Australian Banking Association

24 October 2022

Future Directions Unit
Consumer Data and Digital Division
Treasury
Langton Cres
Parkes ACT 2600
By email: data@treasury.gov.au

Consumer Data Right - Exposure draft legislation to enable action initiation

The Australian Banking Association (**ABA**) welcomes the opportunity to comment on Treasury's consultation on the Consumer Data Right (**CDR**) – Exposure draft legislation to enable action initiation.

Recent, significant cyber security incidents and the compromise of millions of customer records have highlighted the cyber risk environment and made Australians more cautious about the safety and security their data. As a result, ABA member banks are significantly concerned about the potential risk implications for consumer and small business data and financial information.

Ahead of the expansion of the CDR through action initiation, the ABA encourages the Government to carefully consider and address the scams, fraud and cyber risks, while the CDR is still in its early stages. Now is the time to ensure regulatory settings prioritise the protection of consumers.

It is critical that the safety and security of the CDR ecosystem is retained and strengthened, and that a careful consideration of the phasing of the rollout of action types based on use value, risk and complexity is undertaken.

To this end, the ABA makes some recommendations to protect customers, and ensure a strategic approach to the implementation of CDR action types:

1. The legislation should not restrict banks from applying and uplifting scam, fraud and cybersecurity measures
2. A strategic assessment should be conducted ahead of declaring any actions
3. Payment initiation needs to align with broader payments work
4. The Government should allow further time for the CDR to mature, bed down CDR sectoral implementations and ensure extensive consultation before declaring actions.

Key recommendations

1. The legislation should not restrict banks from applying and uplifting scam, fraud and cybersecurity measures

As more Australians experience scams, frauds and cyber-attacks, banks are actively working with regulators, conducting awareness campaigns and building a range of sophisticated detection tools to pick up on unusual behaviours in close to real time to stop suspicious transactions. By the engagement of a third party standing in the shoes of the customer, action initiation potentially introduces a range of new risks for which banks may need to develop specific scam, fraud and cyber mitigation tools.

While accreditation, the rules and standards can assist in reducing some risks, the draft legislation appears to open the door to actions carrying high risk (e.g., payments), while limiting the ability of banks as Action Service Providers (**ASP**s) to address them. This is in the context of the need to rapidly increase the maturity and scale of such preventative measures and the growing number and complexity of scams, frauds and cyber-attacks.

Under s 56BZC, ASPs "must perform a validly requested action in relation to a CDR consumer if, having regard to criteria to be set out in the consumer data rules, they would ordinarily perform actions of that type in the course of their business in relation to that consumer."

The Explanatory Memorandum (EM) notes that "this is not intended to prevent an ASP applying extra security or other checks to CDR action requests on the basis that a third party is involved, provided it is consistent with existing practices. Businesses are also still allowed to refuse to perform an action, provided they do not discriminate against instructions that come through the CDR."

While helpful, we note that the CDR law should not force ASPs to comply with any instruction, just as they are not compelled to act on any customer instruction where they have concerns over the risks of that instruction. The phrase "existing practices" seems to limit the ability of banks to apply fraud protections to current and not newer or additional measures in the future. Also, the phrase "provided they do not discriminate against instructions that come through the CDR" does not recognise that CDR action initiation can have its own risks that need to be assessed and possibly addressed through specific measures.

As an example, involving a third party in the place of the customer will mean the loss of some visibility of the customer through behavioural data such as the device used, the IP address of the customer and the time and date of the instruction. Such markers may be used to reduce fraud and cyber risks, potentially on a close to real time basis, and with a third-party instruction a source of behavioural data could be lost or not be available in a form that can be used by the bank. Given this, banks will need to assess the risk profile of those instructions and potentially develop new solutions specific to addressing the risks that may be posed by CDR actions.

The ABA recommends clarifying s 56BZC to explicitly enable ASPs to refuse to act on a request if it does not meet the ASPs scam, fraud or cyber risk appetite. For example, ASPs should be able to set a transaction limit on CDR payment instructions and should be able not to perform actions above that limit, if they assess the risk of such payment channels warrant a higher degree of protection. Furthermore, banks should be able to refuse an instruction where they detect or determine an elevated risk to their customers and/or have not received confirmation from the customer of an instruction, and this should be made clear in the law.

2. A strategic assessment should be conducted ahead of declaring any actions

Before declaring any action type, the ABA recommends a full strategic assessment and a cost/benefit analysis be undertaken by Government to determine whether the cost of building for an action type is outweighed by the consumer benefit. Work should be undertaken to understand potential use cases, the scams, fraud and cyber risks, the utility to customers compared with alternative options, and the regulatory or technology barriers that need addressing ahead of implementing any action type.

Even for the most viable or valuable use cases such as payments initiation, this assessment should be conducted to understand the merits and timing of implementation to ensure a cohesive policy approach.

Other use cases such as opening and closing accounts should also be examined with the lens of utility value compared with current or alternative methods. For example, many action types may require other technology developments such as digital ID, and others may require changes to other legal frameworks such as AML/CTF laws. Where these intervening requirements add friction to the process and deliver a poor customer experience, it may not be worthwhile to pursue those actions.

Finally, we note that the strategic assessment should take stock of developments overseas and consider the learnings from jurisdictions such as the United Kingdom and the European Union ahead of finalising the policy specifications.

3. Payment initiation needs to align with broader payments work

In addition to a strategic assessment of the broader CDR environment, further work is required for some action types such as payment initiation. For example, ahead of declaring payment initiation there should be an analysis of the interlinkages with the Payments System Review recommendations on strategy and licensing, and the timing of payment initiation should consider these developments.

In particular, Accredited Action Initiators (**AAI**) accreditation should align with the payments licence, and there should be clearer co-ordination on standard-setting so that there are harmonised requirements between AAIs and Payment Services Providers (**PSPs**). The license should also ensure a fit-for-purpose liability framework that clarifies circumstances where AAIs are liable for consumer losses.

Payment initiation should also align with the PayTo implementation roadmap, and accreditation for AAIs align with the requirements for third-party payment initiation under the New Payments Platform. We note that utilising PayTo to execute CDR payment initiation instructions may provide an effective and efficient way for ASPs to meet their obligations while resolving some key issues raised above on liability. For this reason, we consider CDR payment initiation should be enabled once PayTo has been implemented and reaches some level of maturity.

4. The Government should allow further time for the CDR to mature, bed down CDR sectoral implementations and ensure extensive consultation before declaring actions.

The CDR is yet to mature, and there are several sectors that are either being progressed for designation or still implementing their compliance obligations as data holders. Use cases are still developing, and customer usage is still low. Research has found that only 18% of consumers feel comfortable sharing data,[1] and we suggest far fewer would be comfortable with third parties initiating actions on their behalf using shared data. This is understandable, given recent cyber security breaches.

In this context, moving quickly can mean consumers are more hesitant to use CDR action initiation, and are likely to be more exposed to higher risks if security and fraud risks are not well considered, resulting further in less trust and less use of the CDR.

The ABA considers the CDR needs more time to grow naturally, and that increasing functionality at this stage may not result in more customers using the CDR. On the contrary, adding these functionalities without allowing the market a level of stability to enable use case development could impede the development of a competitive market for use cases.

Adding action initiation in the near term may also compromise the intended outcome by adding considerable strain on finite resources and staff.

In light of these factors, the ABA recommends the government allow a period of at least 18-24 months ahead of declaring actions for implementation. During this period, work can be undertaken to implement a strategic assessment, support businesses to meet existing and new compliance obligations, build customer awareness and trust, and allow the CDR to mature.

Thank you for the opportunity to provide feedback.

Yours sincerely,

Prashant Ramkumar
Associate Policy Director,
Australian Banking Association

[1] Zepto Consumer research. Source: https://australianfintech.com.au/open-finance-more-than-half-of-australians-not-comfortable-sharing-their-data-to-access-better-deals/