12 October 2018

Submitted to the ACCC via online portal

Dear ACCC,

Consumer Data Right – Rules Framework Consultation

American Express has been a long-time supporter of Open Banking in Australia. Our main objective in providing feedback is to ensure strong uptake of the Consumer Data Right by consumers to ensure that Open Banking succeeds. We value the work and effort of the ACCC to deliver this Framework within such a small timeframe, particularly given the underlying legislation is still subject to consultation and change.

Our view is that the current Rules Framework is a good starting point, but tends too much to the prescriptive, which risks being at the expense of product innovation and delivery.

Safeguarding Uptake of CDR & Open Banking

The Consumer Data Right has little usability or value to consumers where there are no products and services that make use of it. Whilst it is important to put the consumer in the driver's seat, you need a car first (i.e. the products and services). One of the primary objectives with the introduction of Open Banking is to spur competition and innovation in financial services. The current Rules Framework as proposed risks deterring some of that activity. In fact, many of the 'use cases' identified in the Open Banking Report and Recommendations would simply not be possible given some of the restrictions and requirements of the proposed Rules Framework.

It is important that there be sufficient flexibility and incentive in the CDR Rules Framework to ensure high participation from a diversity of new entrants. Where participation is perceived as too complicated or cumbersome, then data recipients will likely simply invest in screen scrapping tools preferring to receive data without the many strings attached.

Specifically, American Express is concerned by the level of prescription around disclosure and consent, and the prohibition on consent based direct marketing.

We believe that the Rules Framework should be principles and outcome driven, to allow Open Banking to develop and grow, as we have detailed more specifically below. We make these submissions out of a genuine desire to see Open Banking thrive in Australia.

SUBMISSIONS

1. CONSENT & DISCLOSURE

Transparency is critical to maintaining trust and confidence in the CDR system. We fundamentally and strongly support that objective, but perhaps have a different idea about the best way to go about it. We think that Accredited Data Recipients (along with their developers and designers) are best placed to determine how to achieve 'best in class' transparency in relation to their products and services.

Behavioural Economics tells us clearly that that more information does not necessarily result in better decision making by consumers. We think the proposed Rules Framework too often ignores this reality.

We submit that the approach to consent should be principles-based and outcome-driven. Specifically, the overarching guiding principle should be 'no surprises'; the principle that a customer should never be surprised by how an Accredited Data Recipient (ADR) is using data. This principle should be reinforced by guidance from the ACCC along with examples of 'best practice' – rather than prescriptive rules. This approach should be complemented by mystery shopping, audits and complaints monitoring/reporting.

Establishing a robust accreditation process means that ADRs can be trusted to design and build user journeys and experiences that safeguard the 'no surprises' principle. Where that trust is breached, consequences should be strong in order to maintain integrity of the CDR system.

We think that the current approach to consent risks 'over-disclosure' which could result in disclosure fatigue, decision paralysis and risks generating a perception that CDR is implicitly risky or unsafe.

Consumers' interests are best served by being able to make simple choices with confidence, knowing that there is a regulatory framework in place that will protect them – not by being inundated with regulatory disclosures.

a) No Pre-Conditioning Consent

- The 'no pre-conditioning' requirement seems to ignore some of the fundamental Open Banking 'use cases' for which access to CDR Data will be a necessary precondition of the service. For example, a Personal Financial Management (PFM) dashboard necessarily requires CDR Data given its fundamental purpose is to aggregate multiple accounts into a single view on a continuous basis. Such a service could not be provided without CDR Data. It would seem like an odd outcome if the rules essentially impose a requirement on a provider to register a customer and set up an account for a service they can't then use?

- To the extent that the manual provision of data by a customer is likely to impose greater resource requirements and cost on a provider, there should be some flexibility in these requirements to allow some pre-conditioning. For example, where a provider seeks to offer a lower cost 'online only' service, it should not be restrained from doing so. Imposing these restraints may impact innovation in certain products and services.

- American Express submits that so long as providers are clear, up-front and transparent that CDR Data is being used and the purposes for use, then they should be given flexibility to determine whether CDR access (and therefore consent) is a necessary component of their product or service offering.

b) Unbundling & Express Consent

- As above, context is important to determining how a consent journey is built. For certain products and services bundled and implied consents may be appropriate where the purpose of CDR Data in relation to the product is clear and obvious. For example, where a Consumer seeks to use a PFM, consent to access CDR Data is a necessary and obvious part of the product. Ongoing active use of that PFM would imply consent to continued access to the CDR Data.

- AS outlined above, the ACCC should issue guidance and provide examples of best practice in relation to consent rather than define specific rules.

c) Informed & Specific Consent

- Informed decision making is a key cornerstone of the CDR regime, however the Rules Framework needs to strike the right balance to avoid overloading customers with information. Often, decisions can be made harder through too much information resulting in decision paralysis (i.e. abandoning the decision) or lead to impulsive decision making (i.e. clicking 'yes' rather than reading a long disclosure). Flexibility should be given to ADRs to determine the optimal amount of information and manner of delivery to achieve 'no surprises' transparency.

- Brevity plays an important role in communication and consumer comprehension. Specific detail does not necessarily result in better understanding.

- Granularity imposes significant operational complexity and cost. There is no clear evidence that it will result in better decision making – conversely, our submission is that it will do the opposite. ADRs should be given flexibility to obtain broader consents, but always working to the principle of 'no surprises'.

- Layered consent models where important information is 'triaged' ensuring that data use that is unexpected or unusual is given greater prominence will ensure that consumers are clear about the things that are most critical and relevant to their decision. We think that can be achieved better using simplified general disclosures, over complex and detailed ones.

Listing 3rd Party Intermediaries & Outsourced Providers

- Requiring an ADR to specify in detail its arrangements with 3rd parties is onerous and assumes an unrealistic level of consumer engagement. It is unclear why the ACCC feels

such detail is necessary or how a consumer should act on this information? A consumer has no real framework by which to assess or use this information.

- The principle should be that all times a consumer is 'held harmless' by the Data Recipient irrespective of whether or which 3rd parties it retains. Ultimately, the Data Recipient is better placed to make a decision about the reliability of a third party than the consumer.

- Including this information just adds length to disclosures, without improving decision making. Consumers are much less likely to engage with long disclosures.

- Customers should of course be able to request and find information about third parties – but there should be flexibility as to how that is done.

Consumer Testing

- American Express engage in extensive consumer testing and customer research. Whilst we believe there is benefit in such testing, it should not be subject to a universal rule requirement. The CDR consent decision is a relatively straightforward process. The challenge to comprehension and understanding derives not from the risks of the underlying decision to be made, but from the amount of information the Rules Framework is seeking to mandate. In any event, consumer testing is pointless in circumstances where the Rules are mandating the content and manner of disclosure given that changes would not be permitted.

d) 'Minimum Data Necessary' Principle

- Whether data is 'necessary' or not is highly subjective. For example, where certain data is used in an algorithmic decision making process, the value of each data point in the model will vary (i.e. some will be critical and others will be for refinement, but have little impact on the ultimate decision outcome). Who determines whether each data set is ultimately necessary? And in the end, why would it matter to the consumer so long as they knew how it was being used in the first instance?

- We submit that the main objective of the Rules should be to ensure that there is always a clearly disclosed purpose for accessing the data and a nexus between the data and that purpose – rather than a principle of necessity. So long as an ADR is only collecting data for which it has a clearly disclosed purpose, necessity is likely to be irrelevant to a consumer.

e) 90 Day Re-Authentication

- It is unclear why a consumer is likely to change their mind about consent every 90 days and need prompting. American Express full supports transparency and awareness, but re-authenticating every 90 days will just prove a paint point for both Consumers and CDR Participants.

- The 90 day limit is out of step with how consent is managed under the Australian Privacy Principles.

- Ongoing consent can be implied in certain contexts. For example, in respect of a consumer who uses a PFM App every few days, it would seem fairly evident from the ongoing use of that App that the consumer's consent to the access of CDR Data continues.

- Again, these types of notices and disclosures risk implicitly suggesting to consumers that the CDR system is unsafe or not trustworthy – requiring ongoing vigilance. This could affect uptake of the CDR Right unnecessarily. We would reiterate, that it is critically important for consumers to have trust in the CDR System. Trust is better maintained through robust accreditation and strong enforcement, rather than detailed and laboured consent journeys.

- Finally, consumers already have a persistent right to withdraw consent at any time under the Rules Framework. The 90 day rule therefore seems superfluous.

f) Consent Withdrawal without Detriment

- As outlined above, where access to CDR Data is an inherent part of the underlying product or service, it is not possible for the customer to continue to use that product or service after withdrawing consent. By implication therefore, withdrawing consent will necessarily result in detriment in some instances. More flexibility is required here.

g) Dashboard

- The requirement to build an online dashboard imposes a major infrastructure build on Data Holders and Data Recipients. As above, CDR Participants should be given flexibility to determine a consent management process that suits its underlying product or service offering. For simple use cases, a Dashboard seems unwieldly – for example, where an ADR credit provider conducts a one off API call as part of a card application process, why would it need to build a dashboard? Similarly, a Data Holder should have flexibility around how that information is made available having regard to their usual tools and practices.

- A dashboard for CDR Data, which is a specific set of personal information, is likely to be confusing to customers given that it will sit in isolated contrast to how all other personal information held about them by that organisation is treated. It is unclear why CDR Data justifies this dashboard treatment?

2. BAN ON DIRECT MARKETING

- Banning an ADR from using CDR Data for direct marketing creates a competitive imbalance as between Data Holders and ADRs. This runs counter to one of the fundamental objectives of

Open Banking, which is to level the playing field to spur competition and innovation in financial services. The practical impact of imposing such a ban, is that a Data Holder is freely able to use customer and transaction data for marketing purposes (with consent), whereas an ADR cannot.

- The approach to direct marketing is out of step with the Australian Privacy Principles which allows for the use of personal information for direct marketing with consent. There is no principled basis for treating CDR Data any differently. There are far more sensitive data sets available in the broader economy, particularly those data sets held by big tech, which are used freely for marketing and advertising (with consent)?

- Many of the main product/service 'use cases' that Open Banking would enable would be unworkable with this prohibition. For example:

    - a product comparison site could not use Product or Transaction data to make a tailored recommendation about an alternative product.

    - an electricity plan recommender service, could not use electricity information to offer an alternative electricity plan.

    - a financial management tool could not use Transaction Data to make money savings suggestions by identifying 'live' deals/offers in the market.

    - an online challenger bank who onboards a customer using CDR Data including name, address and contact details would forever be prevented from using that data for marketing despite having an ongoing banking relationship with the customer.

- If the objective with Open Banking is to unlock competition, it is unclear how that is to be achieved when a competitor would be restricted in its ability to offer its own products/services to the consumer?

- American Express recommends that the approach to Direct Marketing should mirror the approach under the Australian Privacy Principles.

3. ACCREDITATION OF ADRs

a) AFSL & Credit Licensees Streamline

- AFSL and Credit License holders are regulated by ASIC and subject to rigorous conduct, reporting and complaints requirements. Such providers already hold large amounts of customer data and are well placed to receive CDR Data.

- Given the likely backlog of accreditation applications that will need to be considered by the ACCC, we submit that AFSL and Credit License holders should be given automatic accreditation upon application or be subject to a 'streamlined' application process.

b) Accreditation Tiers

- Amex has always been of the view that a single standard of accreditation (rather than tiers) should apply to maintain utmost trust and confidence in the CDR system. Security of data is paramount. Creating a tiered approach to the CDR system creates operational complexity for CDR Participants, compromises security and risks causing potential uncertainty and confusion for consumers. To the extent that there are costs relating to prudent management of data, that is simply part of the cost of responsibly engaging in business in 2018.

4. OUTSOURCING BY ADRs

- ADRs should be responsible at all times for any outsourced service providers under the Rules. An ADR will then necessarily have a strong commercial incentive to be selective, prudent and diligent when appointing 3rd party providers.

- As to how an ADR satisfies itself that a 3rd party will not jeopardise the ADR's compliance with the ADR Rules, that should purely be a matter for the ADR. There is little value in imposing 'model contract' requirements between ADRs and their service providers, as there is no guarantee in any event that a 3rd party will comply with the terms of the contract. So long as consumers are protected, everything else is purely a commercial matter between the ADR and their 3rd party.

5. SHARING WITH CUSTOMERS & NON-ACCREDITED PARTIES

a) Sharing Direct to Customer Data

- American Express believes that care should be taken in considering how consumers may be able to access CDR data directly as part of the CDR System. The Open Banking Report did not expressly recommend that consumers be able to receive CDR Data under Open Banking, rather – a consumer should be able to direct their data to accredited parties who meet requisite security requirements.

- Consumers have an existing right to access their data under the Australian Privacy Principles, however the format and medium of transfer is not prescribed. As such, requests are met through a range of data formats. Standardising the data format as contemplated under the CDR system could concentrate the risk of trawling, phishing and interception.

- Further, providing CDR direct to consumers in a standardised format allows the potential creation of less scrupulous business models whereby a provider may seek data directly via the consumer and avoid seeking accreditation.

- The Rules Framework proposes robust security requirements on Data Recipients and 3rd Parties, however, there are no such requirements or safeguards around direct consumer receipt of such data. American Express is not suggesting that consumers should be prevented from

accessing their data, but that the ACCC and the Data Standards Body need to take care to avoid vulnerabilities in the CDR system. These issues require careful consideration given trawling and phishing risks to data.

b) Disclosure to Non-Accredited Parties

- Giving access to non-accredited entities at the direction of consumers will fundamentally compromise the CDR system. It risks incentivising the creation of business models and relationships which allow for the use of CDR Data in unregulated ways and will which potentially create vulnerabilities. The primary objective of the Rules should be to establish and preserve the integrity of the CDR system.

- Whilst opportunities to share data with non-accredited parties may emerge as Open Banking develops, it is important that Open Banking be allowed to develop safely and securely first.

- The only circumstances in which a non-accredited entity should have access to CDR Data, is in circumstances where it is to an ADR's outsourced service provider and provided always that the ADR remains fully responsible and liable for that third party (as outlined in 4 above).

6. COMPLEX ACCOUNTS

a) Joint Accounts

- We believe that it is critical for Joint Accounts to be included within the CDR system from the outset. Given the prevalence of joint accounts in Australia, CDR Data is likely to be materially compromised from the outset if such data is excluded.

- Joint Accounts are in practice very simple propositions. We think CDR consent should just follow account permissions (i.e. any account holder who has permission to access joint account data should have the ability to provide consent to access that same data). It is a matter for the Data Holder to manage account permissions, and those permissions should simply flow through to the CDR system (rather than creating additional/conflicting rules).

- Of course for such data to be reliable, accurate and usable within the CDR system and to avoid privacy concerns, it is important that the data is properly segmented as between account holders (for example, where an ADR requires Transaction Data in respect of a single Joint Account Holder, the Data Holder should ensure that it can make available only that set of data). This is largely a matter for the Data Standards Body but we think the Rules Framework should emphasise the principle.

b) Corporate Card Expense Accounts

- The ACCC has asked for feedback on complex accounts. Given American Express' experience with corporate expense accounts (used for company expenses and travel), we felt it appropriate to comment on those accounts. Including corporate expense account data within the CDR system poses unique challenges given that the data on the account may relate to an employee,

an employer or both. How and when such data may be shared raises a range of privacy, employment, intellectual property and contractual considerations.

- Our corporate account structures vary depending on the company (for example, liability for transactions under a Corporate Card Account may fall on the employer, the employee directly or on both). Further, the manner in which the card is to be used will be subject to an Employer's Policies on travel and expenses (which may allow for some personal spend and reimbursement). Access and administration of a Corporate Card Account may not be given directly to the individual, as it is often delegated to program administrators (however admin authorisations often vary and sometimes overlap).

- For corporate expense accounts, determining which data can be provided, by whom, for which account and with whose authority within the CDR system is not clear. Unlike with joint accounts, there are no simple principles under which to operate.

- We think these matters require careful consideration. Corporate expense accounts are not critical to the operation of the CDR system at this stage and we would submit that they should be dealt with as part of subsequent iterations of the Rules. American Express would be happy to assist the ACCC and provide further information at that time.

7. AUTHENTICATION & AUTHORISATION

- The rules framework proposes a range of consent, authentication and notification steps from both Data Holders and ADRs. As set out above, this approach should be rationalised to avoid confusing the customer with multiple notices and disclosures. Further, such an approach will impose a complex set of APIs to manage which creates additional cost and operational complexity.

- The primary responsibility should fall with the ADR to explain the data they will be accessing and to obtain an appropriate consent. Requiring the Data Holder to police the precise type of consent adds a layer of unnecessary complexity and creates an opportunity for Data Holders to frustrate access.

8. METADATA SETS

- CDR Consumers cannot be expected to make informed choices in relation to data sets they don't understand or cannot relate to. Whether and which types of metadata should be included in the CDR system raises a range of considerations. A significant amount of metadata collected by a Data Holder is for fraud detection and prevention purposes such as IP Address, Device ID or Geo Location. That data is shared amongst the participants in the payments network for authentication purposes and is not seen or made available to customers. Sharing such information could raise security issues. In principle, American Express recommends that only metadata that is currently made available to consumers today, should be available.

- Some sets of metadata are collected as competitive differentiators. They are collected, stored and displayed as the result of specific investment and commercial agreement on the part of the Data Holder. In those instances, the data represents the intellectual property of the Data Holder or another party, and is often subject to confidentiality obligations under contracts with that third parties. Some financial institutions may, for example, have arrangements with specific merchants to display more detailed transaction information (i.e. details about the product purchased). American Express recommends therefore that only metadata that is common or standard across the sector should be shared.

9. PRIVACY POLICIES & CDR POLICIES

- The Rules Framework should make it clear that a company's Privacy Policy and CDR Policy can be combined. It is unrealistic and unfair to consumers to expect them to read two separate documents.

10. DIGITAL IDENTITY

- Evidently, Digital Identity is a critical piece of infrastructure that would improve the efficiency and security of the CDR system. As the ACCC would be aware, the Australian payments industry through AusPayNet is engaged in work to create a Digital Identity solution for Australia. American Express would recommend that ACCC consult closely with AusPayNet to ensure that the implementation of CDR is consistent with Digital ID (and vice versa) – if it is not already doing so.

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.