Future Directions Unit
Consumer Data and Digital Division
Treasury
Langton Cres, Parkes ACT 2600

24 October 2022

By email only: data@treasury.gov.au

Australian Payments Network (AusPayNet) thanks Treasury for the opportunity to respond to its consultation on the exposure draft legislation ('the draft Bill') to enable action initiation in the Consumer Data Right (CDR, 'the Program'). This consultation is a positive first step in empowering consumers with more choice by enabling them to instruct businesses to initiate actions on their behalf and with their consent.

Introduction

AusPayNet broadly supports the draft Bill, noting that it establishes a compulsory period of extensive consultation before an action type is declared and that rules will be made by the Minister to reflect the applicable obligations.

With the understanding that payments could be the first action type to be declared, this submission focuses on laying a solid foundation and setting the Program up for success. Specifically, we suggest sequencing the establishment of necessary supporting frameworks and legislative changes. For instance, this could involve starting with a cybersecurity assessment and then updating the Privacy Act. It would also require alignment with the payments licensing regime being implemented under the Government response to the Treasury Review of the Australian Payments System. This would lead to the creation of CDR rules and standards – reflecting the cybersecurity assessment and updated Privacy Act – with which payment licensees would need to comply.

Creating an environment based on security and trust

The recently released report on the Statutory Review of the CDR ('the Review') recommended (recommendation 2.6) that the Government 'consider undertaking a whole of ecosystem cyber security assessment to ensure that the CDR cyber security architecture continues to be fit for purpose into the future.'[1] Within the same month, there was a spate of cyberattacks on sizeable companies in Australia such as Optus[2] and Medibank[3], leading to the loss of personal identifiable data of over 2 million customers and shaking the confidence of Australians in companies' data handling practices. Research by the Australian National University found that people's trust in institutions such as Governments, banks, social media and telecommunications has fallen since the middle of the pandemic in 2020.[4] The same report shows that the percentage of Australians who agreed or totally agreed that they are concerned about the security and

[1] Commonwealth Treasury, 29 September 2022, Statutory Review of the Consumer Data Right - Report, p 43 (link).
[2] Australian Broadcast Corporation News, 3 October 2022, '*Optus Reveals More than 2 Million Customers had Personal ID Numbers Compromised in Cyber Attack*' (link).
[3] Australian Broadcast Corporation News, 20 October 2022, '*Medibank Admits Personal Data Stolen in Cyber Attack*' (link).
[4] Australian National University, 19 October 2022, Data Trust and Data Privacy: A Brake on the Data and Digital Dividend? - Report, Figure 1, p 7 (link).

misuse of their personal data and information – for example, data not being kept secure by websites, or becoming a victim of cybercrime and identity theft – has risen. These developments have proven recommendation 2.6 to be sound.

The draft Bill suggests a clear delineation between the regulatory obligations at the instruction layer (which is specific to the CDR) and at the action layer (which is covered by existing privacy regulation) to avoid creating challenges for Action Service Providers (ASPs) to comply with dual regimes. Nonetheless, Treasury raises the issue that the Australian Privacy Principles would not apply to Action Service Providers if their turnover is less than $3 million. In response to the Treasury's call for feedback on this matter, AusPayNet notes that privacy obligations should apply to all industry players. This is consistent with our submissions to the Privacy Act reviews held in 2020[5] and 2021[6]. We noted then that an exemption may create both a market distortion and confusion for individuals as to whether their information is handled fairly and transparently. It also implies that privacy is only important for larger organisations. We now add that there is a reasonable belief that if well-resourced companies like Optus and Medibank could falter, the risk is likely to be greater with smaller companies. This view aligns with recommendation 1.5 of the Review, which asks for privacy to be properly factored into the CDR designation design.

For these reasons, AusPayNet suggests undertaking a cybersecurity assessment and updating the Privacy Act to minimise the risk exposure of the whole CDR ecosystem.

Developing payment specific security and consent management in the CDR rules

Once the broader, minimum cybersecurity and privacy obligations are established, there is value in deeper consideration in the next consultation of payment specific security and trust issues, including factors such as resilience, exceptions and liability. This additional work to define the liability model for third party payment initiation should ensure that fraud, disputes, returns and data loss accountability are addressed across the instruction layer (which is specific to the CDR) and action layers (i.e. existing payment systems). This liability model should not conflict with existing payment scheme liability models but instead leverage them to ensure they can be extended to the wider range of participants in CDR.

When developing the rules, we also continue to note the need to harmonise the consent processes of CDR and PayTo[7].

Together, this will ensure a positive outcome for consumers and aid their understanding of both how they are protected and where they can seek redress if needed (e.g. defining the primary contact for the customer in a disputed transaction).

In addition to the abovementioned submissions, we would also point to our submissions on consultations on cybersecurity[8] and data security[9] given their relevance to the prevention of economic crime.

---

[5] AusPayNet, 29 November 2020, Submission to the Attorney-General's Department's Review of the Privacy Act 1988 (Cth) (link).
[6] AusPayNet, 10 January 2022, Submission to the Attorney-General's Department's Review of the Privacy Act 1988 (Cth) (link).
[7] PayTo (link).
[8] AusPayNet, 2 September 2021, Submission to the Department of Home Affairs' Consultation on Strengthening Australia's Cyber Security Regulations and Incentives (link).
[9] AusPayNet, 10 June 2022, Submission to the Department of Home Affairs' Consultation on the National Data Security Action Plan (link).

Aligning with the upcoming changes in the regulation of payments

Currently, Treasury is preparing to implement the recommendations in the Review of the Australian Payment System.10 The three key recommendations are a strategic plan (to provide certainty on policy priorities), introducing a single, tiered payments licensing framework (to regulate entities performing a defined list of payment functions) and mandating the ePayments Code (to provide common consumer protections). These developments can potentially support the rules to enable payment initiation in CDR:

- They would clarify the entities performing the payment initiation or function and provide further input on the liability model initially proposed in the report on the Future Directions for the CDR.[11]
- They would also (through the strategic plan) provide the context for which payment systems would support CDR payment initiation and which (for example, legacy systems such as cheques and BECS) would not.
- And finally, they would provide a basis for payment licensees (including payment initiators) meeting the standards set within CDR.

The alignment of CDR with the implementation of the recommendations from the Review of the Australian Payment System would therefore create tremendous synergies.

Conclusion

AusPayNet appreciates this opportunity to advise the Government and assist in setting the Program up for success through our submission. We look forward to sharing our insights in further consultation on payment initiation and providing consumers with safe and efficient payment methods. We are pleased that the Review was supportive of our suggestions to date.[12]

About 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 currently has over 150 members, including financial institutions, operators of Australia's payment systems, merchants, and financial technology companies.

---

[10] Commonwealth Treasury, December 2021, Transforming Australia's Payment System - Report, p 43 (link).
[11] Commonwealth Treasury, October 2020, Future Direction for the Consumer Data Right - Report (link).
[12] Commonwealth Treasury, 29 September 2022, Statutory Review of the Consumer Data Right - Report, p 71 (link).