Mr Scott Farrell
Chair
Inquiry into Future Directions for the Consumer Data Right
C/-Secretariat
Inquiry into Future Directions for the Consumer Data Right
The Treasury
Langton Crescent
Parkes ACT 2600

25th May 2020

Dear Mr Farrell,

Thank you for the opportunity to respond to the *Inquiry into Future Directions for the Consumer Data Right.*

As a major participant in the global payments industry, Mastercard has a stake in policy development affecting financial systems in countries where we operate. In responding to the Inquiry, we consider the interests and perspectives of consumers, businesses, industry participants and other stakeholders in the payments industry as well as the financial system.

Our perspective is further informed by our role as a trusted service provider to a significant number of retail banks worldwide, our experience of payment services regulation and our role in receiving and processing data in the context of our wider business.

About Mastercard

Mastercard is a technology company in the global payments industry that connects consumers, financial institutions, merchants, governments, digital partners, businesses and other organisations worldwide, enabling them to use electronic forms of payment instead of cash and cheques. We make payments easier and more efficient by creating a wide range of payment solutions and services using our family of well-known brands, including Mastercard®, Maestro® and Cirrus®.

Our Core Operations and Network

We operate a unique and proprietary global payments network, our core network, that links issuers and acquirers around the globe to facilitate the switching of transactions, permitting account holders to use a Mastercard product at millions of acceptance locations worldwide. Our core network facilitates an efficient and secure means for receiving payments, a convenient, quick and secure payment method for consumers to access their funds and a channel for businesses to receive insight through information that is derived from our network.

We authorise, clear and settle transactions through our core network for our issuer customers in more than 150 currencies and in more than 210 countries and territories. Vocalink expands our range of payment capabilities beyond our core network into real-time account-based payments.

Our broader capability

We are a multi-rail network. Through our core global payments processing network, we facilitate the switching (authorisation, clearing and settlement) of payment transactions and deliver related

products and services. With additional payment capabilities that include real-time account-based payments (including automated clearing house (ACH) transactions), we offer customers one partner to turn to for their payment needs for both domestic and cross-border transactions across multiple payment flows. We also provide value added offerings such as safety and security products, information and analytics services, consulting, loyalty and reward programs and issuer and acquirer processing. Our payment solutions are designed to ensure safety and security for the global payments system including as it evolves.

We have an interest in the application of the Consumer Data Right to open banking and a capability to play a constructive role as it develops. This extends to related areas such as digital identity (which of course has applications that are not limited to open banking). We hope it is useful that we touch upon these capabilities at appropriate points as we contribute our comments to the consultation exercise.

Future directions for the Consumer Data Right

Mastercard has taken a keen interest in reforms to date and has participated in consultations supporting the creation of the Consumer Data Right (CDR). We believe that the safe, transparent and informed exercise of consumer choice as to how they pay should drive the future direction of the Consumer Data Right as it applies to open banking.

Write Access

In general, Mastercard believes that write access is a potential and natural evolution of a developed open banking environment. Write access has the potential to deliver greater competition, increased convenience, and improved efficiencies for consumers and industry alike. We focus our comments in this section on payment initiation. Our comments relating to data and digital identity that follow are broader. They extend also to those aspects of write access that Treasury describes as the possibility for a third party to change data about the consumer including applying for new products that would change the relationship of the financial institution and the consumer on a lasting basis.

Write access empowers the third party in the relationship between consumers and financial institutions to act in different ways than with read access. The standing or accreditation of that third party is critically important. The CDR construct is intended to provide a considered way to engage with this issue. However, given the increased risks associated with write access, we think there are specific issues to be addressed as moves to allow write access are considered.

- **Fraud, data security and wrongful use of data provided:** We note that the industry is still working through security and other issues relating to read access. We think that the approach should be sequential with these issues relating to read access being resolved before write access implementation moves ahead. Phased implementation and gradually expanding functionality will ensure all stakeholders have sufficient adoption time to address related technological challenges.

  A key point is stakeholder reassurance that the write access framework has adequate safeguards and protections for consumers in relation to fraud and data security and to minimize the risk of data breaches. As was recently demonstrated by the fraud issues associated with the COVID-19 related early withdrawal of superannuation benefits,

fraudsters will quickly exploit any system weakness.[1] In the case of write access, this is of particular concern for vulnerable consumer groups, all the more so if this goes to transactions for which dispute resolution mechanisms are not fully developed.

Further, if data is provided for a specific purpose related to the processing of a payment or is otherwise intended to change the relationship of the consumer and the relevant financial institution, it should not also be used so as to change the relationship of the consumer with the third party providing open banking services.

- **Dispute resolution:** Mastercard notes the Part 6 of the Consumer Data Rules outlines rules relating to dispute resolution. Given the potentially increased risks with write access (as outlined above) we believe that the Government must ensure that these rules are robust enough to deal with the points of difference between read and write access. Mastercard urges the Treasury to consult with industry and consumer stakeholders to ensure that the CDR dispute resolution mechanisms are enabled that are fit for purpose, in an environment with write access. We hope this will be in a way that balances the needs of participants and encourages uptake of services within the data sharing ecosystem. We note here that industry enabled solutions do have a potential role: we make this comment as an organisation that supports our network participants in resolving issues arising (e.g. via our chargeback mechanism) across our global network.

Protection of personal data

We recognize the efforts of the Treasury and other stakeholders involved in implementing the Consumer Data Right to address data privacy matters. We are supportive of that work. We think that write access as described by the Treasury raises specific issues which should be taken into consideration:

- Holding data that may be used to change a consumer's relationship with its financial institution including by way of initiating a transaction particularly if that includes consumer authentication credentials is powerful.

- We see several principles as important here:

    - Data responsibility: for Mastercard data responsibility dictates that personal information belongs to the individual, who controls how it is used and shared. Individuals should have knowledge of how their personal information is handled. An example of the way this relates specifically to payments is that, if a consumer has provided data to make a payment in a specific way, that data should not be used to make payments in a different way without an actual (rather than inferred) agreement about that payment. Otherwise there would be inconsistency with the customer knowing how their data is used.

    - Alignment with existing privacy and consumer protection regulations: ecosystem participants must demonstrably uphold best-in-class security and privacy practices. The point here goes beyond knowledge to the consumer's confidence and trust. Mastercard believes that confidence and trust must be at the centre of any data sharing ecosystem including where third parties are given greater scope to use data.

[1] https://www.afr.com/politics/federal/super-early-access-frozen-amid-afp-fraud-investigation-20200508-p54r1z

- Level playing field: existing or new participants should not be unintentionally preferred or barred and that the framework should enable both new players and incumbents to innovate and compete. Specific parties should not be put at a competitive disadvantage unless this is because they are unable to comply with the principles described above.

- Parity of treatment: a related point is that all actors within the chain between data origination and data (re-)use should accept the same standards, responsibilities and restrictions on use depending on the type and sensitivity of the data and the use case. For example, if a financial institution is limited in its use of transaction data to market services to a consumer, the same restriction should be placed on all relevant data holders.

Digital Identity and the Consumer Data Right

Mastercard believes that a strategy to combine CDR with digital identity platforms, could create the opportunity for significant consumer benefit in frictionless product switching, increased competition and to better serve the future CDR industries (Energy, Telecommunications).

Seamless product switching

When consumers apply for new financial products (bank accounts, credit cards, personal loans, mortgages) a crucial task for them is to prove their identity and relatedly to allow the financial institution (or Reporting Entity) to perform related KYC obligations.

Even in digital or online channels, up to 30%[2] of consumers are unable to present sufficient identity documentation, or be found on credit bureau data sources, so as to allow them to automatically be approved for a new financial product. Typically, these consumers must manually upload documentation, visit bank branches or post-office outlets to complete their verification, often leading to substantial consumer frustration.

The benefits brought by the Consumer Data Right for a consumer to digitally prove their income and expense data through bank transaction data will be undermined to the extent that consumers have no choice but to use manual and inefficient identity verification processes when they are attempting to switch products.

From a consumer's perspective, where their original identity verification result (or KYC status) could be shared from their existing Data holder to the Data Recipient, this would result in substantial productivity benefits for industry, greatly reduce friction in switching products and likely lead to higher satisfaction with outcomes flowing from the Consumer Data Right.

In late 2019, when amendments were proposed to the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019*[3], it was determined that the opportunity for financial institutions "relying on" the original identity verification would be:

[2] https://www.digitalid.com/business

[3] https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/ems/r6431_ems_02d35e3c-143d-4d83-8877-e31cf490ce8a%22

1. A reduction in the time to verify the identity of new customers of up to 66%;
2. A reduction in the cost to verify the identity of new customers of up to 80%; and
3. A total reduction in compliance costs and regulatory savings of $3.1 billion across 10 years for the financial services industry in Australia.

Indeed, a key recommendation of the 2017 Farrell "Review into Open banking"[4] was for value-added data to increase such identity verification inefficiencies:

"…granting customers the right to instruct their bank to share the result of an identity verification assessment performed on them could improve efficiencies in the system. A bank could simply affirm whether the customer is who they say they are without sharing the original data or data on the process by which that conclusion was reached. This approach would make it easier for customers to switch between providers by simplifying the process of sending copies of their personal documents and increase the efficiency with which competing providers are able to secure and on-board new customers. It would also enhance customer privacy and security, as obtaining access to the supporting documents provided by an individual as part of an identity verification is one of the most common methods of identity theft. Reducing the frequency with which customers are required to transfer such documentation will help to reduce that risk."

Mastercard believes the following actions should be taken to enhance the utility of the Consumer Data Right:

1. Add both "Date of Birth" and "KYC Status" as attributes that maybe supplied by Data holders in furtherance of a consumer exercising the CDR Data holder; and

2. At a policy level, for the ACCC and AUSTRAC to be involved with a specific view to providing guidance as to the appropriate treatment and considerations of such identity data derived from CDR.

Enabling future segments for the Consumer Data Right with Digital Identity platforms

Optimizing the CDR in new segments and industries (Open Telco, Open Energy) involves data holders being able to leverage the existing technology and identity verification assurance they have with their consumers.

Where this identity infrastructure is not in place, the ability for consumers to authenticate themselves towards their data holders and share high-quality and well verified identity data to data recipients is substantially compromised.

In the existing Open banking environment, such challenges are essentially solved through:

1. Consumers being strongly engaged with their data holders through a high penetration of their mobile apps/ internet banking site. Therefore:
    a. Consumers can easily receive a one time password through that app, or through a verified mobile number held by the bank.
    b. Consumers login regularly to such apps (daily/weekly) which allows them to notice fraud activity on their bank transaction data
2. Identity verification (KYC) being regulated in financial services means the consumer identity data held by data holders (and potentially shared with data recipients) to be of a relatively high quality.

[4] https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

For the Telecommunications and Energy industries:

- the usage of such 'apps' is far less common (particularly in Energy) and consumer engagement is lower. A consumer's primary relationship and engagement with their Telco or Energy retailer is either through an emailed or postal addressed bill, received monthly or quarterly; and
- the quality of the identity data is typically of lower quality, as the verification of customer onboarding data is largely unregulated and not required.

Digital Identity platforms offer organisations the ability to:

- remediate and verify customer data to higher standards to improve contactability e.g. by verifying email addresses that will deliver, and mobile numbers that are attributed to the individual customer;
- create customer journeys for onboarding and managing of personal data that is privacy centric and with consent driven interactions and
- offer strong authentication, for account modifications or usage, either through existing credentials or preferably through high-quality user biometrics which promotes the security of the customer's account.

Our recommendation for the evolution of CDR into Open Telco and Open Energy is that steps are taken to:

1. ensure that upcoming industry segments are encouraged to adopt tools and technology that provides their consumers with reliable, secure and safe ways to authenticate and share their data; and
2. promote requirements that identity data shared from data holders has been verified to a strong standard, and that secure methods are promoted for consumer authentication – particularly where those practices will largely not exist today.

Further discussion

Mastercard appreciates the opportunity to comment on the *Inquiry into Future Directions for the Consumer Data Right.* We would be pleased to meet with Treasury to discuss the contents of our submission further. If you would like to discuss our submission, or require additional information, Chris Siorokos, Director Public Policy, can be contacted on 02 9466 3720 or via email to chris.siorokos@mastercard.com.

Yours sincerely

Rich Wormald
Division President Australasia