Australian Banking Association

6 March 2023

Senate Standing Committees on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

By email: economics.sen@aph.gov.au

Treasury Laws Amendment (Consumer Data Right) Bill 2022 – Senate Economics Legislation Committee Inquiry

The Australian Banking Association (**ABA**) welcomes the opportunity to comment on the Economics Legislation Committee's (**the Committee**) – inquiry into the Treasury Laws Amendment (Consumer Data Right) Bill 2022.

We would like to bring to the Committee's attention that the ABA provided its submission to Treasury on action initiation, dated 24 October 2022, for its consultation to the Consumer Data Right - Exposure draft legislation to enable action initiation. This is included as an attachment (Attachment A) to this submission for the Committee's consideration and review.

Our Views

Feedback from our Members remains consistent with what was submitted to Treasury in October 2022. Therefore, we wish to reiterate key summary comments in both the following bullet points and paragraphs from the same submission, while raising additional member feedback from recent industry working groups.

- Legislation should ensure that banks can continue to use existing and future technologies to protect consumers from fraud, scams, and cyber-attacks.
- Align the implementation of action initiation to Treasury's Strategic Plan for the payments system, particularly having regard to the proposed new payments licensing regime.
- New payments licensing regime to clearly define liability across participants.
- Apply a maturity period for CDR read access to embed before implementing action initiation.
- Phased implementation of payments action initiation based on each payment type's risk profile. *(**Recent Member feedback**).*
- To the extent feasible, recognition of the recent review of the *Privacy Act 2001* (Cth) and the Government's recommendations, to ensure the Privacy Safeguards that underpin CDR are sufficiently fit for purpose under an action initiation framework. *(**Recent Member feedback**).*

Bill limits banks' ability to implement necessary anti-scam and cyber security protections

As noted in our 24 October 2022 submission to Treasury, the ABA is concerned that the unamended drafting of s56BZC may inappropriately limit the ability of banks to apply critically important anti-scam, fraud, and cyber security protections to transactions initiated through CDR.

The Explanatory Memorandum (**EM**) provides some reassurance that s56BZC *"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."*

Australian Banking Association

However, the phrase *"provided they do not discriminate against instructions that come through the CDR"* suggests that banks are unable to identify any risks particularly associated with a CDR action initiation request and develop appropriate safeguards and mitigants tailored for those risks.

For example, third-party initiated payments may not include existing behavioural markers, such as device information, IP address, transaction date and time, used by banks to combat against scams, fraud, and cyber-attacks.

While recognising that anti-scam and cyber precautions should not be applied unnecessarily, the apparent prohibition on identifying and managing risks unique to CDR transactions creates the potential for CDR action initiation capabilities to have a lower level of anti-scam and cyber protections than the equivalent non-CDR transactions.

In light of this, the ABA recommends that s56BZC should be amended to provide certainty that the obligation to carry out a valid CDR action request does not exclude necessary and appropriate anti-scam and cyber security checks and precautions (as they evolve over time) and ensure an equivalent level of security as a non-CDR transaction.

Restatement of other recommendations from October 2022 submission

In our October 2022 submission, the ABA recommended:

- prior to implementing action initiation, that the CDR read access framework reach a sustained level of maturity and that designation of payment actions should be timed with completion of the Treasury's Strategic Plan for the Payments System. Specifically on a payment licensing applicable to **Accredited Action Initiators** (**AAIs**) and **Payment Service Providers** (**PSPs**), to clearly establish liability to AAIs where customers incur losses.
- the need for alignment between Treasury's payment licensing regime, and the accreditation of AAIs, who will also be regulated in the payments space, as overseen by the Australian Competition and Consumer Commission's (ACCC).

Recent developments

Members have proposed action initiation, specifically payments, be implemented across different phases. This would be similar to the implementation of Phases 1, 2, and 3 of banking products when data sharing (**read access**) was phased in. This phased implementation could be staged with lower risk-based payment products first available for action initiation, followed by higher risk-based products reserved for future implementation. This would provide the industry more time to learn from the phased implementation, potentially limit risk exposures, while also presenting an opportunity to better monitor scams and fraud, and to develop safeguards for existing and future phases.

Members have raised uncertainty on the additional compliance requirements that will likely crossover to action initiation brought on by the recent Privacy Act Review (**Privacy Review)**. The industry is still reviewing the key recommendations of the Privacy Review and will participate in consultation with Government on the several proposed reforms. During which, the industry will develop greater awareness when designing and building these requirements into the CDR action initiation.

Members have sought clarity that this Bill does not impose new obligations on how the action layer is performed. We note section 1.14 of the EM states that CDR and its expansion to action initiation does not alter how the 'action layer' operates. We suggest that this could be clarified by modifying the sentence to state that the Bill does not impose new obligations on how the action layer is performed, without reference to "alter".

Australian Banking Association

Closing Comments

In closing, the ABA again recommends the Government ensures that the implementation of action initiation aligns to the broader agenda for reform of the payments regulatory framework.

In the interim, work could be undertaken to conduct a strategic assessment, support ecosystem participants to meet existing and new compliance obligations, and build customer awareness and trust of the CDR.

To maximise regulatory efficiency, we further recommend that the outcome of the Privacy Act review and other proposed amendments to the Privacy Act are considered before settling revisions to the Privacy Safeguards in the Bill.

Thank you for the opportunity to provide feedback, and please do not hesitate to contact me, if you require further information at,

Yours sincerely,

Christos Fragias

Policy Director,

Australian Banking Association

Australian Banking Association

Attachment A: ABA's submission to Treasury's Consumer Data Right - Exposure draft legislation to enable action initiation.

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

Australian Banking Association

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

Australian Banking Association

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/