9 September 2024

**By Email**
CDRRules@treasury.gov.au

The Treasury
Langton Crescent
PARKES ACT 2600

Dear Treasury,

RE: **CDR Rules – Consent and operational enhancement amendments**

Thank you for the opportunity to respond to the consultation regarding consent and operational enhancement amendments to the CDR Rules (the **Draft Rules**). Mastercard acknowledges the work completed by Treasury to date in producing the Draft Rules and supporting materials.

Mastercard is an unrestricted Accredited Data Recipient (**ADR**) and is actively involved in the CDR ecosystem. We recently supported FinTech Australia in the publication of the 4th edition of the Australian Open Banking Ecosystem Map and Report, and we are committed to supporting the growth of Open Banking in Australia.

**Consultation response – executive summary**
Mastercard considers that many of the proposed changes, particularly in the consent review section, are clear, sensible and straightforward changes that will be welcomed by the majority of CDR ecosystem participants as they are currently drafted.

However, we have provided some detailed feedback with respect to the following changes, which we believe merit further consideration or amendment by Treasury:

- **De-identification:** Mastercard does not support the proposal with regards to de-identification. We remain concerned that the adoption of a "deletion by default" approach to redundant data will severely impact the ability of ADRs to access de-identified data. This in turn will negatively affect the ecosystem and undermine some of the core objectives of the CDR regime. Requiring an explicit de-identification consent in all cases sets the bar too high for ADRs and is inconsistent with the requirements that apply to other forms of personal information. Ultimately, proceeding with the proposed change will most likely serve as a barrier to product development, innovation in the CDR and uptake. Instead, we recommend amending this proposal to include de-identification as a permitted use of CDR data, subject to the consumer not having exercised an opt-out mechanism.

- **Supporting third parties:** Mastercard does not support the proposal to require ADRs to include additional information regarding outsourced service providers in the consent flow. This change undermines many of the other consent review proposals by inserting unnecessary information and adding to the cognitive load of the consumer. In our view, inclusion of additional information about OSP arrangements in the consent flow does not

add any meaningful value, given it is already required to be included in the CDR receipt and the ADR's CDR Policy. We recommend that this proposal should not be adopted.

- **ADIs treating data as data holders:** Mastercard strongly supports the proposed change to this provision, which will better enable banks to leverage the CDR in the manner that was originally intended. However, we feel the inclusion of the condition requiring ADIs to inform the consumer of the privacy treatment that will apply (and the resulting implications, for example the interaction between the CDR privacy safeguards and the APPs) adds unnecessary technical complexity to the consent flow. We recommend that this wording be removed.

Please see our detailed responses to the specific consultation proposals in **Annexure 1**.

**Further discussion**

We would be pleased to meet with Treasury to further discuss the contents of our submission. If this would be helpful or if you require additional information, please contact Mitch Thorp, Senior Counsel, Open Banking at mitch.thorp@mastercard.com.

Yours sincerely,

Richard Wormald
**Division President**
**Australasia**

**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 providing a wide range of payment solutions and services using our family of well-known and trusted brands, including Mastercard®, Maestro® and Cirrus®. We operate a multi-rail payments network that provides choice and flexibility for consumers and merchants.

At Mastercard, our key strategic priorities are:

1. **Expand in payments**. We continue to focus on expanding upon our core payments network to enable payment flows for consumers, businesses, governments and others, providing them with choice and flexibility to transact across multiple payment rails.

2. **Extend our services**. Our services drive value for our customers and the broader payments ecosystem. We continue to do that as well as diversify our business, by extending our services, which include cyber and intelligence solutions, insights and analytics, test and learn, consulting, managed services, loyalty, processing and payment gateway solutions for e-commerce merchants.

3. **Embrace new network opportunities**. We are building and managing new adjacent network capabilities to power commerce, creating new opportunities to develop and embed services.

Through our third strategic priority, we are focused on opportunities to enable Open Banking with everyday consumers. We are inspired by the vision of empowering consumers with control of their data so that they have more choice, at a greater convenience and with trust in the ecosystem, to switch products, make better decisions and ultimately benefit more tangibly from the digital revolution. We currently do this by providing our Fintech and financial institution partners with Open Banking products and services that enable them to reliably access, transmit and manage consumer data to meaningfully enhance their customer experience and win in a rapidly changing market at a global scale.

## Annexure 1 – Responses to Design Paper consultation questions

| No. | Proposed amendments | Mastercard Response |
|---|---|---|
| **Consent Review** | | |
| **1.1** | ***Allowing a data recipient to bundle CDR consents, so that consumers can give multiple consents with a single action*** | Mastercard **strongly supports** this proposal, subject to our comments below.<br><br>This is a sensible change which will simplify the consent flow by reducing the number of actions a consumer is required to take, without detracting from the need to ensure consumers are providing informed consent. We agree with the proposal to link the ability to bundle consents (including disclosure consents) with the data minimisation principle (**DMP**), which will ensure that only those consents that are "reasonably needed" for the provision of the service can be bundled together.<br><br>We note the recommendation in the Privacy Impact Assessment (**PIA**) for Treasury to consider whether excluding disclosure consents from bundling would provide better transparency to consumers. In our view, bundling disclosure consents (where they are reasonably needed to provide the service) will not affect the ability of consumers to be sufficiently informed about the parties with whom CDR data may be shared. This is because, in the vast majority of use cases involving a disclosure consent, the disclosure *is the service* that the consumer is asking the ADR to provide. The consumer will already be aware of the identity of the disclosure recipient and the purpose of the disclosure – indeed in many cases the consent flow will have been triggered from the disclosure recipient's environment (for example where a trusted advisor or business consumer disclosure consent flow is triggered from within an accountancy platform). As such, our strong view is that disclosure consents ought to be able to be bundled where they are reasonably needed to provide the service, as currently proposed in the Draft Rules.<br><br>We also note the alternate recommendation in the PIA for Treasury to consider a "right to object to bundled consents", which could trigger an obligation for the accredited person to provide further explanation about why bundled consents are essential to provide the product or service. Accredited persons are already required to provide information about how the consents being sought comply with the DMP[1] and we consider that a "right to object" would effectively duplicate this requirement, providing no material benefit to consumers. Our strong view is that this recommendation should not be adopted as it would add undue complexity – and as the 2022 Statutory Review noted, "*Extensive consent requirements can perversely inhibit a consumer's understanding of what they are consenting to, and complicated consent processes can also deter consumers from engaging with CDR products and services*"[2]. We also consider that inserting this type of functionality into the consent flow would be difficult and costly to implement. |
| **1.2** | ***Allowing a data recipient to pre-select the elements of an individual consent that would be*** | Mastercard **strongly supports** this proposal, subject to our comments below.<br><br>As with the proposal above, this change represents a sensible way to reduce fatigue in the consent journey. The Consultation Paper also rightly identifies the false choice that can currently be presented to consumers, where a service cannot be provided without specific selections being made. |

[1] See paragraphs 4.11(3)(c) and 4.20E(3)(f) of the Draft Rules.
[2] *Statutory Review of the Consumer Data Right – Final Report*, 29 September 2022, page 44.

| | | |
|---|---|---|
| | ***reasonably necessary for the data recipient to provide the good or service*** | While we agree with the proposition that only those consent elements that are reasonably needed to provide the service can be pre-selected, we consider that the wording in paragraph 4.11(3)(caa) of the Draft Rules is unnecessary and should be removed, because it effectively duplicates the requirement in paragraph 4.11(3)(c)[3]. We also assume the reference to pre-selection will mean that an ADR will not need to provide for any level of user interaction (i.e. no ability for these elements to be deselected or unticked), given the fact those elements will have been deemed by the ADR as reasonably needed in order to provide the service.<br><br>In addition, the comments we made above in relation to the PIA recommendation to consider a "right to object" for bundling apply equally to this proposal. This functionality will add no material benefit for consumers, but will significantly increase implementation cost and complexity for accredited persons. The focus of these changes must be simplifying the consent flow – adding duplicative and unnecessary language such as that envisaged in this PIA recommendation would run counter to the core objective Treasury is seeking to achieve. |
| **1.3** | ***Simplifying the information a data recipient is required to provide to the consumer at the time of consent*** | Mastercard **strongly supports** this proposal.<br><br>This is a sensible measure that reduces the amount of information that needs to be provided to the consumer at the time they provide consent. |
| **1.4** | ***Allowing a data recipient to consolidate the delivery of 90-day notifications to reduce consumer notification fatigue*** | Mastercard **supports** this proposal.<br><br>This is a sensible measure to mitigate the "notification fatigue" that consumers can experience. We agree with the proposal to move the information requirements to the Standards. |
| **1.5** | ***Simplifying obligations in relation to CDR receipts*** | Mastercard **supports** this proposal.<br><br>We agree this change will simplify the content of CDR receipts and improve consistency. We agree this matter is better addressed in the Standards – and as a general principle we would advocate for further CX matters to be moved from the Rules to the Standards in future, including for example consent flow information requirements. |
| **1.6** | ***Requiring a data recipient to provide consumers information about all supporting parties who may access the consumer's data at the time a*** | Mastercard **strongly disagrees** with this proposal, specifically as it pertains to outsourced service providers (**OSPs**).<br><br>Requiring additional information about each direct and indirect OSP to be included within the consent flow:<br>1. Does not add meaningful value to the consumer, particularly considering that the current Rules already require an accredited person to include a statement of the fact that data will be disclosed to an OSP in the consent flow, with further details of the identity of the OSP and their use of the data included within the CDR Policy and CDR receipts. Individual consumers who wish to seek out this level of information will naturally refer those artefacts; for all other consumers, the inclusion in the consent flow of a statement that OSPs will receive their data and a signpost to the CDR Policy is sufficient.<br>2. Directly undermines many of the other beneficial changes proposed in the Draft Rules, which have been designed to simplify the consent flow. Including additional information about each OSP will complicate the consent flow and unnecessarily add to the |

[3] The same comments apply to the corresponding provisions for CDR Representatives in paragraphs 4.20E(3)(f) and (fa) of the Draft Rules.

| | | |
|---|---|---|
| | ***consumer gives a consent*** | cognitive load of the consumer. The specific details of each OSP arrangement are less critical for the purposes of the consent flow, and are better provided in the CDR Policy, which can be updated dynamically over the life of the consent as OSP arrangements change. We think the position on this point is analogous to the position with respect to inclusion of information about withdrawal of consent being better suited to the CDR receipt than the consent flow.<br><br>3. Increases the compliance burden for ADRs, particularly given some 89% of all data recipients use a third-party intermediary (such as an OSP) of some kind.[4] Requiring the specific details of each OSP arrangement to be surfaced in flow will add implementation cost and complexity, given the flow would need to be updated each time there is a change to those arrangements. There would be a materially adverse impact on those ADRs who, by virtue of the size/scale or the variety of use cases they support, have appointed multiple direct / indirect OSPs.<br><br>This change would also represent a further instance where the CDR Rules would go beyond what is ordinarily required to be disclosed to a consumer under the Privacy Act in equivalent circumstances. Consumers are very familiar with the concept that third parties may assist the business they are dealing with in the collection and management of data. Where this occurs under the Privacy Act, businesses generally are *not* required to disclose the specific identity of the supporting third parties that will receive personal information – instead they are required to refer only to the "types of entities" to whom data may be disclosed.<br><br>**Recommendations**<br>Mastercard's strong recommendation is to **not proceed with this change**. By including a requirement to provide notification of the use of OSPs in the consent flow, with a signpost to the CDR Policy where further information can be found, the current Rules already strike the right balance between keeping the consumer informed of the parties who access their data and simplifying the consent experience.<br><br>If this change is to proceed, Mastercard would recommend that additional information in the consent flow be required for direct OSPs only. This would go some way towards mitigating the effect of the negative consequences of this change described above. In addition, Mastercard's strong view is that if this change is to proceed, **it must be subject to an implementation period**. The Draft Rules currently appear to provide that this change would become effective immediately, but this will cause significant issues for ADRs who would effectively be required to update their consent flows overnight. As with all other changes that impose compliance requirements on participants, it is essential that ADRs are afforded time to implement. Mastercard would recommend that 6 months would a suitable implementation period for this change. |
| **1.7** | ***Requiring data recipients to delete redundant CDR data unless a consumer has given a de-identification consent*** | Mastercard **strongly disagrees** with this proposal.<br><br>We acknowledge the perceived complexity in the current Rules related to de-identification and treatment of redundant CDR data. However, the proposed change, which would require an explicit de-identification consent to be obtained in all cases before an ADR can access and use de-identified data, will give rise to a number of unintended consequences that will detrimentally impact the ecosystem as a whole. We would also welcome further clarity from Treasury on the legal basis for this change, given the primary legislation appears to clearly contemplate a CDR entity taking steps to either delete OR de-identify redundant data.[5]<br><br>Instead, we are advocating for an alternative change to the existing Rules that would remove any overlapping requirements while still supporting sensible access to de-identified data and a consumer's right to elect for their data not to be de-identified.<br><br>Our key concerns with the proposal in the Draft Rules are as follows: |

[4] Fintech Australia | Mastercard, *Australian Open Banking Ecosystem Map & Report*, 4th Edition, published May 2024.

[5] See subsection 56EO(2) of the *Competition and Consumer Act 2010* (Cth).

| | | |
|---|---|---|
| | | 1. Deviates from the original intent of the Rules by inhibiting product development and innovation<br><br>De-identified data is widely used in the financial services industry to develop, enhance, test and improve business products and services. In order for products and services that leverage data aggregation and categorisation engines to remain accurate, reliable and up-to-date, large data sets of current consumer data are required both to create initial models,[6] and also to refine these models as time goes on.[7] Almost all of the key CDR use cases of lending, PFM, accounting and payments will need to leverage models of these nature in order to allow consumers to unlock the value of their data.<br><br>We are concerned that the likely consequence of the change proposed by the Draft Rules is that the rate of consumers who will permit their data to be de-identified will be materially reduced.[8] We expect there will be a marked drop in provision of consent where consumers are required to provide explicit consent, as opposed to circumstances where an opt-out is always available[9] (as is the case with redundant CDR data de-identification currently).<br><br>Restricting the ability of ADRs to access de-identified data for research, product development and modelling purposes will stifle innovation. This directly undermines one of the fundamental objectives of the CDR, as expressed in the Explanatory Statement accompanying the original version of the Rules: "The CDR is designed to promote competition and give consumers more control over their data which will *facilitate innovative new products and services for consumers*".[10] It will also increase the risk that inaccurate, biased or unreliable models are developed – because where fewer consumers provide their data, the more likely it is that the data used to create a model lacks quality, accuracy and fails to be representative of wider society.[11].<br><br>Given the current levels of uptake of the CDR in Australia, it is even more important that policy settings are designed in way that fosters safe access to data for meaningful and accurate product development and innovation.<br><br>2. Exaggerates the risks to consumers of use of their de-identified data<br><br>Many of the arguments in favour of the "deletion by default" proposal are grounded in only one of the original CDR policy objectives of providing consumers with more control over their data. Indeed, the PIA characterises this proposal as a "privacy positive" change which "preserves consumer autonomy" over how their data is treated. In our view, this position exaggerates the risks posed to consumers by use |

[6] "The exact amount of data required to train a foundation model is unclear. Some argue data is the single biggest issue for developing them. For example, after building of a model of the value of generative AI, (Hunt et al., 2023[21]) estimates that around 70-75% of model value is from data." See page 19, OECD (2024), "Artificial intelligence, data and competition", *OECD Artificial Intelligence Papers*, No. 18, OECD Publishing, Paris, https://doi.org/10.1787/e7e88884-en.

[7] "In general, fine-tuning and refinement requires many of the same inputs as foundation models, albeit with some key differences. Building on a general model, the volume of data and scale of compute required will likely be lower. However, these could still be significant…." See page 22 , OECD (2024), "Artificial intelligence, data and competition", *OECD Artificial Intelligence Papers*, No. 18, OECD Publishing, Paris, https://doi.org/10.1787/e7e88884-en.

[8] Although there is a lack of quantitative research comparing the attitudes of consumers in respect of their behaviour in cases of opt in vs opt out consent in a banking context, research in the health sector has shown that the rates at which consumers consented to their data being used for research purposes was more than 10% higher where consent was opt-in by default (with an ability to opt-out at any time) as opposed to where explicit consent was required – see Köngeter A, Schickhardt C, Jungkunz M, Bergbold S, Mehlis K, Winkler EC, *Patients' Willingness to Provide Their Clinical Data for Research Purposes and Acceptance of Different Consent Models: Findings From a Representative Survey of Patients With Cancer*, J Med Internet Res 2022;24(8):e37665, accessible at https://www.jmir.org/2022/8/e37665/.

[9] We note the findings from the Digital Platforms Enquiry that support the argument that when consumers are provided with an opportunity to "opt out", they do take advantage of this ability: "Australian digital platforms users have indicated that they will actually opt-out of sharing information when offered the opportunity. 57 per cent of digital platforms users surveyed in the ACCC consumer survey indicated that they select opt outs when they are available. The CPRC survey also found that 89 per cent of Australians surveyed indicated that they select opt-outs when they were available", Paragraph 7.7.1, *Digital Platforms Inquiry* – Final Report, July 2019, accessible at https://www.accc.gov.au/about-us/publications/digital-platforms-inquiry-final-report.

[10] Explanatory Statement – *Competition and Consumer (Consumer Data Right) Rules 2020*, accessible at https://www.accc.gov.au/system/files/CDR%20Rules%20Explanatory%20Statement%20-%206%20February%202020.pdf?ref=0&download=y.

[11] "Artificial intelligence, data and competition", *OECD Artificial Intelligence Papers*, No. 18, OECD Publishing, Paris, accessible at https://doi.org/10.1787/e7e88884-en.

| | | |
|---|---|---|
| | | of their de-identified data and ignores the counterfactual position that without access to de-identified data, ADRs cannot deliver innovative products and services to consumers in the first place – another of the core objectives of the CDR regime.<br><br>The Rules already adequately protect consumers from the potential for misuse of their de-identified data. De-identification of CDR data is required to be undertaken as a multi-step process and to a high standard that is explained in the De-identification Decision Making Framework.[12] Research has shown[13] that where de-identification of data is done in this way using proper techniques, the risk of re-identification and subsequent harm to the consumer is minimal, as re-identification is a complex, time consuming and costly process.[14]<br><br>We also note that de-identification of personal information outside of the CDR regime does not require a consumer's explicit consent today, and that this position appears set to continue even following the forthcoming reforms of the Privacy Act. The Final Report of the Privacy Act Review and list of Recommendations was released in December 2022, and while it included some recommendations dealing with the definition of de-identification and how de-identified personal information was to be handled and protected from misuse, it did not recommend that de-identification of personal information be restricted to circumstances where consumers had given explicit consent. Given this position, and noting the extensive review process that informed these recommendations (comprising a number of consultations and reviews over several years), it would be incongruous and unnecessary for the CDR to impose a higher standard than will apply to personal information under the reformed Privacy Act.<br><br>3. <u>Out of step with global laws that promote competition and innovation</u><br><br>We reviewed the data protection laws applicable in jurisdictions outside of Australia and did not find a comparable law that permitted data recipients to de-identify consumer data solely in circumstances where the explicit consent of the consumer has been obtained.<br><br>Some examples of comparable regimes are below:<br><br>a. <u>European Union</u>: the GDPR considers that the act of de-identification of data is a type of processing for which there needs to be a legal ground. In accordance with Article 6 of the GDPR (Lawfulness of Processing), consent is one of these grounds, however there are also five other legal grounds that can be used as a legal basis for de-identification, including 'legitimate interest', 'necessary for the performance of a contract' and "compliance with a legal obligation".<br><br>b. <u>Singapore</u>: the government developed a financial data exchange service called the Singapore Financial Data Exchange (SGFinDex)[15] that enables Singapore residents to use their national identity numbers to retrieve and share their personal financial information with participating financial institutions, including banks and insurers, to enable individual financial planning. The SGFinDex is similar to the CDR in the sense that it has established an authentication and consent framework that is accessed through a centralised gateway and data sharing is based on common data and API standards. Consumers must provide explicit consent to retrieve and share their data with business that are parties to the SGFinDex, however this consent is contained in standard terms and conditions which consumers agree to as part of the data exchange, and which includes permission for recipients of the data to use it for "developing, improving or enhancing new or existing services or functionalities", without a requirement to de-identify it. |

[12] Accessible at https://www.csiro.au/en/research/technology-space/cyber/A-framework-for-data-de-identification.

[13] K. El Emam, E. Jonker, L. Arbuckle, and B. Malin, "A Systematic Review of Re-Identification Attacks on Health Data," PLoS ONE, vol. 6, no. 12, p. e28071, Dec. 2011, as quoted in the article "De-identification: A Critical Debate" by El Emam, Khaled and Arbuckle, Luk, accessible at https://fpf.org/blog/de-identification-a-critical-debate/.

[14] Ibid.

[15] More information available at https://www.mas.gov.sg/development/fintech/sgfindex.

c. United States: the United States currently does not a federal open banking law, although the framework for this was established under the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. Earlier this year the Consumer Financial Protection Bureau (**CFPB**) released a Proposed Rule on personal financial data rights (**US Draft Rule**) which would be similar in nature to the Australian CDR Rules. The US Draft Rule required third parties to limit their collection, use, and retention of covered data to what was "reasonably necessary" to provide a consumer's requested product or service, equivalent to the data minimisation requirements of the CDR. Although not expressly provided in the US Draft Rule, these data minimisation requirements would likely permit use of de-identified consumer data to the extent it was "reasonably necessary to provide a requested product or service to a consumer", which appears similar to the GDPR standard explained above.

In the jurisdictions outlined above, businesses that collect consumer data as part of their product or service are (in most cases) able to use this data in *identified* form to ensure quality control, accuracy and reliability of their product or service, without obtaining explicit consent from the relevant consumers. While the Australian CDR Rules currently do not permit providers of CDR products/services to use identified CDR data in this way, they do permit de-identification of redundant CDR data without explicit consent (subject to opt-out). Clearly, the original policymakers were comfortable with the idea of CDR data being able to be de-identified where consumers did not actively have to "opt in" to this process, and in a global environment where similar jurisdictions permit use of *identified* financial data for internal product development and quality control reasons, we believe that requiring a blanket "deletion by default" change would leave Australia significantly out of step with its global peers.

Positioning Australia as the outlier from a global perspective will make it more difficult for local businesses to innovate and compete. It also reduces the attractiveness of Australia as a market for global corporations, particularly where data use restrictions impede interoperability of their global platforms. [16]As the OAIC noted in its submission to the Privacy Act review: "*An overarching theme of this review and Australia's shift to a digital economy is to ensure global interoperability – put simply, making sure our laws continue to connect around the world, so our data is protected wherever it flows and the burden on businesses operating globally is reduced*."[17]

4. Risks further reducing the ability of industry participants who do not have access to de-identifiable consumer transaction data to compete with those who do

If the proposed changes in the Draft Rules are made, those ADRs who already have access to large volumes of consumer transaction data acquired outside of the CDR regime (such as authorised deposit-taking institutions (**ADIs**)) will hold an unfair advantage over those ADRs who do not. As explained above, the Privacy Act currently does not (and likely will not in future) require an explicit de-identification consent to be obtained from consumers in order for personal information to be de-identified and used. This means market participants such as ADIs will be able to continue de-identifying and using the enormous transaction datasets they have acquired outside of the CDR for purposes including product development, without needing explicit consent. In contrast, ADRs who rely on access to data via the CDR would be unfairly impacted by this change, as they would be required to obtain an explicit de-identification consent.

Given our comments above about the likely opt-in rates of an explicit de-identification consent, the only practical option available to a smaller ADR who needs de-identified data for product development will likely be to acquire it through other means, e.g. by screen-scraping data and de-identifying it, or purchasing a de-identified dataset from a third party. The rules and requirements pertaining to de-identification must be consistently applied to all datasets, irrespective of how that data was collected.

**Recommendation**

[16] Falk, Angeline, Submission by the Office of the Australian Information Commissioner, Privacy Act Review – Discussion Paper, 23 December 2021, page 11, accessible at https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-discussion-paper.
[17] Ibid.

| | | |
|---|---|---|
| | | We offer the following alternative options which in our view would address the issues with the current Rules, whilst still preserving the ability of ADRs to access and use de-identified data to support innovation – which in turn will benefit Australian consumers:<br><br>Option 1 (preferred approach): We propose that the Draft Rules should instead provide a single mechanism that permits ADRs to de-identify a CDR consumer's data, unless the consumer has opted out of this prior to their CDR data becoming redundant. This approach would still provide consumers with the choice both at the time a consent is given, and during the lifetime of their consent, to decide if they did not want their data de-identified. We consider that this would strike the best balance between promoting the autonomy of the consumer with respect to the processing of their data, and supporting the needs of the CDR ecosystem, which intrinsically requires access to de-identified data.<br><br>Option 2 (first alternative approach): make the change as proposed by the Draft Rules, but allow de-identification consents to be bundled with other consents, where they are "reasonably needed" to provide the service. As explained above, de-identified data will often be reasonably needed in order for the ADR to provide the service – for example in the context of a PFM use case which involves data categorisation. In this situation, an ADR should be permitted to bundle a de-identification consent with the relevant collection and use consents. In contrast, bundling of a de-identification would not be permitted in use cases where de-identification is not reasonably needed to provide the service, which for example could include an account verification or balance check use case.<br><br>Option 3 (second alternative approach): do not make the proposed change and instead leave the Rules as they are today. While retaining the status quo would mean some of the perceived complexity in the Rules is retained, we think this outcome is clearly preferable to the outcome that would arise under the Draft Rules, and would afford Treasury and the DSB more time to consider the impact of requiring an explicit de-identification consent on the ecosystem as a whole. |
| **Operational Enhancements** | | |
| **2.1** | ***Nominated representatives*** | Mastercard **supports** this proposal.<br><br>Mastercard agrees that the process for appointing nominated representatives is a clear barrier to business participation in the CDR. In our view, the proposed obligation on data holders to offer a service which is simple and straightforward to use, and prominently displayed and readily accessible, should be uncontroversial. This is a sensible, principle-based amendment that should result in an improvement in the processes that CDR consumers are required to complete.<br><br>Similarly, Mastercard agrees with the proposed requirement for data holders to offer an electronic process for allowing online account administrators to be appointed as nominated representatives, for partnership and non-individual CDR consumers. But we also acknowledge the practical concerns raised by data holders on this issue, and the myriad potential complexities that can arise with respect to account authorisations, roles and permission structures, particularly in the context of large corporate and institutional banking customers.<br><br>To that end, and to the extent the current proposals are ultimately deemed unsuitable or too difficult to implement, Mastercard would urge Treasury to explore options to remove the nominated representative concept altogether, particularly with respect to small and medium sized enterprises. In other jurisdictions (for example the EU and UK), there is no equivalent requirement for businesses to have to appoint nominated individuals who can consent to data sharing. Instead, any user with online access to a particular account can consent to share information pertaining to that account with a regulated third party. This position recognises the fact that the same user could equally provide their credentials to a screen scraper, or download account information/statements and provide them directly to a third party, without needing any further authorisation from the account holder. |

| | | |
|---|---|---|
| | | Removing the concept of a nominated representative would remove the complexity that is caused by the interaction of the nominated representative provisions with data holders' existing account authorisation and permission structures. The position reached in relation to joint-accounts is instructive here – and while we appreciate there is a distinction between joint account holders and users of an account (who are not themselves account owners), an "on by default" position will inherently be much simpler to use and therefore see much greater uptake than an "opt-in" model. |
| **2.2** | ***Expanding the circumstances in which accredited ADIs can hold CDR data as a data holder*** | Mastercard **strongly supports** this proposal.<br><br>The current rule allowing ADIs to treat CDR data as a data holder is undermined by its narrow scope and the overly onerous requirement to obtain the explicit agreement of the CDR consumer. The proposed change addresses both of these issues and we welcome its inclusion in the Draft Rules.<br><br>In our view, the utility of this provision could be further enhanced by removing the obligations on ADIs to:<br>• notify CDR consumers that data will be held as a data holder rather than as a data recipient; and<br>• inform CDR consumers of the privacy safeguards that will apply and the manner in which the ADI proposes to hold the data.<br>The language an ADI will be required to include in the consent flow in order to satisfy these requirements is likely to be technically complex and not easily understood by the ordinary CDR consumer. This will add friction to the journey and undermine many of the other changes proposed by the Draft Rules. CDR consumers understand and expect that when they are giving consent to an ADI to collect their data, that ADI will hold their data in accordance with their usual practices and the requirements of Australian privacy law – it ought to be sufficient for this to be confirmed in the consent flow, without the ADI needing to delve into the complexities of which rules apply to data holders vs data recipients and the interaction between the CDR privacy safeguards and the Australian Privacy Principles.<br><br>Mastercard would also support thoughtful future expansion of this provision to include other classes of ADRs who routinely hold and manage customer banking and transaction data and who are subject to other regulatory frameworks. This could potentially include, for example, Australian Financial Services Licensees or Australian Credit Licensees. |
| **Additional item** | | |
| **3.1** | ***Definition of "CDR business consumer"*** | Mastercard wishes to raise the following additional item for consideration by Treasury.<br><br>The current Rules state that a CDR consumer is taken to be a CDR business consumer in relation to a consumer data request to be made by an accredited person if the accredited person has taken reasonable steps to confirm that:<br>(a) the CDR consumer is not an individual; or<br>(b) the CDR consumer has an active ABN.[18]<br>Under this definition, sole traders who do not have an active ABN cannot be treated as CDR business consumers (noting that a sole trader, as a natural person, is an individual). This was confirmed by recent regulatory guidance published by the ACCC.[19]<br><br>Our experience has been that a significant percentage of sole traders do not hold an ABN, for example because they are trading at an early stage or at a very small scale (e.g. under the GST turnover threshold of $75,000). The effect of the current definition of CDR business |

[18] See subrule 1.10A(9) of the CDR Rules.
[19] See section 2.1 of the CDR business consumers fact sheet, published by the ACCC on 8 July 2024.

| | | |
|---|---|---|
| | | consumer is that those sole traders are unable to leverage the 2023 Rule changes that were designed to boost business uptake, including the ability to give a business consumer disclosure consent.<br><br>The Explanatory Statement accompanying those changes referenced the need for businesses to be able to share their CDR data with specified third-party recipients including bookkeepers, consultants and software providers. By excluding the ability of sole traders who do not hold an ABN to share their CDR data in these scenarios, the current drafting fails to give effect to the policy intention and acts as a significant barrier to small business uptake of the CDR.<br><br>Mastercard would therefore recommend Treasury consider amendments to the current subrule 1.10A(9) that would allow sole traders without an ABN to be treated as CDR business consumers. |