10 May 2019

Submitted to the ACCC via online portal

Dear ACCC,

Submissions on the Competition & Consumer (Consumer Data) Rules 2019

As always, we appreciate the opportunity to share our feedback and thoughts on the Competition & Consumer (Consumer Data) Rules 2019 – Exposure Draft. American Express remains fully supportive of Open Banking in Australia and we provide these submissions with a genuine desire to see the Consumer Data Right succeed.

American Express remains concerned about the level of prescription, complication and restriction in the CDR Rules. We believe that these elements will lead to sub-optimal user journeys, low usability and a lack of investment in products and services using CDR Data (likely with a proliferation in screen-scraping services). We think this would be regrettable.

American Express is disappointed that reciprocity has been left out of the Exposure Draft. We appreciate the ACCC's previously stated concerns about the complexity of reciprocity – but we think that its application to non-ADI product providers is relatively straightforward. We believe that allowing non-ADI providers to participate on a voluntary basis from the outset will give Open Banking a better chance at early success. More importantly though, we think the failure to allow non-ADI product issuers the right to participate as a Data Holder, raises competition issues.

American Express Australia makes the following submissions:

1. **Reciprocity & Equivalent Data**

   The concept of 'equivalent data' has been a constant since Treasury's first consultations on Open Banking and it has had broad support throughout the process. Recommendation 3.9 of Treasury's Open Banking report recommended that data recipients should be subject to an obligation to share any data 'that is the equivalent of transaction data' upon request by data subjects.

   We note the ACCC's observation that 'equivalent data' raises complex issues. However, we do not think this is the case for non-ADI issuers of products that are already within scope of CDR (i.e. mortgages, credit cards, charge cards). For example, 'equivalent data' in relation to non-ADI credit card issuers is a relatively straight forward concept; the data set held by American Express in respect of its credit cards is essentially identical to that by ADI credit card issuers.

Whilst the ACCC may be reluctant to impose a mandatory requirement on all holders of 'equivalent data', which we understand, there is no reason why the ACCC should not permit non-ADI issuers of products to participate on a voluntary basis under the first iteration of the CDR Rules.

We note that under Schedule 2, Rule 4.2, the ACCC already contemplates the voluntary participation of ADIs in the CDR on an early basis. We see no reason why this privilege should be limited to ADIs.

The absence of a right to participate for non-ADI product issuers as a Data Holder, means that customers of non-ADI product issuers will be unable to share data with ADRs in the CDR environment. In order to avail its customers of such data access rights, non-ADI issuers would either need to allow their sites to be screen-scraped or negotiate bilateral agreements with ADRs on a 'case by case' basis to allow data to be made available through APIs. Consumers will be excluded from the protections afforded under the CDR Rules and will not have access to dispute bodies. That outcome is not desirable for consumers and certainly not desirable for non-ADI product issuers who want to be part of Open Banking.

We also firmly believe that this scenario creates a competitive imbalance. ADIs will be in a position to offer full Open Banking data sharing access within a secure and regulated system – whereas non-ADI issuers will be forced to fend for themselves. Once Open Banking proliferates, data access will become a baseline expectation of customers and one that non-ADI issuers will be eager to meet for its customers.

We think voluntary participation for non-ADI issuers on an equivalency basis can be achieved simply and easily through the creation of a new rule that mirrors Schedule 2, Rule 4.2. The new Rule could:

- Create a new CDR participant: a 'Voluntarily Participating Data Holder'.
- Stipulate that a 'Voluntarily Participating Data Holder' is deemed a 'Data Holder' for the purposes of the CDR Rules in respect of Equivalent Data that it voluntarily shares in accordance with the CDR Rules.
- Define 'Equivalent Data' simply as data which is 'the same or substantially similar to Customer Data, Account Data, Transaction Data or Product Specific Data'
- Provide that 'an accredited person that issues a Product and holds Equivalent Data may notify the Commission that is seeking to participate as a Voluntarily Participating Data Holder'.

The benefit of approaching this in a voluntary way is that parties who wish to participate will not be excluded from the benefits of CDR and the ACCC will not be in a position to mandate any data sharing without further consultation with impacted parties. The ACCC would then have time to further consider the concept of 'equivalency', and whether or not to mandate it, as part of future iterations of the CDR Rules.

2. Requirement to have Contract for Goods and Services:

The consensual basis of CDR already provides the basis for a contract between a CDR Customer and an Accredited Data Recipient. The data subject agrees to provide specific data sets for specific purposes which are notified to the data subject. A requirement to have a documented contract seems unnecessary, unworkable in certain scenarios and achieves little except more documentation for consumers to read.

In certain circumstances, the existence of a contract or applicable terms and conditions will make sense – for example, an ADR that provides a PFM service will necessarily have terms of use governing that Service.

However, in other instances, a CDR Contract makes little sense. For example, an ADR that uses data on a 'one-off' basis in relation to a credit card application. The applicant may end up in a contractual relationship with the ADR if approved, but if declined, there will be no resulting contract. The operation of R4.3 (1) means that the ADR would need to have some kind of contract in place to govern the card application before starting the process?

The requirement is also unnecessarily prescriptive. The definition of CDR Contract at R1.8 (3)(d)(iii) extends to matters of fees, pricing and termination rights. The ability to withdraw consent at any point during a contract term without any financial consequence will affect how products are structured and priced, likely leading to higher prices for consumers. Product providers should have flexibility to determine pricing and fee structures.

We submit that the rules should not mandate a formal contract requirement and should not prescribe the contents of a contract.

The sharing of data is already a long and overly complicated process under the CDR Rules, requiring 5 steps before data can be shared: Contract/Consent/Request/Authorisation/Data sharing; we think many of these steps are unnecessary and should be rationalised, beginning with the first step of requiring the parties to enter into a CDR Contract.

3. Refusing Access under R4.7 (2).

We fully support the right of a Data Holder to refuse data access in circumstances where there is a risk of harm, however there needs to be strong sanction for its misuse. If not controlled properly, this could be used as a way for Data Holders to subvert the intent of CDR. 4.7(2) should require the Data Holder to provide evidence to demonstrate the reasonableness of its belief that sharing would cause harm.

4. 90 Day Notification Requirement (R4.14)

We believe the number of communication touch points with consumers is excessive under the CDR Rules. In principle, we agree that customer's decisions about their data should be determined by active action and not inertia – however, balance is required.

As we have submitted previously, sending consumer notices every 90 days will likely prove a source of annoyance for customers. Particularly for consumers who are actively engaged with their CDR product or service.

Based on our experiences and much of the research identified in the ACCC's previous reports, customers do not respond or act upon these types of disclosures or notices. They therefore serve little purpose.

The number and frequency of notices to customers seems to implicitly suggest that consumers should not be giving ongoing consent or that CDR is so risky and dangerous, they should be re-thinking their preferences quarterly? That seems contrary to the objective of CDR which is to allow them access to data securely and with confidence.

As a minimum, there should be an option for a consumer to turn off these notifications (at the time of enrolment) in recognition that many consumers will find them unnecessary and annoying. Customers should have flexibility to make these choices for themselves (i.e. 'remind me in 3 months, 6 months, 2 years').

Given the current direction of the CDR Standards, these notifications will be sent by email. We have strong reservations about mandating email as a channel. We think email communications (over more seamless inApp or push notifications) will be a significant customer dissatisfier and lead to a very 'Spammy' experience. Further, the number of emails from ADRs and Data Holders will increase phishing risks given that consumers will struggle to understand what is and what is not a legitimate communication given the sheer volume. Bombarding customers with email notifications is almost certainly not the path to success for the CDR.

5. 12 Month Expiry & Re-Soliciting Consent R4.12(c)

A 12 month expiry is a helpful safeguard in situations where consumers have taken a 'set and forget' approach to their data and have ceased to engage with their underlying CDR product or service. However, in circumstances where a data subject continues to actively use the product or service (for example, on a daily, weekly or monthly basis), we think the automatic expiring of consent makes little sense. Again, it is likely to simply be a point of frustration and annoyance for customers.

Highly engaged customers will expect to be able to continue to access their CDR product or service without interruption in those circumstances. We think R4.12 should be updated to provide for such an exemption.

Consumers should also be given an opportunity to agree to a longer consent period than 12 months, recognising that some consumers are genuinely comfortable to provide enduring consent – subject to a cancellation right. If CDR is about giving consumers choice and control, that should extend to matters of consent duration.

Renewing Consent

It is unclear in the Rules what the process is for re-soliciting consent when it expires under R4.12 (1)(c)? We do not think customers will appreciate being forced to go through the original consent process all over again.

Given the granular and customisable nature of the consent, there is a possibility at renewal that consent choices may change (either deliberately or inadvertently). Changes to that consent may mean the CDR product or service cannot be continued – or the customer's experience of the product or service will change in a way they did not expect or anticipate.

We submit that a Rule should be introduced that allows for a simple process for consents to be 'renewed' on a 'one click' basis directly via the Dashboard or through an in-App or online capability delivered to consumers. Again, to the extent CDR is about convenience, customers should be able to renew their consent easily.

6. **CDR Consent Standard (R4.10)**

Rule 4.10(2)(d) requires ADRs to seek consent in accordance with the Standards. We do not believe that the consent process should be subject to a mandated standard. Mandated standards are necessary in circumstances where issues of format and interoperability would prevent sharing between parties, however, it is not necessary in relation to an ADR's own user experience.

We agree that there is a need for the Data Standards body to develop guidance and 'best practice' in relation to consent, but ADRs should have flexibility to determine an overall UX that works best for its customers having regard to the underlying product or service. A 'one size fits all' approach to consent is unrealistic and unnecessary given the range of services and products that will make use of the CDR Data and how consumers will interact with them.

Rule 4.10(1) already requires consent to be voluntary, express, informed, specific, time limited and easily withdrawn – which binds all ADRs. ADRs should be able to meet these requirements in a way that best suits their UX objectives. There seems little point in having these principles under the Rules if ultimately, the Data Standards body is mandating the manner of consent collection.

We are also concerned by the risk that large Data Holders may influence the design of these consent standards in such a way as to make them unwieldly to inhibit uptake of the CDR Right.

7. CDR Consent Granularity – Rule 4.10 (3) & 4.16 (3)

Rule 4.10(3) and 4.16(3) effectively creates divisible consents for the i) act of collection ii) data set and iii) the purpose of data collection - which could result in an large number of possible consent outcomes. Whilst in principle, such a customisable consent process is desirable – in practice, it will be unworkable.

Depending on the choices made by a consumer, a service provider may not ultimately be able to provide the service requested (or may only be able to provide a sub-optimal version of that service). It may require providers to provide customisable/dynamic service propositions which will come at a higher cost than 'off the shelf' propositions – or not at all.

Providers need to be able to mandate minimum data sets and purposes to make their product or service offerings viable – whilst always having regard to the Data Minimisation principle. The main

objective should be transparency around what the ADR is proposing to collect and the purposes for which it will use that data. The data subject then has full control whether to proceed or not.

Presenting false options to the customers is problematic from a UX perspective. For example, an ADR can present a user with an un-ticked box relating to Transaction Data – but if the ADR ultimately needs Transaction Data to provide its PFM service, what benefit is there in giving the data subject that choice when signing up for the PFM?

Similarly, if a user is applying for a credit card and the ADR requires as a minimum, the current account balance and transaction data for responsible lending verification, why would the ADR give the user the ability to de-select those fields? It achieves nothing.

We find it perplexing that Rule 4.10(2)(a) requires an ADR to make the consent process 'easy to understand', given that the entirety of the consent process is mandated by the CDR Rules & Standards, and as proposed, will be a very confusing and complicated experience.

We therefore recommend that 4.10(3)(b) and 4.16(3)(b) be deleted. And 4.10(3)(c) and 4.16(3)(c) be updated accordingly.

8. Authorisation – R4.5 and 4.22

The Authorisation step between a Data Holder and Consumer is duplicative and creates an unnecessary break in the customer journey which is likely to lead to significant drop-outs. We do not think that an authorisation step is warranted given that a data subject has already provided a detailed consent to a regulated ADR entity. CDR creates a framework of trust between participating parties and gives rise to a contract binding between an ADR and a Data Holder. By design, the authorisation step is redundant and unnecessary, because a Data Holder is able to trust the request of the ADR. There are significant consequences for an ADR if it requests data for which consent has not been given.

Requiring Data Holders to police consent is unnecessary. Customers will rightly query why they have to consent twice to the same thing? It is simply poor design and creates unnecessary barriers. Again, we think this will materially impact uptake due to increase drop-out at the authorisation stage.

For clarity, these comments relate to the authorisation process, not authentication per se.

Authorisation Detail

The level of detail under 4.22(2) is unnecessary. If the ACCC is intent on keeping the authorisation step, we believe authorisation should be limited to a simple message notifying the data subject that a request has been made, providing the name of the ADR and asking the data subject to confirm their consent. It is unclear what value is added by asking consumers the same questions twice.

9. Usability Metrics in Testing of CDR Standards

8.11(3) requires the Standards authority to engage in consumer testing, but is silent as to what metrics it is being test against. We think that the rule should make express reference to matters of user experience and usability (i.e. ease of interaction, convenience, time). For CDR to succeed, it is crucial that consent, notification and authentication steps are reviewed through a usability lense with a view to likely uptake. We think there is a significant risk of drop-out with the current journeys which will seriously hamper the success of CDR. The objective of the testing should not be to simply test whether consumers have understood information presented to them – but whether they found the process simple, convenient and intuitive.

10. Notification Requirements (R5.12(d))

Rule 5.12(d) is very broad and should have a materiality threshold. As a minimum, we recommend replacing 'could' with 'would'.

11. **Dashboard Requirement (R1.13) - Cancelled products and 'one off' data requests**

We think the Dashboard obligations should differ as between Data Holders and Accredited Data Recipients. Specifically, Accredited Data Recipients should not be subject to a requirement to provide a dashboard in relation to 'one-off' data requests. For example, in respect of a credit card applicant where the user's card application is not successful, it seems unnecessary for that ADR to provide ongoing access to a Dashboard.

A dashboard should only be a requirement for so long as the ADR has an ongoing relationship with the consumer. Where consent is cancelled or there is no ongoing relationship, the ADR should not be required to maintain access to its systems. A consumer would of course, be able to see a history of data access requests and authorisations on its Dashboard with the Data Holder.

Requiring an ADR to provide access to its systems to people who are no longer customers, gives rise to security risks and operational complexity. ADRs would be forced to manage access and security credentials of those non-members in perpetuity.

We recommend therefore that Rule 1.13 be updated with an exception to the requirement on ADRs to provide a Dashboard where:

- There is no ongoing relationship with the consumer (i.e. the relevant product/service is cancelled or the applicant was unsuccessful);
- Consent has expired or been withdrawn;
- Data is no longer being accessed by the ADR; and
- All CDR Data has been purged or de-identified.

12. 'Prohibited Use or Disclosure'

The definition of 'prohibited use or disclosure' currently extends to aggregating CDR data for the purpose of compiling insights in relation to any person who is not the CDR Consumer for that data. This prohibition is inherently problematic and removes one of the major commercial incentives for participation.

The ability to use data for insights and analytics does not of itself harm consumers, it is simply a way of understanding behaviours across groups. Using data in this way is critical to innovation and development in a range of fields. As drafted, the CDR Rules would prevent an ADR from applying learnings and insights about a group of people derived from CDR-Data more broadly outside of its CDR segment. For example, an ADR may obtain insights from CDR Data that suggest large transactions at a particular merchant type are a risk indicator for default based on an analysis of data obtained through a PFM. The ADR would be prevented from using that insight to inform its broader risk modelling given that it could indirectly have application to non-CDR individuals.

Insights obtained in relation to a specific CDR sample set will necessarily be applied more broadly in the same way that sample sets are used to extrapolate and infer in a range of fields. Insights from CDR Data will tell us something about groups beyond the subject sample group – it seems unnecessary to prohibit the use of those insights more broadly.

13. Screen Scraping

Schedule 1, Privacy Safeguard 12, Control Requirement 3 – Data Loss Prevention, requires ADRs to block or prevent screen scraping. In practice, this will likely mean that ADRs will need to block screen-scraping across the entirety of its online environment, impacting CDR and non-CDR customers (for example, where American Express is an ADR, it would likely need to block screen scraping for all American Express customers – not just those who use and access its CDR services).

Many companies today choose not to block screen scraping based on a range of considerations such as relative security risks, cost, resource and effectiveness and sustainability of blocking measures. However, a primary consideration is also the desire to meet a customer need on the part of those customers who are happy to use products and services that employ screen scraping. The CDR Control Requirement would effectively force ADRs to block access to these products and services that large parts of its customer base are currently using.

From the outset, Open Banking and CDR has been about giving customers choice. By blocking screen scraping, customers are denied a choice. Screen Scrapers are used today across the financial services ecosystem and are crucial to banks and financial institutions to achieve a range of regulatory and business objectives. To impose an effective ban on scraping will have a significant impact on accessibility of those services with no guarantee as to when and if those services will be replaced by CDR versions.

We are hopeful that CDR provides a viable exchange mechanism for data in Australia which renders screen scraping obsolete, however there remain questions around uptake of CDR given its current design. Until CDR is a viable alternative, it is important that consumers are given the flexibility to choose how to access data.

14. Data Standards that Must Be Made – R8.11

As outlined above, we consider that the number of areas subject to Data Standards is too broad. We think that standardisation should be limited to areas where standardisation is required to ensure interoperability between participants. To the extent that standards impose requirements on service or product providers around the design of their own interfaces, we consider that this is unnecessary and goes too far.

AS a minimum, we think the following should be removed:

- 8.11(1)(a) the process for making data requests;
- (1)(b)(ii) in relation to authorisations (*which we believe should be eliminated as a step under the CDR Framework*)
- 8.11(1)(g) relating to communications and notice between CDR participants and their customers.

We think it would be appropriate for the Data Standards Body to develop standards of 'best practice' and guidance in relation to these matters, but not to prescribe process.

15. Transaction Data - Schedule 2, 1.3(3)(c)

The current definition of Transaction Data is broad and includes 'any data provided by a merchant'. As we have submitted previously, certain transaction data will be a point of competitive difference between account providers and issuers.

For example, a payment provider may include SKU level transaction data in its transaction statements which it has secured under commercial terms with the merchant. Its arrangements with those merchants typically impose confidentiality restrictions and prevent the ADR from sharing that data with other parties. Further, it creates a point of competitive difference with providers who are not able to deliver SKU data.

We recommend therefore that R1.3(3)(c) be qualified with a caveat that it only applies to information in relation to the transaction that is 'standard' for that Product Type and which is not subject to a confidentiality restriction with 3rd parties.

16. Associated Features and Benefits

Schedule 2, 1.3(4)(d) refers to 'features and benefits' of products. One of the key features of credit cards in the Australian markets – as is well known by the ACCC – is loyalty points. We think the definition of product data under the CDR Rules should expressly reference loyalty points to ensure their inclusion, rather than leaving it to the Standards body. We are concerned by the ability of ADIs to influence the CDR Standards to exclude data points which may render their products less attractive when compared to competitor products. Prescribing these features and benefits at a rule level prevents their exclusion at the Standards level, and will ensure that consumers can compare products across a range of useful metrics, driving competition.

17. Date of Birth – customer Data (Schedule 2, 1.3(1))

Under 1.3(1), DOB is excluded from Customer Information. DOB is a key field for lenders. For example, DOB is required in order conduct credit bureau requests and is critical to some of the verification use cases required by lenders to meet a range of regulatory requirements. The ability to access DOB would allow data subjects to seamlessly compare products, check eligibility and apply for a card product with a single data pull. This would reduce friction for consumers and improve competition. It is unclear where DOB has been excluded, when the full range of other personal information has been included. We believe that this matter should be revisited.

18. Joint Accounts – Schedule 2, Part 3, 3.2

Under R3.2 of Schedule 2, ADI's have complete freedom to determine how a joint management service works. This is at odds with the rest of the CDR Rules which prescribe in great detail how consents and authorisations are managed.

Joint Accounts constitute a large proportion of accounts in Australia. Giving ADIs the ability to determine how Joint Account holders can make requests, allows them to impose obstacles to authorisation and access, effectively gating data as they see fit. Given that ADIs can even determine whether to make the service online or not, in theory, an ADI could impose a requirement for a joint account holder to come into a branch with identification and sign an authorisation, before data will be released.

Given the number of joint accounts in the market, we are concerned that this gives too much power to Data Holders to frustrate the objectives of CDR and to prevent the sharing of data in relation to joint accounts.

American Express would be more than happy to discuss any part of this submission in more detail or to discuss Open Banking or CDR more generally. Please contact Julian Charters at [redacted] or Adam Roberts at [redacted] for further information.