10 June 2022

Data Security and Strategy Team
Department of Home Affairs
Via webform.

RE: The National Data Security Action Plan

Australian Payments Network (**AusPayNet**) welcomes the opportunity to respond to the Department of Home Affairs' (**DHA**) '*National Data Security Action Plan*'. We share the DHA's policy objective of delivering a consistent whole-of-economy approach to data security.

AusPayNet Membership and Role

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop procedures, policies and standards governing payments in Australia. Our purpose is to enable competition and innovation, promote efficiency, and control and manage risk in the Australian payments ecosystem. AusPayNet has 150 members, including financial institutions, operators of Australia's payment systems, merchants, and financial technology companies.

Introduction and Scope

This submission has been developed through prior consultations with AusPayNet's members and seeks to present views on facilitating secure information sharing as it specifically relates to payments in Australia. We highlight where further clarity in the action plan is required through relevant examples including the tension within current legislation that either directly or indirectly prohibits information sharing to detect malicious actors, and 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, including ensuring that any new data security regimes remain consistent with the recommendations of the Australian Treasury's Review of the Payments System (the Treasury Review).

Importance of Data for the Payments Industry

With the advent of open banking through the Consumer Data Right, data hosting and the ability to securely share data is crucial to the Australian payments industry.

Further, 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 Frontier Payroll data breach, which involved malicious actors obtaining unauthorised access to sensitive payroll information including tax file numbers and bank account details, impacting private sector and government employees in Australia. At the 2021 AFR Banking Summit, APRA chairman Wayne Byres noted that, whilst the Australian Banking sector had yet to be impacted by a significant cyberattack, recent breaches demonstrate "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]

Question 3. Guidance and Principles-Informed Approach

What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?

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*.

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. The following is a summary of mandatory initiatives:

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

[1] Frost,J; Shapiro, J, March 2021, 'Cyber-attacks the 'biggest risk in banking', *Australian Financial Review* (link).

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.[2]

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 any regulatory regime for cyber information should look to streamline existing regulatory requirements and platforms to avoid further regulatory overlap and/or overly burdensome administrative requirements. Many of AusPayNet's members are subject to APRA's 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 cybersecurity 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.

Question 4. Streamlining Australian data Legislative and Policy Measures

How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market? What obligations are you most commonly subjected to from international jurisdictions?

Compliance obligations within the relevant pieces of legislation (i.e. *Privacy Act 1988* (Cth)*, Corporations Act 2001* (Cth) and Australian Consumer Law[3]) 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 of the *Corporations Act,* where the sharing of such information or negative news 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.

---

2 AusPayNet, November 2020, Submission to the Review of the Privacy Act by the Attorney-General's Department (link).

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

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 customers' privacy and reputation.[4] This concern has led to the prohibition on information sharing through s123 in the *Anti-Money Laundering and Counter-Terrorism Financing Act* ('*AML/CTF*' Act). Under the s123 "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.

Best practice from other jurisdictions

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.

1. Policy change to enable information sharing with clear legal tests.

GDPR Article 6[5] 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.

---

4 AUSTRAC, 2021, *How to comply and report: guidance and resources on tipping off*, accessed 25.08.21 (link).
5 EU, 2021, General Data Protection Regulation Article 6: Lawfulness of processing, accessed 25.08.21, (link).

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

2. 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.[6] 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.[7] 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.

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

The Transaction Monitoring Netherlands (TMNL)[8] initiative 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.

Question 5. Data localisation

Does Australia need an explicit approach to data localisation?

With the advent of the Consumer Data Right, which currently applies to banking but is being rolled out to other industries in due course, the consideration of who owns data and where is it stored is an important one for the payments industry. AusPayNet would like to highlight the Treasury Review recommendations which noted the importance of consistency between payment policy objectives and regulatory frameworks, especially in relation to data standards. [9]

---

6 FS-ISAC, 2021, *Our History*, accessed 25.08.21 (link).
7 FS-ISAC, 2021, *Traffic Light Protocol (TLP) Designations*, accessed 25.08.21, (link).
8 TMNL, 2021, *Transaction Monitoring Netherlands: a unique step in the fight against money laundering* and the financing of terrorism, accessed 25.08.21, (link).
9 Commonwealth of Australia Treasury: Review of the Australian Payments System p. 72

Question 12. Business of Different Sizes

Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).

AusPayNet supports a 'same risk, same rules' approach. Reiterating our response to the review of the Privacy Act and the proposed Small Business Exemption and threshold, AusPayNet notes that some smaller, especially newer, payment service providers might fall under the definition of a small business and many more if the selection criteria were changed to, say, number of employees. We also note that some smaller FinTech companies may have smaller workforces and therefore benefit if number of employees was used. Exemptions may create an incentive to create a corporate structure such that activities for which it is difficult to demonstrate compliance with the Act may be moved to a wholly owned subsidiary which met the definition of a small business. This may have unintended consequences, especially as many FinTech providers provide data-rich services to consumers. While these services may have a small footprint, they may still have significant impact, and would be expected to be protected by the relevant data or privacy legislation.

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.