Australian Banking Association

28 October 2019

Katherine Armytage - Partner
Caroline Atkins - Partner
Maddocks
Level 1 Maddocks House
40 Macquarie Street
Barton ACT 2600

By email: cdrpia@maddocks.com.au

Dear Katherine and Caroline,

Treasury consultation on Open Banking Privacy Impact Assessment (PIA)

The Australian Banking Association (ABA) welcomes the opportunity to contribute to the development of the PIA for the Consumer Data Right (CDR) regime. Further, the ABA is appreciative that the Department of Treasury has responded to stakeholder feedback through its appointment of an independent party to undertake this PIA. The Maddocks process has been welcomed by the ABA for its open and collaborative approach.

Given the significantly advanced state of the design of the CDR regime, this PIA remains an opportunity to critically and rigorously assess the privacy impacts of Open Banking on participating Australians. The ABA appreciates that set timeframes for delivery of both the PIA and the regime are ambitious. However, the ABA requests that identified privacy risks which are inherent in the design of the CDR regime are addressed and mitigated prior to the regime being launched.

This submission is structured as follows:

Section 1 identifies ABA concerns and points for further investigation in respect to the methodology adopted in undertaking the PIA. In particular, the ABA notes that given the point-in-time nature of the PIA, that a regular scheduled privacy assessment of the CDR regime be incorporated into the Department of Treasury's work schedule.

Section 2 provides specific feedback on the recommendations and risks analysis contained within the PIA.

The ABA would be pleased to provide further explanation of the comments and recommendations contained within this submission. Should you have any questions please do not hesitate to contact me.

Kind regards

Emma Penzo

Policy Director

(02) 8298 0417

Emma.Penzo@ausbanking.org

Australian Banking Association

1. PIA Methodology

1.1 A point in time review

The ABA appreciates the undertaking of a revised Consumer Data Right (CDR) Privacy Impact Assessment (PIA) to assess developments in the establishment of the CDR regime. This is particularly timely with the formalisation of the CDR regime's Rules[1] and the Data Standards[2] since the initial PIA was undertaken.

The ABA notes the statement that this PIA is a point in time review and that it ought to be treated as a "living document" (p6). The ABA believes that the PIA process would benefit from prescheduled ongoing reviews the timing of which is not subject to external triggers (such as changes in the law). Further, the ABA notes that the PIA suggests that 'further legislative reforms are unlikely to be a viable option for enhancing privacy in the short-term' (p68). Whilst the ABA appreciates the fact that the ***Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth)*** (the CDR Act) has passed and received royal assent, to the extent that further legislative changes are warranted to mitigate privacy risks, the ABA suggests that legislative change should be pursued.

Generally, the PIA does not consider the adequacy of the testing and assurance framework to mitigate the privacy risks, nor does it address the detailed nuance of the Rules and the Standards. These concerns are discussed in later sections in more detail.

The ABA highlights that previous versions of the PIA outlined the 'severity' and 'likelihood' of potential privacy risks. This risk taxonomy is missing from the September release. Following the approach of the previous versions would have allowed for more fulsome consideration of the impact of the risks.

1.2 CDR Rules

The ABA notes that the PIA does not assess the privacy impact of the Rules. The ABA would expect that there would be an assessment of the privacy risks associated with or arising in connection with the Rules as part of the PIA, particularly given the fact that much of the detail associated with the mechanics of the CDR is set out in the Rules.

Note for example, that Rule 7.2(5) currently requires a description of de-identification techniques used in an entity's CDR policy. ABA member banks would like to understand whether the security implications of this requirement have been considered. The ABA queries whether requiring the disclosure of de-identification techniques increases privacy and security risk to consumers, thereby enabling bad actors to more readily employ techniques to re-identify data sets.

The ABA would also welcome clarity regarding the treatment of "redundant data" in the Rules. In particular the ABA seeks guidance on the intent behind the introduction of the concept of 'deletion' and the ability for consumers to elect for deletion (which appears to be a lower standard than destruction as required by Privacy Safeguard 12). Further, the PIA does not seem to address the risk that 'redundant data' is de-identified and then accidentally used for commercial purposes (without consent).

1.3 CDR Data Standards

The Data Standards are the detailed specifications required to build and implement the CDR ecosystem. Therefore, it is an important element to consider as part of the PIA. As a point in time document, the PIA does not reflect the most recent baselined Data Standards issued by Data61, '*September 2019 Release of Consumer Data Standards V1.0.0'*.

Recommendation: The ABA strongly recommends that, in the course of finalising this PIA, there is a more granular review of the latest Data Standards (and specifically identify which version of the Standards have been considered) in order to ensure that the correct sequencing of information flows is representative of the Data Standards (e.g. the registration of an ADR is a pre-requisite to seeking

[1] the Competition and Consumer (Consumer Data Right) Rules 2019
[2] Consumer Data Standards as published by the Data Standards Body

consent as this is not represented as in the draft PIA report). This would also ensure that associated key risks in the information security system are identified.

Further, the ABA recommends that the PIA consider privacy impacts considering the security threats identified in the CDR Security Review performed by Fortian for the Data Standards Body. A review of the report by Fortian may provide deeper insights into the risks arising from the information flows, in particular:

- #OBS-10 Consent – deep access to data (p41)
- #OBS-11 Consent – rich access to data (p41)

ABA members seek clarification that the next PIA will be completed when the Rules and the Data Standards are finalised as this is not noted to be a trigger under Recommendation 1 of the draft PIA Report.

1.4 Non-individual consumers

The CDR regime and its privacy safeguards apply to the data of both individual and non-individual consumers. The PIA has not considered privacy issues for non-individuals despite non-individuals being able to share their data under the CDR regime. The PIA should address privacy risks associated with the CDR regime as a whole.

2. Feedback on specific sections

Whilst the ABA is broadly supportive of the recommendations made in the PIA, in this section the ABA notes areas that would benefit from additional review.

2.1 Part B: Executive Summary

2.1.1 Recommendation 1

This recommendation is consistent with OAIC's '*Guide to undertaking privacy impact assessments*', which recommends that "the PIA should be revisited, and updated or revised if developments in the design or implementation of the project create new privacy impacts that were not previously considered" (p34). Further, in terms of the trigger to update the PIA, the ABA notes that the Department of Treasury is subject to a requirement under the '*Privacy (Australian Government Agencies – Governance) APP Code 2017*' to conduct a PIA for high privacy risk projects.

The ABA views any changes to the CDR regime as likely to have a significant impact on the privacy of individuals, thereby warranting reconsideration of the risks and recommendations made by the PIA. This review process is crucial to ensuring that the CDR regime will meet its stated goal of being 'consumer focussed'.

2.1.2 Recommendation 2

The ABA supports recommendation 2 and notes that the OAIC have recently released draft guidance.

The CDR regime will introduce a new set of obligations in the Privacy Safeguards, which will either supplement or co-exist alongside the Australian Privacy Principles (APPs), depending on whether the entity is a Data Holder or an Accredited Data Recipient. The ABA agrees that there is a substantial risk that CDR consumers, as well as Data Holders and Accredited Data Recipients, will not understand the co-operational nature of the Privacy Safeguards and the APPs and that therefore the implementation of the privacy obligations may not occur as intended.

Recommendation: To mitigate this risk, the ABA recommends that the relevant regulators produce a comprehensive suite of guidance, addressing all the areas identified in Recommendation 2. In addition, the ABA also recommends that guidance is produced to provide clarity on the following questions:

- How does the data minimisation principle apply in practice? Do the same relevant considerations in determining whether a collection is 'reasonably necessary' under APP 3 (as outlined in paragraphs 3.17 – 3.21 of the APP guidelines) apply to CDR data?
- What relevant considerations apply in determining whether the key elements of consent are met? Where these elements overlap with the OAIC's existing guidance on consent, will the APP guidance apply to the CDR regime?
- How will the OAIC and ACCC approach CDR regime complaints? The ABA recommends that the *OAIC's Guide to Privacy Regulatory Action* is updated to incorporate the intended approach, including the difference between how complaints will be handled by the OAIC and the ACCC.
- How will the CDR regime address scenarios where a Data Holder has a concern about a Data Recipient's information handling practices? In particular, the ABA would like to see guidance in respect to the grounds to refuse disclosure. The provision of examples and a discussion on where these might apply would be helpful.
- What steps are needed to be taken to ensure that CDR data is appropriately handled in CDR outsourcing arrangements? It is especially important that regulator guidance addresses this question, given that Accredited Data Recipients will retain responsibility for any uses or disclosures that occur in these arrangements.
- Further guidance will be sought from the OAIC on the prohibited uses of CDR data as specified in ACCC CDR Rule 4.12 (3)(b) which prohibits the aggregation of data for the purpose of identifying, compiling insights in relation to or building a profile in relation to any identifiable person who is not the CDR consumer who made the CDR request. For example, would this prohibition include the application of insights gained from aggregated (and de-identified) data to an identifiable person who is not the CDR consumer?

2.1.3 Recommendation 3

Recommendation 3.1: Data Holders collect personal information from customers and keep it secure from unauthorised access and misuse in accordance with the Privacy Act. In addition, ADIs are highly regulated and have additional security obligations in relation to information assets, including under CPS 234. Paragraph 26.6 of the draft PIA Report acknowledges the existence of the two privacy regimes and that the intent of the CDR regime is not to replace the current Privacy Act regime. Therefore, the review of the CDR regime should not be a review of the adequacy of the Privacy Act, as is the implication of Recommendation 3.1.

Recommendation 3.3: To the extent that Recommendation 3.3 of the draft PIA Report is adopted, the ABA seeks guidance and examples from the OAIC on what form these disclosures will take.

Recommendation 3.7: The recommendation is not necessary. A technical mechanism, called the revocation endpoint, is already in-place to enable notifications between Data Holders and Data Recipients when authorisation is withdrawn. And vice versa when consent is withdrawn on the Data Recipient's side.

2.1.4 Recommendation 5

The ABA strongly supports Recommendation 5 of the draft PIA Report. The ABA further notes that the Data Standards will continue change on a frequent basis and that there is currently an absence of adequate version control around updates to the Data Standards. For example, the change log on the Data61 Data Standards and ACCC Registry API standards website is inconsistent in the level of detail specifying changes made to data standards and does not enable easy identification of changes. This presents a risk to consistent implementation of the Data Standards across all participants.

Recommendation: The ABA recommends the implementation of adequately detailed version controls.

The definition of 'optional' v 'mandatory' is not clearly defined and understood in the Data Standards. Both 'optional' and 'mandatory' fields are required in the Data Standards but an 'optional' field may return an empty string where the Data Holder does not have the required data.

This approach is confusing. A 'mandatory' field should refer to a field that requires a response. Where the data is required but not held by a Data Holder, an empty string or error could be returned in a valid response. 'Optional' fields should refer to data fields that a Data Holder may provide at their discretion. The latter category would extend in future versions to potentially chargeable data fields that may not be held by all Data Holders or standardised across the industry.

2.1.5 Recommendation 6

The ABA supports this recommendation and adds that this topic be subject to formal regulator guidance.

2.2 Part C: Methodology

The draft PIA at 8.17.2 notes that is it not a privacy impact assessment of *'the internal design or operation of the Accreditation Register or the ACCC's broader ICT system for the CDR regime'.* The Register is a key piece of regime infrastructure which provides the physical checks and controls to protect against rogue and unauthorised access to the CDR regime and therefore serves to protect CDR consumers against rogue and unauthorised use of CDR data. The ABA does not consider that a PIA can be finalised without a detailed review of the internal design and operation of the Register.

For example, the draft PIA does not address privacy risks associated with the unavailability of the CDR Register.

The current ACCC CDR Register API standards propose that:

- participants will continue to operate until their metadata caches reach a maximum age.
- consumer data will not be shared once the maximum age is reached
- and once the CDR Register becomes available, all participants will receive a refresh cache notification.

Under this scenario, there is a risk that a Data Recipient's accreditation could have been revoked or suspended immediately before the CDR Registry becomes unavailable and the Data Holder continues to share data as the Data Holder is required to continue operating on outdated cached data which does not reflect the Data Recipient's revoked status. Similarly, the risk of the Data Holder being required to share with a Data Recipient without a valid accreditation will arise if there is an information security threat to the CDR Registry, the CDR Registry becomes unavailable and communications are not possible, for example, in a denial of service attack.

Recommendation: The ABA recommends reviewing risks around the unavailability scenarios and mitigating strategies, as part of analysis in Part G, Step 6, No. 2.

2.3 Part E: Fundamental concepts

Division 5 of the *CDR Act* provides under:

- Section 56 EB that:
    - Privacy Safeguards only apply to CDR data for which there are one or more CDR consumers.
    - The Privacy Safeguards apply to CDR data whether the CDR data is true or not.
- Section 56 EC sets out how the Privacy Safeguards interact with other laws. Specifically, subsection (4) regulates the interaction of the Privacy Safeguards with the APPs.

While valid consent is required to trigger the CDR, once that right is triggered the protections apply as a matter of law. That is, the protections of the Privacy Safeguards are immutable and not the subject of consent. They cannot be qualified by that consent or any subsequent modification/qualifications.

Recommendation: The ABA recommends a review of the PIA draft to ensure that actual or inferred commentary suggesting that the Privacy Safeguards can be qualified be removed from the document.

2.4 Part F: Analysis of APP application and compliance

Generally, the operation of two privacy regimes creates complexity and the potential for confusion for both organisations subject to the APPs and Privacy Safeguards (PS), as well as for consumers in understanding their rights and protections. Clear guidance must be provided to ensure that the right consumer outcomes are achieved.

Obligations**	Risk/issue
PS 1, APP 1, PS 5, and APP 5	While the ABA appreciates the importance of providing consumers with transparent information, there is a risk that the duplication of policies – and, in particular, the inability for privacy policies and CDR policies to be combined – could contribute to information overload and fatigue, and overall does not provide a simpler customer experience. In 2018, the Consumer Policy Research Centre found that only six per cent of respondents read the privacy policies for products.
PS 4 and APP 4	The PIA has correctly noted that PS 4 requires the destruction of unsolicited information, which is a standard higher than APP 4, where unsolicited information can be destroyed or de-identified. However, there is a risk that the Data Holders (banks) may not be able to meet this higher threshold in situations where it is not technically feasible to irretrievably destroy the relevant CDR data. The OAIC currently provides for destruction where information is 'put beyond use', and the ABA would prefer to see a similar provision apply for the destruction of CDR data under PS 4.
PS 8 and APP 8	The ABA notes that while PS 8 and APP 8 are broadly consistent, there are several issues with the application of APP 8. There is a lack of guidance in respect to what constitutes a similar 'law or binding scheme' which is likely to exist for PS 8 as well. This raises risks for the cross-border disclosure of data and limits the ability to legitimately transfer data across borders. **Recommendation**: The ABA recommends that regulator guidance addresses this issue and provides guidance on when the other exceptions in PS 8 will apply.
PS 10	PS 10 requires that Accredited Data Recipients take steps to notify CDR consumers about disclosures of CDR data, however, as the PIA identifies no such steps have been identified in the Rules. **Recommendation**: The ABA recommends that guidance is provided as to what constitutes 'reasonable steps'.

** In this table: **PS** refers to the CDR regime Privacy Safeguards; **APP** refers to Australian Privacy Principles

2.5 Part G: Analysis of risks associated with information flows in the CDR Regime

2.5.1 Testing of the Regime

The ABA recommends that the references to industry testing as a mitigating strategy for various risks in Part G be reviewed in closer detail to ensure alignment to the current planned regime testing, as developed and overseen by the ACCC, and to assess whether the mitigating strategies are sufficient.

Given that the success and safety of the system is dependent on all participants being compliant, if a test of compliance against Data Standards is expected the ABA recommends the test be applied uniformly to all participants in the CDR ecosystem.

The ABA also recommends security testing of all interactions between participants in the CDR ecosystem.

The ABA seeks clarification as to whether ongoing regime testing (in whole or in part) is a requirement under the Rules, and if it is a pre-requisite for accreditation and an ongoing requirement when the CDR regime is operational under Open Banking.

2.5.2 Ongoing monitoring and enforcement by the regulators

The ABA supports the reference in Part H that the regulators will have a critical role to play in ensuring that privacy risks are addressed through the provision of guidance, educational material, and the implementation of effective ongoing monitoring and enforcement.

Recommendation: The ABA recommends that more detailed reference to the appropriate use of these controls is made throughout Part G of the PIA Report.

2.5.3 The journey of data

In several instances, the PIA relies on the Customer Experience (CX) guidelines, which are being developed by Data61, to mitigate a privacy risk. Generally, customer experience (which usually addresses useability and accessibility) will not be appropriate controls to privacy risks emerging from poorly designed standards or processes. Further, customer experience guidelines are limited in their effectiveness as they address in-flow education. A broader-scale consumer education program should be undertaken to ensure consumers are appropriately informed about the risks and protections of data sharing using the CDR regime and Open Banking.

Further, the PIA does not fully consider the ways in which the Data Standards (and Registry standards) can reduce or amplify privacy risks. For example, *step 1B – Risk No 2* refers to the risk that a CDR consumer may be asked to provide consent which is too broad to be a valid consent. The mitigants refer to Rules requiring consents to be 'specific', 'informed', and the data must be required to provide the requested good or service. They also refer to the CX guidelines to assist consumers in comprehending consent. These are not entirely satisfactory mitigants as the true risk mitigants occur in the way in which the standard has been designed, the PIA does not investigate to this level of detail. In the example being discussed, the PIA does not consider the ways in which authorisation scopes have been designed in the technical standards and the decision not to include a consent API.

Risk Number	Risk outline	Comment
Step 0 – Risk No. 4	A CDR consumer requests a Data Holder to destroy/de-identify their CDR data	Paragraph 26.2.1 notes that this step 'occurs in the ordinary course of the Data Holder's business and before any request is made by the CDR Consumer for access to their CDR Data.' (p67) There is no CDR data at this point in the process and therefore the ensuing analysis confuses the nature of the data. The risks identified on the Data Holder are not true risks for the CDR regime. The APPs do not currently afford individuals with a right to erasure, so this risk does not present a gap. However, it will be important that CDR consumers understand the protections that do/don't apply to their CDR data.
Step 1B – Risk No. 1	Consent given by CDR consumers is not voluntary	The PIA notes existing mitigation strategies (Rule 4.9 requires that consent be express and voluntary) but does not make any additional recommendations. **Recommendation**: The ABA recommends that guidance is provided on what constitutes 'voluntary' and 'express' consent, and that this guidance is consistent with the OAIC's current approach for the APPs.
Step 1B – Risk No. 2	CDR consumers are asked to provide consent which is too broad to be a valid consent	There is currently OAIC guidance on what constitutes 'specific' and 'informed' consent. **Recommendation**: the ABA recommends that this guidance is applied consistently to the CDR regime. The PIA should consider how the decision not to include a consent API in version 1.0.0 of the Data Standards amplifies the risk that consumers will be required to authorise a larger scope of data than they may otherwise wish to consent to.
Step 1B – Risk No. 4	The CDR consumer is not adequately informed before giving consent	As above.

Risk Number	Risk outline	Comment
Step 1B – Risk No. 8	Non-accredited persons pose as ADR to obtain CDR data	If a malicious third party poses as an Accredited Data Recipient outside of the eco-system, it will be difficult for consumers to identify that the request is fraudulent. The ACCC and Treasury should undertake consumer education about how consumers can identify genuine Accredited Data Recipients. Additionally, Accredited Data Recipients should be required to provide customer facing content or education which clearly sets out how that organisation will communicate with consumers so that consumers can differentiate between legitimate and illegitimate communications under the regime.
Step 2 – Risk No 1	The Data Holder does not seek listing and undertake the ICT testing regime	The recommendation appears to misunderstand that a Data Holder will be required to provide certain information to the ACCC as part of on-boarding with the Registry. Further, Data Holders are required to complete a range of testing as outlined in the ACCC Assurance Strategy including functional and non-functional testing and penetration testing.
Step 3 – Risk No. 1	Risk of malicious attacks occurring as part of the CDR Consumer Re-direction.	The mitigants outlined by Maddocks suggest that "requiring Data Holders to authenticate the identity of the CDR consumer using their usual banking credentials" is a mitigant. This may be a misunderstanding that "authentication by known channel" does provide additional protections. The use of banking credentials increases the risk of loss arising from malicious attacks.
Step 3 – Risk No. 2	Data Holder refuses to accept the request	**Recommendation**: The ABA recommends that the CDR regime guidance provides advice on the grounds to refuse disclosure and examples where these might apply.
Step 3 – Risk No. 3	Pathway between the ADR and Data Holder is compromised	Gap analysis incorrectly states that there is not a requirement for the Data Holder to undergo any testing. Data Holders are required to complete a range of testing as outlined in the ACCC Assurance Strategy including functional and non-functional testing and penetration testing. Further, to call the Registry a Data Holder must authenticate themselves like any other client.

Risk Number	Risk outline	Comment
Step 4 – Risk No. 1	Authorisation does not match initial consent provided by the CDR consumer	The Data Standards provide mechanisms for matching of consent and authorisation – as identified in the PIA. However, there is no mechanism for the Data Holder to re-consent, update or modify a consent where the consumer believes the request does not match what they consented to. This may lead to consumers authorising requests where the consent is broader than requested.
Step 5 – Risk No. 1	CDR Data is transferred to a non-accredited person	If an entity is not accredited, they won't be issued with a certification, and therefore will not be able to request CDR data.
Step 6 – Risk No.3	CDR data is intercepted by malicious attack during the transfer between Data Holder and ADR	Guidance should be provided on how Data Holders should approach these scenarios.
Step 7A – Risk No. 1 and 2	Risk 1: Accredited Data Recipient collects and uses CDR data outside the scope of the consent Risk 2: Use for prohibited consents	As an additional control, there could be a mechanism under which Data Holders can escalate concerns about whether an Accredited Data Recipient is a 'fit and proper' person for purposes of the CDR regime.
Step 7A – Risk No. 3	Security of CDR data held by Accredited Data Recipient	**Recommendation**: The ABA recommends that the accreditation process is transparent, with all participants provided with information on the types of attestation and/or security testing that Accredited Data Recipients have undergone generally. This should also include a process for escalating security concerns to the relevant regulator, and a means to withhold data sharing while those issues are being considered/addressed.
Step 10 – Risk No. 1 and 2	CDR data is released to a suspended/ revoked Accredited Data Recipient	Suspension may not result in the revocation of a certificate. Therefore, the status endpoint must be updated immediately, and a forced refresh is to be issued to stop data sharing. If this is not undertaken, there is a risk of data leakage. Similarly, if a decision to revoke accreditation is made but there is a delay in cancelling the certificate/or updating the status endpoint then there is a risk of data leakage.

Recommendation: The ABA recommends that this section of the PIA would benefit from an analysis of the 'journey of data' in, through and out of the CDR as the interaction between the APP and the Privacy Safeguards are points of significant privacy risk.

2.6 Part H: Other privacy risks

2.6.1 Australian Financial Complaints Authority (AFCA)

The ABA notes that for the initial implementation of the CDR regime, it is intended that the ACCC will recognise an external dispute resolution scheme (EDR) under the CDR Act for the resolution of disputes and for the banking industry, this will be the AFCA (note that the OAIC can also hear privacy complaints). AFCA as an EDR has not traditionally been tasked with dealing with complaints relating exclusively to privacy. Given the complexity of the CDR regime and the number of regulatory bodies involved, there is potential risk of inconsistent outcomes arising.

Recommendation: The ABA recommends a review of adequacy of resourcing for this specialty area.

2.6.2 Scope of historical information shared

The CDR consumer is able to specify to the Accredited Data Recipient how far back in time the data request should be for (e.g. for a request made on 2 July 2020, data can be collected from the period 2 July 2019 to 2 July 2020), however, current Data Standards do not enable the Data Holder to be advised of this. Hence, there is a risk that the Accredited Data Recipient collects data from the Data Holder for a period greater than specified without CDR consumer consent and without the CDR consumer being aware.