NATIONAL AUSTRALIA BANK SUBMISSION

Consultation on *Consumer Data Right Rules amendments (version 3)* exposure draft released by Treasury 1 July 2021

30 July 2021

Introduction

NAB welcomes the opportunity to respond to the Department of Treasury's (**Treasury's**) exposure draft of the *Consumer Data Right Rules amendments (version 3)*, released on 1 July 2021 (**CDR Rules v 3.0**).

NAB has been an active participant in the Australian Competition and Consumer Commission's (**ACCC's**) and Treasury's consultation processes including in relation to previous amendments to the Consumer Data Right Rules (**Rules**) and the Data Standards Body's (**Data61's**) development of the Consumer Data Standards (**Standards**).

This submission builds on NAB's extensive contributions to the public policy debate on Open Banking and the Consumer Data Right (**CDR**). These include:

- NAB's September 2017 submission in response to the Review into Open Banking;
- NAB's March 2018 submission in response to the Review into Open Banking;
- NAB's September 2018 submission in response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018;
- NAB's October 2018 submission in response to a further Treasury consultation on the CDR Bill;
- NAB's October 2018 submission in response to the ACCC's consultation on the Consumer Data Right Rules Framework;
- NAB's May 2019 submission in response to the ACCC's consultation on the Consumer Data Right Exposure Draft Rules;
- NAB's November 2019 submission in response to the Office of the Australian Information Commissioner's consultation on the draft CDR Privacy Safeguard Guidelines;
- NAB's February 2020 submission in response to the ACCC's consultation on how best to facilitate participation of third party service providers;
- NAB's May 2020 submission in response to Treasury's inquiry into future directions for the Consumer Data Right;
- NAB's July 2020 submission in response to the ACCC's consultation on the draft Consumer Data Right Rules and Privacy Impact Assessment that allow for intermediaries;
- NAB's October 2020 submission in response to the ACCC's consultation on the Consumer Data Right Rules expansion amendments; and
- NAB's May 2021 submission in response to the Data Standards Body's Design Paper on an 'opt-out' data sharing model for joint accounts.

NAB has also contributed to the Australian Banking Association's submissions to the above consultations.

Overview

The exposure draft sets out significant proposed amendments to the CDR. In providing its submission on the CDR Rules v 3.0, NAB has in mind the following guiding principles: technical assessment, timeliness for delivery, privacy and security impact, and customer experience and consent.

NAB is supportive of increased participation of intermediaries in the CDR ecosystem as well as decreased friction for customers accessing the CDR. However, NAB is concerned that some of the proposed changes to the Rules create risks around information security and privacy, and undermine the consent-based model of the CDR.

Joint accounts

As set out in past submissions, NAB is supportive of CDR data sharing mechanisms for joint accounts where achieved in a way that is secure, consent-based and maintains consumer confidence in the ecosystem.

The proposed rules for joint accounts, specifically moving most joint accounts to the default 'pre-approval' setting, do not promote a consent-based system (which is one of the pillars of Open Banking). Further, NAB is concerned that the proposed changes add complexity to the regime, particularly for NAB's main brand customers with joint accounts who have only recently commenced participating in the CDR under the current joint account rules.[1] It is for these reasons that NAB does not support the proposed joint account rules as currently drafted.

Participation models

NAB is of the view that intermediaries should play an important part in the CDR system and should be included under a tiered accreditation model. However, the proposed sponsored accreditation, CDR representative, outsourced provider and trusted advisor models do not provide the level of data and privacy protection and information security that NAB considers is necessary for an effective CDR ecosystem.

As NAB has reiterated in previous submissions, the success or otherwise of the CDR turns on whether consumers have trust and confidence in the system and its participants. Critical to this is that there are sufficiently strong information security measures and appropriate privacy protections in place.

It is for this reason that NAB does not support the transfer of CDR data to non-accredited entities. Accreditation should provide a level of data privacy and security that protects consumers CDR data and promotes confidence in the system. NAB considers that the proposals in relation to sponsored accreditation, CDR representative, outsourced provider and trusted advisor models may put this level of security and protection at risk.

Joint accounts

NAB has concerns that the proposed changes to joint accounts undermine a central principle of the CDR regime, being that consumers should be in control of their CDR data, and any movement of CDR data should be based on consent. Automatically moving joint accounts[2] to the 'pre-approval' setting as a default with only 7 days' notice impacts on the ability of an individual to consent to that approval setting to begin with, as well as to all future consents made to share CDR data from that joint account where made by another account holder.

The default 'pre-approval' setting raises concerns in relation to privacy, the protection of vulnerable customers, as well as general customer friction and poor experience.

Privacy issues and vulnerable customers

Under the 'pre-approval' setting, one account holder may unilaterally consent for data to be shared on behalf of both account holders. In NAB's view, there are risks associated with this pre-approval setting because consumer control and privacy are diminished if sharing is done as a default without both account-holders' consent. NAB appreciates that the CDR Rules v 3.0 proposal is seeking to strike a balance between consumer control and ensuring minimal friction to data sharing, however, NAB does not consider that this should come at the cost of privacy and in particular the privacy and safety of vulnerable consumers.

Whilst NAB notes that there are mechanisms within the Rules for Data Holders to restrict sharing to prevent physical or financial harm, NAB echoes previous comments made in relation to the limitations associated with these provisions, as they rely on the ability of organisations to recognise and detect these risks to individuals. The reality is that in many cases this may not be practically feasible, where for example vulnerable customers themselves are not in a position to identify that they are in a coercive or an abusive relationship with a joint account holder, or there is insufficient awareness or information available to an organisation to identify and mitigate these risks to customers.

[1] NAB's main brand excludes UBank.

[2] With the exception of joint accounts currently set to the 'non-disclosure' option under current Rules.

NAB notes the comments made in the explanatory note to the CDR Rules v 3.0 that the "Rules reflect current data sharing capabilities on joint accounts for PDF and CSV files." NAB thinks this analogy fails to recognise the difference between the current scenario, where individual account holders would be able to download statements in CSV and PDF format and share this information themselves, without any facilitation by or assistance of a Data Holder (as would be the case under the CDR). Further, if the CDR Rules are changed in the manner proposed to prescribe default sharing where one party elects to do so (which we would not recommend), then this also has the potential to raise regulatory risks to Data Holders that share data at the request of one account holder (but not both) and NAB considers that it would need to be made clear (within the Rules) that if a Data Holder shares information in this way (i.e. by virtue of a pre-approval), it would not be contravening other applicable laws (such as privacy laws).

Customer friction and poor experience

NAB is of the view that introducing the proposed changes to joint accounts will cause significant confusion and friction for NAB's main brand joint account holders, who less than twelve months ago began to participate in the CDR using the Joint Account Management Services (**JAMS**) under the current joint account rules. Most notably, the 'pre-approval' setting is inconsistent with transaction authority settings currently in place for most joint accounts.

It is likely that customers will experience confusion with the 'pre-approval' setting for data sharing being out of sync with the existing transaction authority setting in place for their account. Similarly, one joint account holder may change the account's CDR data sharing setting (e.g. from 'co-approval' to 'pre-approval') and fail to understand that the account's transaction authority settings have not also changed, and that conflicting permissions exist in relation to their account. NAB foresees further issues of this nature when the CDR is extended to include write access, including matters of technical complexity in building for this.

The proposed rules for joint accounts represent a significant change in approach from the approach set out in the JAMS. JAMS is currently specified on an 'opt out' model, unless a joint account holder takes action to opt in. Most of NAB's joint account holder have not made any positive step either to opt in or opt out – they have remained inactive under the JAMS system. As a practical matter, it will be difficult for NAB to determine whether these inactive joint account holders should be moved to the default 'pre-approval' setting, the 'co-approval' setting, or the 'non-disclosure' setting.

Suggestions

In relation to the proposed changes to joint accounts, NAB makes the following suggestions:

1. The 'non-disclosure' setting should be the default setting all new joint accounts are moved to. This is most consistent with customer experience on JAMS to date.
2. The 'co-approval' setting should be a mandatory option offered by all data holders.
3. The Rules should clarify how changing the disclosure setting from 'pre-approval' to 'non-disclosure' impacts on the consents that are active for that joint account. For example, would this change in disclosure setting have the effect of putting the existing consent on hold, or would the consent be revoked.
4. In relation to the obligation to notify account holders of relevant notifications through the 'ordinary method' of contacting the joint account holder, amend this requirement to the 'ordinary *online* method'.

Participation models

The proposed sponsored accreditation, CDR representative, outsourced provider and trusted advisor models (together, the **proposed participation models**) all involve to some degree non-accredited entities participating in the CDR ecosystem and receiving CDR data.

CDR data should not be shared with non-accredited entities

This issue has arisen previously as part of Treasury consultation on the CDR Bill in September 2018, and ACCC consultation on how best to facilitate participation of third party service

providers in 2020. NAB maintains its previous position that CDR data should only be shared with accredited entities.

NAB is of this position for the following reasons:

a. The non-accredited participants included in the proposed participation models are not subject to appropriate information security processes, privacy safeguards or (in most cases) all the Privacy Act. This has serious potential consequences for the security of consumer's personal data, for example if a non-accredited entity is not required to report a data breach.

b. Appropriate information security and privacy protections must be put in place to maintain consumer confidence in the CDR ecosystem and to ensure that CDR data is safely held, transferred, used and then destroyed. Failure to provide adequate information security and privacy protection risks undermining the integrity of the CDR ecosystem and leading to poor consumer outcomes.

c. Customers should be aware at the time that they consent to the sharing of their CDR data that it is being shared with parties outside the CDR ecosystem. NAB considers there will be challenges in communicating this accurately to consumers, where multiple third parties may be involved under a participation model, and where the explanation must be communicated in a mobile app environment.

d. The proposed participation models do not clearly delineate liability for data breaches. It is unclear, where non-accredited participants receive CDR data, who the consumer has recourse to in the event of a data breach.

e. The obligations imposed on CDR participants should be commensurate to the sensitivity of data that the recipient will receive, and linked to the functions that the recipient will perform on behalf of the consumer. NAB continues to hold the view that all banking CDR data sits at the high risk level. Under the proposed participation models, the banking CDR data that may be shared with participants is unlimited (to the extent it is requested by a consumer) – and so the obligations imposed on these participants should be fulsome and equal to that of accredited participants.

f. If the CDR is later expanded to include write access, then NAB has serious concerns about the involvement of non-accredited participants, who may have write access to change or update personal and sensitive information of consumers without appropriate controls in place to guarantee security of the system. At its extreme, this risks the occurrence of fraudulent transactions that change personal identification information used for second factor authentications for a consumer's financial accounts.

g. In particular under the trusted adviser model, it is challenging for data holders to have confidence that a third party making a request on an API is who they claim to be. Under the trusted adviser model and other proposed participant models, NAB considers there is an increased risk of fraud and data compromise. The result of the proposed amendments is that data will be transferred from a secure environment provided by the data holder to an environment with potentially no security (for example, under the trusted adviser model).

h. There is minimal potential upside to the sharing of CDR data with non-accredited participants given there are existing mechanisms to transfer data from data holders to third parties. These mechanisms, such as the sharing of data with advisers through CSV files, operate materially differently from sharing under the trusted adviser model, including because they occur at an individual and bespoke level.

i. The CDR regime is already a complex one with multiple pathways for consumers to navigate. NAB is concerned that the proposed participation models add further complexity and will lead to consumer confusions, as well as compliance challenges for

small ADIs and uncertainty for ADRs. The proposed changes risk leading to an 'information overload' for consumers, while the ecosystem is still in its nascent stages.

Insufficient information security and privacy protections

NAB has previously provided feedback to ACCC that intermediaries are a necessary element of the CDR and that strong security measures, together with privacy protections are fundamental to the success of the CDR (see further details in NAB's submission to ACCC dated 3 February 2020).

NAB does not consider that the proposed participation models strike the right balance between encouraging further participation by entities in the CDR ecosystem and ensuring appropriate information security and privacy obligations are put in place on participants. Most notably, there are no adequate information security requirements set out for any of the proposed participation models, for example:

- Under the sponsored accreditation model, it is proposed that affiliates may be accredited while self-assessing and attesting their information security capabilities. Accreditation should provide protection such that consumers can have confidence their CDR data is protected by appropriate security privacy safeguards and information security processes. NAB considers that self-assessment and attestation of security capability, as opposed to independent third-party assessments, exposes CDR data to unsafe practices including data breaches, and could impact on the privacy of consumers' data.

- Under the proposed trusted advisor model, trusted advisors are not subject to any additional security or privacy requirements beyond what is already required in their field of practice. The classes of people listed in the CDR Rules v 3.0 include a number of classes of persons that NAB considers are not subject to sufficient professional standards, ongoing obligations, or disciplinary mechanisms that provide an appropriate level of security over data held by these persons.

In relation to the proposed participation models, we think additional clarity is required regarding the Privacy Safeguards that will apply to intermediaries and the adequacy of the security measures that will apply to CDR data. The Explanatory Note to the CDR Rules v 3.0 notes as follows:

> *Trusted advisers do not attract the regulatory obligations that apply to ADRs under the CDR regime. However, these rules recognise that as members of a professional class, they are subject to existing professional or regulatory oversight, including obligations consistent with safeguarding consumer data (e.g. fiduciary or other duties to act in the best interests of their clients).*

Whilst we appreciate that trusted advisors may be subject to a certain degree of regulatory oversight and have obligations consistent with safeguarding consumer data, we do not consider that these necessarily accord with the level of protection consumers would receive under the Privacy Safeguards or the Privacy Act. As noted in previous submissions, allowing CDR data to be transferred to non-accredited entities risks undermining the customer protection which the accreditation process is designed to provide.

Accreditation for data recipients ensures the appropriate security standards and privacy protections (including the privacy safeguards) operate to protect consumers. Non-accredited persons are not subject to the stringent privacy safeguards and may not be subject to the privacy legislation. As a consequence, non-accredited entities may not have requirements to notify data holders of a data breach. This means that data holders may not be made aware of a data breach that compromises their customer's data and presents a fraud risk. Given the nature and the sensitivity of the data which trusted advisors may gain access to, this can have obvious adverse impacts to consumers.

Proposed participation models likely to be commercially unpalatable

NAB considers that the goals of the proposed participation models are unlikely to be achieved as a result of the proposed arrangements being commercially unpalatable to data holders.

For example, under the sponsored accreditation model, sponsors (i.e. accredited data holders or ADRs) must implement a third-party management framework and manage affiliates in line with this framework. Before entering into a sponsorship arrangement with an affiliate, a sponsor must undertake due diligence to ensure the proposed affiliate is suitable for the role, provide assistance to the affiliate on technical and compliance matters, and take reasonable steps to ensure affiliates comply with their obligations. What amounts to 'reasonable steps' and 'appropriate due diligence and assistance' is not defined, other than to be taken in the context of the nature and context of the services being provided by affiliates.

These commercial issues surrounding agreement with sponsors are likely to mean that new entrants to the CDR system continue to face barriers to entry, and there will not be increased uptake. NAB considers the participation of affiliate-like entities could be better achieved through modifications to the existing CAP arrangements – under which the sponsor is not required to play such a significant role in the oversight and assurance of its affiliates.

In relation to the CDR representative model, the liability framework imposes additional liability on the principal which may make entering into representative agreements commercially unviable:

- A principal will remain responsible and liable for the actions of a representative, even where the representative's use or disclosure of CDR data occurs outside the scope of their arrangement.
- A failure by a representative to comply with the relevant privacy safeguard is deemed to have been a breach of the privacy safeguard by the principal.
- As contemplated by the wide ranging group of relationships permitted under the CDR representative model, a principal and representative could operate where the principal assumes responsibility and liability for the actions of a third party representative operating an independent system where it holder CDR data outside an accredited framework.

In practice, while these matters would be subject to commercial negotiation of indemnities between the parties, the additional burden on prospective representatives of having to provide indemnities to the principal may disincentivise the formation of these relationships.

Suggestions

In relation to the proposed participation models, NAB makes the following suggestions:

1. An independent threat assessment should be undertaken by a third party across the entire ecosystem, having in mind the proposed participation models. The risk assessment should consider and report on the risks to consumer's CDR data under these models. Subject to the outcome of this review, it may be appropriate for trusted advisors and outsourced service providers that are not accredited to operate subject to all of the Privacy Safeguards.
2. All participants in the proposed participation models should be subject to the full information security standards in the CDR. NAB notes for example that the CDR Rules v 3.0 does not specify any security standards for affiliates under the sponsored accreditation model. The security requirements for lower tiers of accreditation should be directly linked to the sensitivity of the CDR data the party will receive, and the functions the party will perform on behalf of consumers.
3. The liability structures under each proposed participation model should be made explicit – including as to consumer complaints and insurance. It should be explicit which party is responsible for the discharge of particular obligations (for example in the event of a data breach, which party is responsible for reporting the breach and notifying the customer).
4. Trusted advisors should be limited to classes of professions where there are sufficient professional obligations and oversight mechanisms, including: a professional accrediting

and supervising body, obligations as to due care and skill and to acting in the best interests of a client, obligations under privacy law, obligations as to ongoing professional education and training, and mechanisms for dispute resolution, consumer complaints and other disciplinary mechanisms for misconduct. NAB considers that persons admitted to the legal profession is an example of a class that meets these standards.

5. Reduce the obligations placed on accredited parties entering into relationships with non-accredited entities. In particular, under the CDR representative model, a principal should not be responsible or liable for any use or disclosure by the representative that occurs outside the scope of the representative's agreement (liability should rest with the representative in those cases).
6. Clarify the status of CDR data already held by affiliates under the sponsored accreditation model in the 4-month period in which the affiliate is without a sponsorship agreement.
7. Clarify the status of existing consents held by an ADR, where that ADR enters into a new sponsorship agreement with an affiliate – including whether the existing consents extend to the affiliate.

Sharing of CDR insights

As set out in previous submissions, NAB remains concerned that the sharing of CDR insights with non-accredited participants outside the CDR ecosystem may lead to consumer harm. For example, the categories of CDR insights set out in the CDR Rules v 3.0 around verifying a consumer's account balance, income or expenses, has the potential to include sensitive information. For example, data about a person's expenses may be used to identify a person's daily movement habits, health status and location.

NAB also considers that the addition of a CDR insight consent to the existing categories of consent further complicates a regime that is already complex to navigate. The term 'CDR insight' is not reflected in the definition of a CDR insight, which includes raw data. This is inconsistent with the purpose of the sharing of CDR insights, being to allow consumers to consent to the sharing of limited CDR insights outside the CDR regime for a prescribed purpose where those prescribed purposes are low risk. The proposed definition of CDR insight is likely to cause confusion. NAB considers that as further categories of consent are added to the CDR regime, it poses higher risk of consumer confusion and friction.

Commencement and transition

NAB is of the view that 1 April 2022 is not an appropriate date for transition to the new joint account rules. NAB is currently working towards the commencement of business account sharing rules for 1 November 2021, and there are tech-moratoriums in place in December / January. As such, NAB is unlikely to be able to commence work on the new rules before February 2022.

Based on the build time required for the existing joint account solution, NAB estimates that preparation for the commencement of new Rules 3.0 will require approximately 6 months. Work to be undertaken in this time will include completing the user experience, designing, building, testing, and implementing the technology solution, as well as customer migration from the JAMS to the DOMS. Technical assessments should drive delivery timelines, rather than pre-defined delivery dates. For this reason, NAB considers 1 September 2022 a more appropriate commencement date, including because it will provide enough time to educate joint account holders of the new rules.

In relation to the transition provisions for joint accounts, NAB considers a written notice period of 28 days is more appropriate than the suggested 7 days.