Australian
Payments Council

Gregory Miller
First Assistant Secretary
Cyber Security Policy Division
Australian Cyber Security Centre
14-16 Brindabella Circuit
Brindabella Park
Canberra
ACT 2609

30 October 2019

By email: cybersecuritystrategy@homeaffairs.gov.au

Dear First Assistant Secretary,

The Australian Payments Council (APC) welcomes the opportunity to provide input into the development of *Australia's 2020 Cyber Security Strategy – A Call for Views* consultation (the Strategy). This submission provides a brief background on the APC's role, highlights the relevance of cyber security in ensuring payments system resilience, shares what work APC has undertaken to date on cyber security and future plans to strengthen systemic resilience and tackle financial crime.

Background

The APC is the strategic coordination body for the Australian payments industry and engages directly with the Reserve Bank of Australia's (RBA) Payment System Board (PSB). We foster the ongoing development of the Australian payments system to ensure it continues to meet the changing needs of Australian businesses and consumers with innovative, secure and competitive payment services. The APC's objective is to ensure that the Australian payments system continues to engender trust and confidence by exhibiting these key characteristics, notwithstanding the changing and increasingly fragmented landscape.

As the payments system has become more digital, it has developed a complex network of interdependencies that go beyond the boundaries of individual institutions and transcends borders. Indeed, many dependencies fall outside the traditional regulatory perimeter of the payments sector – and into areas such as the telecommunications and energy sectors. Council membership therefore encompasses members from not only banking and payment organisations, but telecoms and retailers. Alongside the growth in network complexity, consumer expectations have risen.

The consumer-led move away from traditional payment mechanisms such as cash and cheques creates a greater reliance on digital methods; consumers expect that the payments system will be "always on" and work with a minimum amount of fuss, reliably and securely. The payments industry has always been an advocate of security standards, including compliance with the Payment Card Industry (PCI) Data Security Standard (DSS)[1], which provides a minimum state of security for payment cards.

[1] PCI Quick Reference Guide, Understanding the Payment Card Industry, Data Security Standard Version 2.0

Systemic Resilience

In 2019, the Council released *Payments in a Global, Digital World* outlining key developments in the payments system relevant to systemic resilience.

The RBA has also commented on the implications of digitisation on systemic resilience. For example, Michele Bullock, RBA Assistant Governor (Financial System) has made several comments over the last year:

- **October 2018:** *Not surprisingly, given their central role in credit provision and holding deposits, financial institutions are high on the list of entities at risk from cyber-attacks. … If an attack disrupted payment systems it could cause significant difficulties for households and businesses and disrupt economic activity.*[2]
- **June 2019:** *…outages that affect the ability of households and businesses to make and receive payments, or access account information, can cause significant inconvenience and disruption. And with the increasing use of electronic payment instruments and the reduction in people carrying and transacting in cash, the resilience of these systems is becoming critical to day-to-day economic activity.*[3]

Likewise, the RBA's October 2019 Financial Stability review stated:

- *Information technology-related operational risks have become more prominent over time. This reflects the financial system having become more reliant on technology, more interconnected and more complex, with more frequent and sophisticated cyber attacks.*[4]

Other regulators have also noted this change. The 2019-23 Corporate Plan of the Australian Prudential Regulation Authority (APRA) identified cyber security as a component of the industry and technological shifts driving changes within its operating environment. APRA stated that "cyber risks are continuing to grow in scale and sophistication."[5]

In order to assist in positioning industry to respond to this changing environment, the Council's new strategic agenda has identified the new focus areas of ***systemic resilience*** and ***combatting financial crime***. We will release more details on these focus areas towards the end of 2019. Effective cyber security is a critical aspect for delivery on both these strategic areas.

Cyber Security Task Force

Cyber attacks are a risk to payment system availability and resilience and can result in payment fraud, which is why the APC identified robust cyber-security as an important asset for the payments community. In January 2017 the APC established the Cyber Security Task Force (CSTF), which was created to draw on industry expertise to identify strategic areas where further work in cyber security relevant to the payments system may be required. The CSTFs work to date has been focused on 'sharing of actionable cyber information'. Cyber is clearly a key priority for individual CSTF members who have made significant investment and committed resources to ensuring ongoing security and monitoring capabilities. Many

[2] Michelle Bullock, Speech to the 10th Annual Commonwealth Bank Global Markets Conference, *Building Financial Sector Resilience: A Decade Long Transition* (October 2018)

[3] Michelle Bullock, Speech to the Central Bank Payments Conference, *Modernising Australia's Payments System* (June 2019)

[4] RBA, *Financial Stability Review*, October 2019

[5] APRA, *2019-23 Corporate Plan*, September 2019

individual entities have a strong day-to-day working relationships with Government and cyber agencies. However, the CSTF identified a gap in the ability to share relevant and useful information with participants more broadly.

The CSTF considered a number of information sharing methods. These included utilising an existing industry body, building a bespoke solution or partnering with government. The initial focus has been on the latter, working together with the Sydney Joint Cyber Security Centre (JCSC).

In May 2018, the CSTF together with the Sydney JCSC, held a workshop to define the concept of 'actionable' information in this context, the type of data to be shared, ways of sharing the data and any barriers. The workshop was attended by cyber experts, payments community members and federal, state and government agency representatives. JCSC advised that a public/private framework for the sharing of actionable cyber security information, utilising the JCSC's information sharing portal, which was currently in development, could be a potential catalyst and an enabler for this work.

Whilst a number of user requirements, were identified by members for the development of an information sharing portal, including principles of participation and operational requirements. There were questions raised relating to potential legislative constraints to sharing this information, including privacy and ownership of the information shared and resultant data analytics.

The experience of the FinTel Alliance[6] provides a good example of what could potentially be achieved via a Public Private Partnership (PPP). However, PPPs still face a number of challenges, such as those faced by the CSTF, as highlighted in the recent report from the SWIFT Institute. These are "not only legislative, technical or data-driven, they also relate to relationships, trust and risk appetite"[7]. For some entities "concerns remain about their potential exposure to regulatory non-compliance action or the possibility that their commercial competitiveness could be reduced"[8].

In the absence of a PPP with government covering the sharing of information relating to cyber, the APC CTSF continues to explore the development of a technical solution that supports sharing of actionable cyber information in a secure way.

Government Plays a Key Role

The Council is of the view the Government and associated regulatory agencies should play a key role in facilitating specific market initiatives and regulatory changes to allow for a sector wide cyber information sharing portal.

In that context the Council is encouraged by the intention to grow partnerships between Government and industry in this area[9]. Whilst industry can continue to develop and improve closed-circle threat information sharing on cyber, the APC is supportive of the government's role in looking to expand and raise awareness

[6] The Fintel Alliance is a private-public partnership consisting of 25 government and private sector members. Alliance partners include major banks, remittance service providers as well as law enforcement and security agencies from Australia and overseas. They work together to - increase the resilience of the financial sector to prevent it being exploited by criminals and support law enforcement investigations into serious crime and national security matters.

[7] SWIFT Institute Working Paper No2017-003, Public-Private Partnerships to Disrupt Financial Crime, Chadderton and Norton, 28 May 2019, pg2

[8] SWIFT Institute Working Paper No2017-003, Public-Private Partnerships to Disrupt Financial Crime, Chadderton and Norton, 28 May 2019, pg1

[9] Australia's 2020 Cyber Security Strategy, A call for views, pg15

more broadly of cyber security skills for all Australians. This includes continuing to "Partner with Australian governments, business, education providers and the research community in a national effort to develop cyber security skills"[10]. In addition, and as highlighted by the Internet of Things (IoT) Alliance Australia, the increasing connectivity of devices brings with it a "plethora of risks, and three critical success factors are resilience, privacy and security"[11]. Therefore we welcome the launch of the IoT Lab "to enable investigation of IoT product security"[12].

A good international example of what can be achieved in cyber information sharing comes from European Central Bank (ECB) Euro Cyber Resilience Board (ECRB). The ECRB recently presented the *Cyber Information and Intelligence Sharing Initiative* (CIISI-EU)[13]. The core objectives of CIISI-EU are:

(1) to prevent, detect, respond and raise awareness of cybersecurity threats to ECRB members;

(2) to enable relevant and actionable intelligence sharing between ECRB members, law enforcement and be potentially extendable to the wider ecosystem;

(3) to encourage active contribution and active participation within a 'trusted circle', rather than passive consumption or weak usage; and

(4) to synthesise and actively propagate the sharing of strategic intelligence in addition to operational tactics, techniques and procedures (TTPs) and tactical indicators of compromise (IOCs).

Ideally something similar to the ongoing development of the ECRB could be delivered within Australia via the JCSC. This requires Government support, legislative changes and financial commitment. The Councils' CTSF would welcome further engagement with the Cyber Security Policy Division, as part of the development of Australia's 2020 Cyber Security Strategy in order to see what can be achieved in this important area.

If you have any further comments or questions relating to this submission, please contact Pardeep Grewal, Head of Policy ([redacted])

Yours Sincerely

[redacted]

Robert Millner
Chairman
Australian Payments Council

[10] Australia's 2020 Cyber Security Strategy, A call for views, pg31
[11] Internet of Things Security Guideline, IOT Alliance Australia, pg12
[12] Australia's 2020 Cyber Security Strategy, A call for views, pg27
[13] Second meeting of Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)