Level 24
1 York Street
Sydney, NSW 2000
paypal.com.au

03 February 2020

Australian Competition and Consumer Commission
GPO Box 3131
Canberra ACT 2601
By email: ACCC-CDR@accc.gov.au

Dear Sir/Madam,

Consumer Data Right: Consultation on how best to facilitate participation of third-party service providers

PayPal is grateful for the opportunity to provide our comments to the consultation by the Australia Competition and Consumer Commission (ACCC) on how the Consumer Data Right (CDR) rules should permit the use of intermediaries that collect or facilitate the collection of CDR data from data holders on behalf of accredited persons, as well as the possibility of expanding the rules to permit the disclosure of CDR data from accredited persons to non-accredited third parties and the appropriate consumer and privacy protections that should apply to such disclosures.

PayPal recognises the complex regulatory environment in the financial services sector, and we are pleased to provide specific comments in relation to the consultation.

About PayPal

Fuelled by a fundamental belief that having access to financial services creates opportunity, PayPal is committed to democratising financial services and empowering people and businesses to join and thrive in the global economy. Our open digital payments platform gives PayPal's 305 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online, on a mobile device, using an app, or in person.

Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money, and offers choice and flexibility when sending payments, paying or getting paid. PayPal's global platform, which includes Braintree, Hyperwallet, PayPal Working Capital, and PayPal Credit, enables consumers and merchants to send and receive payments in more than 200 markets around the world and in more than 100 currencies, and withdraw funds to

their bank accounts in 56 currencies and hold balances in their PayPal accounts in 25 currencies.

PayPal has been operating in Australia since 2005 and has more than 8 million active customer accounts. PayPal enables Australian businesses to transact online and offline, from sole proprietors and developers to established large merchants. The PayPal service is provided by PayPal Australia Pty Ltd which holds an Australian Financial Services Licence, and is also authorised by the Australian Prudential Regulation Authority (APRA) to provide Purchased Payment Facilities as an Authorised Deposit-taking Institution (ADI).

The Australian payments landscape is evolving at an unprecedented pace. As a global innovator in online payments, PayPal welcomes the opportunity to share insight and knowledge on both the opportunities and threats facing the payments industry, and to encourage innovation alongside responsible management of growth and change. PayPal is passionate about innovation in payments and is excited about the myriad benefits that such innovation can bring to the Australian economy.

PayPal Australia is supportive of Australia's approach to Open Banking which provides customers with choice, convenience, and confidence. The framework represents a considered and reasonable approach to how Open Banking should be implemented and establishes a sound regulatory approach on which to base the broader CDR. We welcome that the framework is based on API technology, as we believe that only an API-based approach for third-party access will deliver the optimal performance and best-in-class experience that consumers expect.

CDR will offer a myriad of opportunities for banks and third parties. PayPal believes that one of the biggest opportunities is related to identity verification. We strongly support that banks as data holders will be obliged to share the outcome of identity verification assessments performed on a customer, provided the anti-money laundering laws are amended to allow data recipients to rely on that outcome. PayPal believes the sharing of data to confirm identity for the purposes of regulatory obligations should be permitted to be securely and confidentially shared between institutions. This will limit customer inconvenience and improve efficiency of identification procedures for all financial service providers.
Below are our responses to the questions posed in the Consultation:

1. If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend (or intend to use an intermediary) to only

collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that intermediaries can bring to the CDR regime and for consumers?

We are of the view that intermediaries should be allowed to collect and use CDR data, as intermediaries allow for the following economic efficiencies:

- The ability to leverage global best practice learnings and solutions;
- Minimise the costs of integration with the CDR data APIs of multiple financial institutions and corresponding operational support; and
- Utilise data-driven value-added services.

2. How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.

PayPal believes that all participants in the CDR scheme should be accredited. This would give data holders and consumers the confidence that the third parties accessing the data will handle and manage that data with the appropriate level of care, security and protection. The rules should therefore be designed to allow intermediaries to be independently accredited to ensure the security of customer data and that the highest standards of data privacy are adhered to. Each entity that utilises CDR data should be solely accountable for the security of and usage of the data within its own ecosystem, technology infrastructure and customer experience flows.

Furthermore, we believe that the rules should provide companies with the flexibility to be engaged with intermediaries on an outsourced-vendor basis. This would provide companies with the flexibility to make arrangements with specific banks or third parties, thereby fostering competition and innovation.

3. What obligations should apply to intermediaries? For example, you may wish to provide comment on:

    - if intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current 'unrestricted' level, and the extent to which intermediaries should be responsible for complying with the existing rules or data standards;

- if intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and intermediaries;
- if the obligations should differ depending on the nature of the service being provided by the intermediary.

The operations of the intermediaries should not compromise the data security and quality of information shared through the CDR ecosystem. As such, on matters of data protection they should be regulated to the same criteria that apply to the current "unrestricted" level and should be wholly responsible for complying with the existing rules or data and security standards. Each entity that utilises CDR data should be solely accountable for the security of and usage of the data within its own ecosystem, technology infrastructure and customer experience flows.

4. How should the use of intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.

Under all circumstances, a data subject should be informed, and consent provided by them for the collection use and processing of their personal data by the third party. This should also clearly state if intermediaries are used and if so that the intermediary adheres to similar standards of data protection as the data controller and as legally required. Such privacy statements and collection notices should be located in an easily accessible place in the organisation's website and at the point of user onboarding.

Transparency is an overarching obligation and consumers should be informed about all aspects of the involvement of intermediaries before or at the start of the data processing cycle, i.e. when the personal data is going to be processed by the intermediary regarding data collected either from the data subject or otherwise obtained. Furthermore, the principle of transparency requires that any information and communication relating to the processing of those personal data be easy to understand, and that clear and plain language be used. The Privacy Statement of the data controller will therefore need to clearly explain the role of the intermediary.

5. How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to consumer consent, notification and deletion of redundant data, as well as any rules or data standards that should be met.

The data controller should be able to share and transfer data to other intermediaries provided the intermediaries meet at least one of the following prerequisites:

- It is for a legal and legitimate business reason
- In the public interest, e.g. prevention of fraud
- The data subject has consented to it

Should the personal data no longer be required for processing by the intermediary, it should be deleted within the confines of the retention schedule and as by law.

Furthermore, data controllers must ensure that personal data are securely delivered by the intermediaries to the right person. The transmission may become a possible source of risk regarding those data (in particular, in case of data exposure during the transmission). The data controller is responsible for taking all the security measures needed to ensure that personal data is securely transmitted (by the use of data encryption) to the right destination, and also continuing to protect the personal data that remains in their systems.

As such, data controllers should assess the specific risks linked with data portability and take appropriate risks mitigation measures. Such risk mitigation measures could include: if the data subject needs to be authenticated, using additional authentication information, such as another factor of authentication, such as a one-time password; suspending or freezing the transmission if there is suspicion that the account has been compromised; in cases of a direct transmission from a data controller to another data controller, authentication by mandate, such as token-based authentications, should be used. Data controllers will need to have appropriate contractual arrangements with the intermediaries regarding the protection of personal data and liabilities.

Another key requirement will be the format and compatibility of systems to ensure that data is provided in a structured, commonly used and machine-readable format, and to transmit those data without hindrance.

6. Should the creation of rules for intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used.

The requirements should ensure that the user is strongly authenticated by the service provider in the process of setting up the arrangement with the intermediary,

and that permission is not open ended. This protects the principle of data minimisation – i.e. only processing the data that is necessary to achieve the purpose consented to by the user, and not providing the third party a 'free for all' with a customer's data just because it is potentially available to the intermediary. Either depending on the level, type of service or user permission, the amount and extent of data shared should be controlled.

For example, if the purpose of sharing data with an intermediary is consolidation of account information, the same APIs should not be used as a way of electronically verifying an individual's identity without the consumer clearly consenting to that additional purpose, even if it is technically possible.

The rules preferably should be consistent with the majority of international jurisdiction's privacy laws. In most cases, data controllers are required to ensure intermediaries have a least a minimum standard of data protection is their own organisation or as required by law. Through instruments such as Binding Corporate Rules (BCRs) or Privacy Shields, data controllers are obligated to ensure that personal data is properly handled to the highest standard through the data protection value chain. Introducing an intermediary of a "lower" standard, may cause such instruments to be invalidated and may lower the overall level of data security protection afforded consumers.

Permitting CDR data to be disclosed to non-accredited third parties

7. If the ACCC amends the rules to allow disclosure from accredited persons to non-accredited third parties and you intend to:
    - receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers;
    - be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers.

We do not support the receipt and use of CDR data by non-accredited parties. Considering the increasing frequency of breaches and the impact on individuals due to lost data, we firmly believe that custodian firms should be held to the highest available standard of security and privacy and should fulfill accreditation requirements on a regular basis.

8. What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?

We do not support the receipt and use of CDR data by non-accredited parties. Considering the increasing frequency of breaches and the impact on individuals due to lost data, we firmly believe that custodian firms should be held to the highest available standard of security and privacy and should fulfill accreditation requirements on a regular basis.

9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to anon-accredited third party?

We do not support the receipt and use of CDR data by non-accredited parties. Considering the increasing frequency of breaches and the impact on individuals due to lost data, we firmly believe that custodian firms should be held to the highest available standard of security and privacy and should fulfill accreditation requirements on a regular basis.

10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?

We do not support the receipt and use of CDR data by non-accredited parties. Considering the increasing frequency of breaches and the impact on individuals due to lost data, we firmly believe that custodian firms should be held to the highest available standard of security and privacy and should fulfill accreditation requirements on a regular basis.

Please do not hesitate to contact Steven Chan, Regional Head of Government Relations for Asia Pacific ([redacted] if you have any questions or feedback in relation to the positions outlined in this submission.

Sincerely,

Neil Matthews
Chief Executive Officer
PayPal Australia