NATIONAL AUSTRALIA BANK SUBMISSION

Consultation on the exposure draft legislation to enable action initiation in the Consumer Data Right

October 2022

Introduction

NAB welcomes the opportunity to provide a submission on the exposure draft legislation to enable action initiation in the Consumer Data Right (CDR). As a member of the Australian Banking Association (ABA), NAB has also contributed to the ABA submission.

NAB has been actively engaged in the Government's consultation processes to date and this submission is in addition to previous submissions that NAB has made to Treasury regarding Open Banking and the CDR since 2017. In particular, we refer to NAB's submission to the Inquiry into the Future Directions of the CDR in May 2020, where we provided feedback in relation to the proposed inclusion of action initiation within the CDR regime. We have **attached** our former submission to this response, as much of that submission is still of relevance.

NAB acknowledges the benefits that action initiation could provide to consumers and the new, innovative use cases that action initiation could catalyse. We note that the inclusion of action initiation represents a substantial extension to the CDR regime. In NAB's view, trust in the ecosystem will be critical to the success of the CDR regime for the long term and with this in mind, NAB provides feedback focussed on ensuring the continued safety and protection of customers and participants within the CDR framework. In particular, we note the following areas in our submission which warrant further consideration: ensuring adequate protections for consumers and participants in the 'action layer;' the increased fraud and scams risk posed by action initiation; and a recommendation for clarity regarding the application of the Privacy Safeguards within an increasingly complex CDR ecosystem.

1. Protections in the 'action layer'

NAB welcomes Treasury's proposal to not regulate the performance of 'actions' by Action Service Providers (ASP), which are already subject to existing legislative regimes. We support Treasury's intent to avoid duplicative laws and infrastructure, where current frameworks are adequate and already address the specific risks associated with relevant 'actions'.

However, consideration should be given to the gap in the legislative framework if Accredited Action Initiators (AAI) are not governed by the same laws, rules and standards that ASPs are subject to. In particular, the risks associated with initiating payments, transferring funds or switching products, are high in banking use cases, as is the potential for consumer detriment.

Protection from liability is currently intended for participants that act in good faith and comply with CDR laws and rules. This is subject to regulations which could further specify other laws that protection from liability would not apply to i.e., Anti-Money Laundering (AML)/Counter Terrorism Financing (CTF) laws. As we have previously submitted[1], any model of payment initiation included in the CDR needs to satisfy consumer protection expectations, including enabling fraud prevention and detection, consent verification, unauthorised transaction recovery, and indemnification to the payer institution from the Payment Initiator.

[1] Please see NAB's Submission to the Inquiry into Future Directions for the Consumer Data Right (May 2020), page 4.

In NAB's view, clarity on liability and ensuring there are adequate protections for parties, including consumers will be critical to ensuring that participants have trust in the system and to ensuring the success of action initiation. We therefore recommend that it be made clear that AAIs will be subject to the same regulatory rules and standards which would apply to ASPs in the 'action layer.' We note that the exposure draft legislation proposes that AAIs must act 'efficiently, honestly and fairly' when initiating actions, and whilst this goes some way to addressing conduct of AAIs, we do not think this provision in and of itself will be adequate to fill the gap in regulatory guardrails that currently apply, particularly around the consumer protections associated with the provision of credit and lending.

In relation to payments, proposed Government reforms arising out of the Payment System Review could also be leveraged, such as requiring AAIs to hold a licence under a uniform licensing framework. We do not think that this will undermine the principle of regulatory overlap or regulation of the 'action layer,' rather it will ensure that there are adequate protections for consumers and guarantee the maintenance of a level playing field in relation to obligations and risk allocation for participants in the ecosystem. To this end, for example, we recommend that payment Initiation occur within approved payment frameworks (such as NPP), so that AAIs will be subject to the same due diligence processes, applicable rules, standards, and regulations that accompany initiating payments (and acting as a Payment Initiator) within these frameworks. Whilst some may contend that requiring AAIs to meet these standards could disincentivise participation as an AAI, NAB is of the strong belief that the risks to consumers and the overall resilience of payment infrastructure should not be subordinated to these views. Without accountability for all parties, the system will not have the level of trust required for it to succeed.

Further to the above, we recommend that the delegation of 'action types' be at a granular level as opposed to a macro level (e.g., the delegation of an 'NPP payment' rather than a 'domestic payment,' with the latter being too broad and potentially processed via a number of different rails, including legacy rails). We also recommend that a minimum consultation period be provided for such delegations.

2. Accreditation of AAIs and liability

Accreditation

In a write access and Payment Initiation model, Payment Initiators may not be ADIs, however, they will need to be suitably capitalised to ensure their ability to cover claims for unauthorised transactions. Financial institutions acting on Payment Initiations and consequently removing funds from customer accounts will need confidence that Payment Initiations are occurring under payment models or schemes that are robust, resilient and allow the financial institution to meet capital, risk exposure and regulatory requirements.

Therefore, we strongly recommend that the current accreditation standards and processes for ADRs be uplifted for AAIs who will act as Payment Initiators, particularly in relation to capital, insurance, cyber resilience and required authentication frameworks. We propose that the accreditation models be changed to create a higher level of accreditation for AAIs that are seeking to offer actions, such as payment initiation. As we have previously submitted,[2] from a regulatory perspective it would be prudent for APRA to have a

[2] Please see NAB's Submission to the Inquiry into Future Directions for the Consumer Data Right (May 2020), page 9.

greater involvement in the accreditation process for action initiation in the banking sector, as APRA will have the relevant expertise, including with regards to liability flows in payments. Similarly, given the risks associated with action initiation in the banking sector, we consider that certain models of accreditation (i.e., sponsorship and representative arrangements) would not be appropriate, as they would likely add unnecessary complexity and dilute governance and accountability.

Liability

As previously submitted[3], in payment systems where an instruction is created by the Payment Initiator (a third party to the payer whether on the payer side or creditor side), the Payment Initiator indemnifies the payer organisation for creating the payment instruction, i.e., liability shifts from the payer organisation to the Payment Initiator. Indemnification in the CDR as it stands is primarily concerned with data breaches and contains an element of 'buyer beware' on the part of the consumer and assumes adequacy of insurance on the part of the Accredited Data Recipient (ADR) to cover liability. To this extent, there is a gap in the protection afforded to consumers and other participants in the ecosystem. For example, if a particular AAI had an unacceptable level of unauthorised or disputed activity, there would need to be a mechanism to monitor, investigate and resolve this. Existing payment systems possess centrally managed frameworks for managing disputes, ensuring compliance with standards, and reporting fraud or scams. Therefore, as noted above, we recommend that AAIs be subject to these same obligations, rather than creating a bespoke framework which would result in potential inconsistency and duplication.

3. Fraud and scams risks associated with action initiation

Across a number of sectors, we are seeing increasing levels of sophistication in relation to fraud and scams, including social engineering and phishing attacks. These attacks are rising at an alarming rate. As previously submitted[4], NAB currently relies heavily on an in-depth understanding of the user, their behaviours, and their device through tools embedded in the way that customers choose to interact with NAB (e.g., internet banking and mobile applications). This understanding helps NAB to establish the fraud and financial crime risk that any user or their actions possess.

If third-party providers make applications on behalf of a consumer and where action initiation is decoupled from our platforms and systems, financial institutions lose the ability to collect and monitor the requisite data points to help protect customers and combat fraud and scams. Accordingly, we would strongly recommend that the data collected and shared with the receiving ASP (i.e., a financial institution) under write-access be expanded to enable more effective fraud and scams controls. Given the dynamic nature of the threats posed, there will need to be flexibility in relation to the types of information that financial institutions, in particular, will need to address this issue.

This will have implications for liability (i.e., if financial institutions do not have required information, then they cannot manage this risk or if the AAI does not have sufficient authentication controls, they will be

[3] Please see NAB's Submission to the Inquiry into Future Directions for the Consumer Data Right (May 2020), page 5.

[4] Please see NAB's Submission to the Inquiry into Future Directions for the Consumer Data Right (May 2020), page 8.

unable to ensure the legitimacy of the action initiation). This will also have implications on the proposals around the application of the Privacy Safeguards to ASPs, in particular Privacy Safeguard 3. We provide further comments on this in part 5 of this submission.

Due to the nature of the instruction layer, there is an increasing reliance on the AAI to ensure an adequate level of customer authentication is completed to guarantee the customer has genuine control of their account. Scams commonly prey on customers who lack understanding or are confused by the end-product they are consuming. An example of this is the recent surge in cryptocurrency investment scams, where consumers willingly hand full control of their portfolios to scammers. As stated in part 2 of this submission, we strongly recommend that the current accreditation standards and processes for ADRs be uplifted for AAIs who will act as Payment Initiators, particularly in relation to capital, insurance, insider threats, cyber resilience and required authentication frameworks.

It is likely that there will be organisations who look at the CDR system as overly onerous and burdensome and seek to utilise or create workarounds. These workarounds, such as tools which request customers to share the passwords to their personal accounts or banking platforms, have the potential to create excessive risk to consumers. Oftentimes, these encourage behaviours which can be preyed upon by scammers, ultimately impacting the trust of the system.

4. Charging models - fair competition and protection of end users

Under the current proposal, ASPs can only charge AAIs fees for processing an instruction received through the CDR if the Rules permit it, with the ACCC able to intervene if charges are too high.

A fundamental overarching principle of the CDR is the importance of ensuring a level playing field for all participants. As NAB has previously submitted[5], ADIs (acting as ASPs) should not be placed at a competitive disadvantage to benefit other industry participants. As ADIs will likely need to build additional technical infrastructure and processes, and there is the potential for increased risk to be borne by ADIs in enabling action initiation by intermediaries, we support the proposal permitting ASPs to charge a fee for processing instructions and recommend that this be built into the legislation, rather than being subject to the Rules.

Further, we note that in determining whether a fee could be charged it is proposed that consideration be given to various factors including whether performers of actions of that type currently charge fees for processing instructions to perform such actions. We note that this factor in and of itself may not be reflective of the commercial model underpinning the way in which fees are charged. For example, for large or business customers pricing for individual products might be offset by the broader relationship the customer has with a financial institution. As a related point, it is critical that customers who make changes to their facilities are aware of the potential impact these decisions could have, including flow on impacts to the services that they receive (i.e., where a switching decision may be promoted on basis of price, instead of a holistic offering, and features and benefits, such as access to an offset account in a home loan context).

[5] Please see NAB's Submission to the Inquiry into Future Directions for the Consumer Data Right (May 2020), page 2.

Lastly, we note that there does not appear to be a corresponding provision in the legislation which restricts or governs whether and how an AAI can charge a fee to a consumer in respect of initiating an instruction. This appears to be a gap whereby AAIs have carte blanche in relation to fees charged to consumers.

5. Application of the Privacy Safeguards to ASPs

We understand that under the proposed legislation, pursuant to Privacy Safeguard 3, an ASP would not be able to solicit additional CDR data outside the scope of an action type. It is proposed that the rules would specify what data is permitted to be shared with an ASP for different action types.

In our view, this needs to be considered in light of the fraud and scam risks raised in this submission and the fact that ADIs need to have a strong understanding about the behaviours around transaction initiation. Where an ADI, acting as an ASP, is disconnected from this process because actions are initiated through an intermediary, it will become extremely difficult for ADIs to monitor and protect customers against fraud and scams. Therefore, to the extent the intended scope of the operation of Privacy Safeguard 3 were to restrict or limit the kind of information that an ADI may seek to collect (whether directly from an AAI or indirectly) as part of performing an action, NAB strongly recommends that there be a carve out to allow ADIs to collect and share information reasonably required for purposes related to protecting against potential fraud and scams.

Additionally, we note that it is proposed that the Privacy Safeguards focus on the instruction layer. Whilst we consider that this should be the case, we think that as the ecosystem grows there is likely to be a level of complexity with entities performing multiple roles and therefore it will be important to have guidance around which legislative frameworks apply. For example, there may be scenarios where an organisation is acting both as an AAI and an ASP and in these scenarios there will need to be clarity that the CDR data that an ASP receives (which it may have also received as an AAI) will not be subject to the Privacy Safeguards (other than as has been proposed in the exposure draft). For example, Suzie wants to find a better deal on her mortgage. ABC Bank is an ADR and also an AAI. ABC Bank offers a product which compares different home loans in market and using Suzie's CDR data, with her consent, informs her that ABC Bank's Everyday Home Loan would provide her with a better deal. Armed with this information, Suzie consents to ABC Bank acting as her AAI to instruct her current provider, XYZ Bank to close her current home loan account and also instruct ABC Bank to open an Everyday Home Loan account. In the current example, ABC Bank is acting as an ADR, AAI and an ASP. In opening the account for Suzie, ABC Bank is acting in its capacity as an ASP, however, certain CDR data that ABC Bank collected as an ADR or AAI in this example may be the same information that ABC Bank is provided/collects to perform the action. Therefore, it will be important to ensure that it is clear that the information which ABC Bank collects and uses in its capacity as an ASP to open Suzie's account would not be subject to the Privacy Safeguards (other than as specifically referenced in the exposure draft legislation).

Related to this, we note that currently if an ADR that is also a Data Holder (DH) collects data as an ADR (for example to open a new account), an ADR can only hold that data as a DH with a consumer's consent.[6] For many ADRs that are also DHs, this is an inhibitor to the development of CDR powered products, as significant work in modifying downstream systems is often needed to account for the regime requirements. From a policy perspective, there is benefit in aligning the current rules to the proposed intention (which we support) to not regulate the action layer, such that DHs could hold product application data as a DH, without having to rely on the current mechanism in clause 7.2 of Schedule 3 in the CDR Rules, which appears to have limited scope and utility.

6. Digital Identity

As the CDR expands to encompass action initiation, there will be an increased need for stronger customer authentication. As NAB has previously submitted[7], digital identity has the potential to support the CDR infrastructure. Digital identity has broader use cases beyond CDR and therefore NAB supports a policy of ensuring interoperability with existing initiatives, including public and private sector digital identity schemes. For example, the ConnectID initiative (which NAB is supporting[8]) is intended to form part of an integrated, interoperable ecosystem, where consumers are empowered to select their preferred authenticator and issue their consent for specific identity attributes, engaging across the private and public sectors. We would strongly recommend that any authentication frameworks which might be embedded in the CDR adopt an open-standards approach which would help to future-proof the CDR and support the uptake and acceleration of digital identity.

7. Other issues

We note that the proposed legislative framework does not seek to regulate the action layer. The framework would regulate the instruction layer, which is made up of the activities associated with consumers sending instructions for the performance of actions. Whilst we support the intent not to regulate the performance of actions which are already subject to regulations, we query whether the distinction between an instruction and action layer can always be neatly drawn and whether in some cases the two may be interrelated. It may be the case that these issues can be dealt with by very clear definitions within the relevant CDR Rules framework.

There also appears to be a potential risk in the proposed legislation that an AAI could, depending on the circumstances, potentially be construed as an 'agent' of the relevant end user customer, where they are engaging on behalf of a customer. The potential relevance of this from an AML perspective is that where an ADI deals with a customer's agent, there are some Know Your Customer (KYC) obligations, which, depending on the circumstances, can apply in relation to the agent. Noting that the Bill that would facilitate the proposed extension to the CDR regime is currently in draft form, and draft Rules that would support the

[6] Please see clause 7.2 of Schedule 3 of the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth).

[7] Please see NAB's Submission to the Inquiry into Future Directions for the Consumer Data Right (May 2020), page 5.

[8] Please see NAB Media Release: 'NAB backs ConnectID to help customers secure their identity - NAB News' https://news.nab.com.au/news/nab-backs-connectid-to-help-customers-secure-their-identity/

regime are not yet available, NAB does not presently have a view on whether such obligations will or could arise in connection with the proposed extension to the CDR regime. However, we suggest that this issue be specifically considered when further developing the proposed legislation (including the Rules) and that the proposed legislation (or Rules) make it clear that the AAI is not operating in the capacity of a consumer's agent for the purposes of AML/CTF laws.

Finally, we note that the draft legislation does not consider multiple consents where multiple parties are involved (e.g., for joint accounts). We recommend that clear requirements are defined for multi-party situations within the relevant CDR Rules framework.

Conclusion

NAB is appreciative of the opportunity to contribute to the policy development of the CDR and the expansion of the regime to action initiation, which builds on our submissions on the subject to date. We look forward to ongoing engagement with Treasury.