues related to ensuring the maintenance of privacy in the handling of personal information and thereby, limit its regulatory scope. Focusing on this Act alone does not cover other harms caused by the improper use of non-personal information. Therefore, the *Privacy Act* itself cannot address all issues associated with cyberattacks.

Insights from current practices and discussions in the payments industry

AusPayNet proposes that if a new specific regulatory regime for cyber information is proposed, it should look to streamline existing regulatory requirements and platforms to avoid further regulatory overlap and/or overly burdensome administrative requirements. We note the discussion paper highlights APRA's CPS 234 requirements as an example of a mature cyber security regulatory framework. Many of AusPayNet's members are subject to CPS 234. They have provided feedback that these requirements could provide a framework for a principles-based 'same risk, same rules' approach to delivering a baseline set of cyber security requirements that could be adopted by other sectors in the economy.

We also suggest that a principles-based 'same risk same rules' approach, based on CPS 234, with oversight from sectoral regulators on a coordinated, streamlined basis would prevent a single point of failure in terms of coordination and administration of the framework nationally. A streamlined approach would also assist with compliance through clear and consistent expectations across the economy.

[10] AusPayNet, November 2020, Submission to the Review of the Privacy Act by the Attorney-General's Department, https://www.ag.gov.au/sites/default/files/2021-02/auspaynet.PDF

Summary of suggestions:

- Enable private-private information sharing by including the concept of "Lawfulness of processing" and applying clear legal tests such as those in GDPR Article 6.
- Establish clear expectations on how data and notification are managed in private-private information sharing.
- Consider streamlining current legislation and regulations instead of adding new requirements to:
  (i) apply a 'same risk, same rules' approach to cover all entities of concern and set consistent expectations; and
  (ii) streamline reporting into a single platform and regulator, sector by sector.

Conclusion

AusPayNet appreciates the opportunity to comment on some of the legislative barriers and challenges our members face in the current regulatory environment and to contribute our insights from the perspective of the payments industry. We welcome a streamlined regulatory environment with improved clarity, coverage and enforcement and would also welcome the opportunity to engage further with the Department at any time on the issues raised in this submission.

Please contact Ms Siew Lee SEOW at [redacted] if you have any further questions.

Thank you and yours sincerely,

[redacted]

Andy White
CEO, Australian Payments Network