The Secretariat
Inquiry into Future Directions for the Consumer Data Right
The Treasury
Langton Crescent
Parkes ACT 2600

21 May 2020

Via email: data@treasury.gov.au

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to the Treasury Issues Paper, *Inquiry into Future Directions for the Consumer Data Right* (the Inquiry). AusPayNet is the industry association and self-regulatory body for the Australian payments industry. AusPayNet manages and develops frameworks, procedures, policies and standards governing payments clearing and settlement within Australia.

As the Issues Paper states, the Consumer Data Right (CDR) "*could be expanded to include 'write' access, that is enabling a trusted third party to change or add to data about a customer at the customer's direction and with their consent.*"

Introduction

A data economy can be described as a digital ecosystem in which data is gathered, organised and exchanged by a network of vendors for the purpose of deriving value from the accumulated information.[1] It has the potential to be transformational and expand opportunities and choices for the community as a whole. However, these opportunities do not come without risk. In order to maximise its potential, a well-functioning data economy needs a well-functioning governance framework.

In ensuring that there is a level playing field for an effective data ecosystem that is competitive for all Australians and Australia, the Inquiry should seek to lay the foundations that allow innovative products and services to be delivered with a high degree of confidence and trust.

Our submission will highlight how the payments sector, also a networked digital ecosystem, through the management of frameworks, provides a useful basis from which learnings and insights can be applied to establish the foundations of Australia's data economy.

The Australian payments system has undergone a substantial transformation over the past few decades. Much of this has occurred as competition between payment systems and participants, and improvements in technology have driven innovation in payment offerings to consumers and merchants[2]. During that time AusPayNet has evolved its governance of the payments system to meet changing customer needs, moving from predominantly cash and paper-based transactions to digital transactions. Through these changes we

[1] European Commission, *Communication on Building a European Data Economy, Digital Single Market*, COM (2017) Retrieved, 20 August 2018

[2] Modernising Australia's Payment System, Michelle Bullock, Assistant Governor (Financial System), Speech to the Central Bank Payments Conference, 25 June 2019

have successfully created a shared purpose amongst all stakeholders that has engendered confidence in the payments system. This was also recognised by the Productivity Commission in its Final Report on *Competition in the Australian Financial System*.

The successful operation of the payments system is predicated on trust; trust that the underpinning technology will work and trust that funds will reach the intended recipient at the right time. This trust is enabled through the operation of frameworks that deliver security and interoperability, and support the management of liability, between a wide range of competing service providers.

At its core, AusPayNet's constitution is designed to facilitate collaboration, and to champion self-regulation and system-wide standards; under that constitution, adherence to common frameworks has enabled competition and innovation, and promoted efficiency and control whilst effectively managing risk.

Applying this approach to data, the requirements for the success of a data economy are twofold:

1. **An Effective and Robust Governance Framework.** Payment initiation and write access will significantly increase the volume of customer interactions and underpin a wave of new interactions between consumers and businesses. Alongside this we are likely to see new risks in the broader economy, particularly with respect to consumer protections against criminal activities such as fraud.
2. **Customer Identification and Verification.** Financial institutions and organisations that offer payment services carry great responsibility to those they serve, given they are custodians of their money. Because of this, the identification, authentication and verification of individuals and organisations, with their consent, forms a key part of engendering confidence in the system.

The CDR should build upon existing structures across sectors rather than developing specific and siloed new ones. Across the financial services sector a number of regulators and organisations perform complementary roles and functions including the Reserve Bank of Australia (RBA), APRA, ASIC and AFCA. It would be cost effective and efficient to leverage the licensing, accreditation, standards setting and dispute resolution processes and procedures already in place. Whilst there should be consistency across the various sectors designated by the CDR, a single regulator responsible for managing all of these responsibilities would not, in our view, be able to fulfil the regulatory functions needed to support industry specific requirements nor the broader data economy needs.

As such, we would like to draw the Inquiry's attention to the need for alignment with existing inquiries and workstreams being undertaken by both industry and government, into the payments system. These include the RBA's *Review of Retail Payments Regulation*, the Senate Select Committee on *Financial Technology and Regulatory Technology* and the Council of Financial Regulators (CFR) *Review of Retail Payments Regulation: Stored Value Facilities.* It is important to consider the implications these reviews an inquiries may have for write access in a data economy.

Governance

Given the similarities between the requirements to support the safe flow of information in a data economy and the flow of money in the payments system, how the Australian payments industry enables the latter may provide a useful blueprint for establishing a safe, resilient and sustainable governance framework for the former.

An effective payments system exhibits four characteristics: resilience, adaptability, accessibility and efficiency (**Appendix 1**). These characteristics shape the industry's vision and could also be expanded to the broader data economy.

Implementation of these principles requires a robust governance framework that gives consideration to two related issues: firstly, the identification and composition of the governance structure itself (the "who") and the types of activities and functions it performs (the "what").

- **Who:** Australia's payments system operates on a co-regulatory model, involving the RBA and AusPayNet. This has proven highly effective, allowing Government and the RBA to set high-level principles and broad policy objectives, while industry focuses on operational implementation, creating innovative solutions and providing competitive offerings to business and consumers.
- **What:** The networked nature of payments means much of the ongoing operational work undertaken by the co-regulatory governance structure includes monitoring, compliance, reporting and enforcement. This is necessary to identify any challenges, pinch points and opportunities for all stakeholders. Many are delivered via shared projects. The shared approach ensures that consumer experience is always front of mind, and that changes and developments are implemented as seamlessly as possible. Other key areas include:
    - **Security:** Broadly defined, considerations include entry and access criteria, operational standards and interactions with consumers.
    - **Standards:** Standards operate at the international, national and industry-wide levels. Aside from security, standards also extend to areas such as the consumer experience, messaging interoperability and liability. Accessibility standards are also of increasing importance.
    - **Consumer protection:** This will be critical to success, particularly if the CDR is extended to include write access and payments initiation.

These aspects are outlined in more detail below.

Co-Regulation

The co-regulatory framework underpinning Australia's payments system has proven effective domestically and in a global context over a long period. In the absence of internationally agreed best practice for the management of a data economy, AusPayNet believes that there are learnings and insights that could be gained from the governance approach in payments that can be applied to the data economy.

The *Payments System (Regulation) Act 1998* was designed to operate on a presumption of self-regulation. This has meant intervention "only where it has considered it necessary in the public interest and where the industry has been unable or unwilling to address the Bank's concerns."[3]

The chief benefit of this approach is that it logically splits governance functions. Industry focuses on operational implementation (including shared projects), providing the regulator more independence to oversee the sector and set broad policy objectives. Given the rapidly accelerating pace of change in payments, self-regulation enables the industry to be more efficient and effective in response – meeting the needs of the participants in the system, as well as consumers. Collaboration amongst all key stakeholders (including incumbent financial institutions, international entities, new entrants and regulators) is a vital pre-condition to

[3] RBA Submission to Select Committee on Financial Technology and Regulatory Technology

implementing consistent, appropriate and acceptable standards, while retaining enough agility to rapidly adapt to the changing environment.

A similar approach might also serve the data economy – with Government setting a broad consumer right and industry identifying how and which system(s) are best suited to achieving the required outcomes (such as payment initiation). This approach allows Government to draw upon industry's deep technical knowledge and allows industry to leverage existing industry workplans. In this regard AusPayNet notes that the New Payments Platform (NPP) Roadmap includes implementation of payment initiation.

Security

The security of the overall system is a key element to preserving ongoing consumer trust and is crucial when moving money. Payments take into consideration security requirements at all stages: entry, ongoing operational requirements and customer interactions.

With respect to entry, AusPayNet's Frameworks have a tiered access/membership structure, based on risk. Our risk-based model promotes fair and transparent access. In alignment with our constitutional objectives, it ensures that we strike the right balance between safety/security and accessibility, competition and innovation. This model enables access at different levels, in a transparent and objective way, balancing the need for security against the need to enable sufficient access.

Taking security requirements into account, payment streams offer different entry paths. The direct entry systems allow for both Authorised Deposit-Taking Institutions (ADIs) and non-ADIs to connect, either directly or indirectly. Likewise, the Issuers and Acquirers Community permits members who are direct participants (issuers and acquirers); operator participants (such as the card schemes) and affiliate participants (manufacturers, vendors etc). While AusPayNet does not operate any cards infrastructure, we have been successful in developing a governance model that enables a wide array of stakeholders to come together to develop standards and guidelines on a range of issues. This was evidenced recently, for example, by the quick and flexible way in which the contactless PIN limit was temporarily increased from $100 to $200 in response to COVID-19.

Security requirements are ongoing, not just at point-of-entry. This requires a reporting infrastructure to be maintained within the governance body. Ongoing security requirements can also operate on a tiered model, on a risk-assessed basis. Again, our experience and model has proved effective.

Consumer protection is a key element of security. This broadly includes technical security aspects (encryption and tokenisation), legal aspects (liability) and social aspects (education and victim support). In recent years, the payments industry has invested significantly in technical security, including chip-and-PIN, biometrics and tokenisation. A more detailed discussion of consumer protection is provided below.

Standards

A payment system that is used by only a small number of businesses and consumers is less valuable than one broadly accepted across the economy. To drive wide acceptance, a system needs to operate to a common set of agreed standards. Given the international nature of the payments system, global standards recognise that end-to-end security for customer data is critical.

Developing and maintaining technology, security and data principles and standards is a key governance function for any digital channel. Common standards across the system are needed for a variety of purposes: security, message interoperability and consumer protection.

In line with the co-regulatory approach, AusPayNet has experience at all levels of standard setting. We represent the Australian industry in international bodies, work with the industry on local standards and have experience in developing voluntary guidelines and principles for the domestic market.

Payment standards operate at several levels:

- **International standards.** Including those developed by the International Standards Organization, Payment Card Industry, World Wide Web Consortium and EMVCo.
- **Domestic Standards**. The adoption and application of international standards to the domestic market.
- **Industry-specific Guidelines.** These are developed on an as-needs basis to address emerging issues. AusPayNet recently undertook work to create the *Guidelines for Accessibility in PIN Entry on Touchscreen Terminals*. These are voluntary industry guidelines designed to assist people living with vision and/or motor impairments to make payments on point-of-sale touchscreens.

Consumer Protection

Accessibility is one of the four key characteristics of an effective payments system. Likewise, Australia's data economy should be inclusive and accessible to all, including those most vulnerable, for example those having low levels of digital literacy. For network industries such as data and payments, preserving overall consumer trust ultimately benefits all participants. Appropriate and effective consumer protection is a critical success factor for the data economy.

Again, the payment system provides a useful guide for consumer protection. The overall level of payment scams and fraud is small, and industry investments over the past several years have contributed to an overall drop in the fraud rate on cards.

Despite the low overall level of fraud, consumer protection remains an ongoing focus within payments. While overall fraud levels are low, the impact on individuals can be significant. As highlighted by the Australian Competition and Consumer Commission *Scamwatch*, scammers use every opportunity to take advantage of consumer uncertainty to exploit and play on their fears. Further, as the data economy evolves, new vectors of attack may emerge. Examples of work that the industry have undertaken in recent years to address these challenges is included at **Appendix 2**.

Liability for fraud, scams and mistaken payments initiated under write access needs to be clear for both organisations and consumers. The Australian Securities and Investments Commission's voluntary ePayments code (currently under review) provides some detail in relation to timeframes for bringing claims and processes for resolving disputes for some payment systems. However, the inquiry should consider how the ePayments Code could be applied to all accredited payment initiators. Clarity is also required on the external dispute body that would make determinations on payments initiated outside the financial sector.

An additional consideration is that current liability frameworks have evolved to cover existing payment methods. Typically, this involves an ADI initiating a payment on behalf of a consumer to a third-party. Payments initiation would add an additional risk vector, by allowing a third party to initiate the consumer payment. Existing liability frameworks would need to be considered in this light. For example, it could result in a transfer of liability from the ADI to the third-party initiator or by making the standards optional (thereby ensuring that adoption is a matter of competitive advantage, consistent with how other payment forms have evolved in Australia to date).

Customer Identification and Verification

The consumer-led trend towards online commerce and digital account creation and service delivery has increased the requirement for robust mechanisms to manage trust. Current approaches to identifying and verifying individuals online are fragmented and siloed, which has resulted in the proliferation of identity credentials and passwords. This proliferation has given rise to security vulnerabilities and created significant inconvenience and inefficiencies, which undermine the effective development of the digital economy.

In reviewing its responsibility to engender confidence in the payments system, and remove barriers to innovation through collaboration, the Australian Payments Council (a strategic body comprised of banks, retailers, telecommunications providers, technology companies and payment schemes) led the creation of the TrustID framework.

The TrustID framework improves the security, privacy and convenience of accessing online services and reduces the sharing of personally identifiable information. The framework is not a solution in and of itself; it presents a series of rules and guidelines for organisations to adhere to in their design and build of products and services. The business rules and technical specifications ensure interoperability between different service providers. Importantly, the framework is designed to support multiple and competing service providers, offering customers choice (**Appendix 3**). The framework could provide an important corner stone of the data economy and is open to all parties that meet the accreditation requirements.

A wide range of service providers are in the process of developing products that comply with the framework specifications which would appear to indicate that there is no requirement for CDR to consider mandates relating to digital identity and verification.

Summary

AusPayNet's submission highlights the prerequisites for a successful data economy: an effective and robust governance framework and customer identification and verification. The payments system relies upon a robust governance framework which addresses the key issues of governance, security, standards and compliance over the long term. This model has been tried and tested over time, as payments technology and consumer preferences have changed, and continue to change. It continues to engender trust from consumers and business alike. Utilising this experience and leveraging existing regulatory processes and procedures, not only provide useful learnings and insights, but could be a more cost efficient way of delivering a world class data economy for Australia.

AusPayNet would welcome further discussions with Treasury and other stakeholders on any of the issues we have highlighted in our submission, please contact Pardeep Grewal, Head of Policy pgrewal@auspaynet.com.au or 0407 616 819.

Yours sincerely

Andy White

CEO, AusPayNet

Appendix 1: Characteristics of an Effective Payments System

Resilience	**Stability**	Payments infrastructure is certain and predictable and provides a basis for delivery of well-defined and valued payment services to users through operators and service providers.
	Reliability	Payment services are available when users and service providers want them, and outages are minimised.
	Security	The system is structured to protect against unauthorised access to value and data.
Efficiency	**Resource Allocation**	Finite system resources are allocated for maximum stakeholder value.
	Sustainability	Operators and service providers are able to develop and maintain sustainable business models.
	Integration	Standardised, automated processes and straight-through processing minimise cost and risk.
	Liquidity	Money circulates rapidly at minimal friction cost.
Accessibility	**Ease of Use**	Consumers and businesses have access to a range of user-friendly payment services so they can choose how to make and receive payments.
	Reach	The payments system is widely accessible amongst users, so that payers can reach payees.
	Competitiveness	Payment service providers and operators have equitable access to underlying infrastructure so as to promote competition.
Adaptability	**Openness**	The payments system is flexible to accommodate new business models, business strategies and technologies.
	Innovation	Innovation in payment networks and payment services is encouraged, so that changing user needs are met over time.
	Collaboration	Where there are strong network effects, governance frameworks encourage operators and service providers to cooperate to bring about payments system improvements.
	Regulatory Certainty	Regulation (including self-regulation and industry standards) is clear, up to date and supportive of both cooperation and competition.

Appendix 2: Industry Work on Consumer Protection

At a technical level, recent industry work includes development and adoption of secure technologies such as real-time monitoring, machine learning, tokenisation and EMV 3-D Secure. As the self-regulatory body, AusPayNet's work has included:

- **Preventing Card Fraud:** Bringing together the entire range of stakeholders, AusPayNet developed and published the *CNP Fraud Mitigation Framework*. In addition to seeking to reduce the levels of online card fraud, the Framework is also designed to build consumer trust and support continued growth in e-commerce.
- **Supporting Victims:** AusPayNet worked with industry experts to develop an *Identity Theft and Scam Response Standard & Guidelines*, which could provide the basis for a consistent approach for victims of identity theft and scams and ensure consumers had the same customer experience regardless of the sector in which the payment was initiated.
- **Supporting Law Enforcement:** AusPayNet established the *Fraud in Banking Forum* in 2013. The forum holds quarterly meetings to promote informal dialogue between fraud specialists from Australia's financial institutions and law enforcement communities.
- **Monitoring and Reporting:** AusPayNet compiles and publishes fraud statistics twice-yearly to help increase awareness about fraud trends, prevention and security.

Appendix 3: TrustID Framework

The TrustID framework is designed to support multiple and competing service providers, offering customers choice. Positive consumer outcomes are enshrined in privacy, convenience and choice:

- **Privacy:** Solutions that adhere to the framework reduces sharing of personally identifiable info. Wherever practical, information is reduced to the minimum need to know. For example, there's a proof of age check threshold “over 18" assertion. It also ensures that data is only shared with trusted parties, accredited under the framework,
- **Convenience:** Organisations that adhere to the framework agree to process transactions from all other organisations. This mirrors the "accept all cards" approach that we see in payments. Consumers don't worry that a merchant will refuse their particular brand of payment card and they shouldn’t worry about it in an ID context either.
- **Choice:** Consumers can choose a service provider from the banking, telco, retail or fintech sector. The framework is open to all providers, as long as they meet the rules and guidelines.

Competition and innovation are enabled by the following elements:

- **Modular approach:** A service provider such as a fintech could be accredited to provide an app that supports digital signature without going through a lengthy accreditation process for identity services. A fintech could start with an app and then grow out and develop greater functionality and be accredited for a broader set of functionalities at a later stage.
- **Level playing field:** A compensation mechanism is designed to promote fairness. Identity service providers control the commercial aspects of contracts with parties they offer services to. However, within the framework there is a cap on the amount that service providers can charge one another for cross framework transactions. The intention is to create a level playing field for new entrants.

Future relevance is not limited by technology:

- **Rules and standards:** The framework comprises a set of rules and standards, with no technology build. This is important because it allows for evolution of technology and the evolution of standards. Service providers select their own technology and can compete on technical expertise.