# Privacy Impact Assessment

## Supplementary PIA to expand the Consumer Data Right to the Non-Banking Lending sector

Prepared for the Department of the Treasury

30 November 2023

**Sydney**
Level 29, 25 Martin Place, Sydney NSW 2000
PO Box Q1164, QVB Post Office, Sydney NSW 1230
t: +61 2 9373 3555 | f: +61 2 9373 3599 | www.sparke.com.au
adelaide | brisbane | canberra | darwin | melbourne | newcastle | perth | sydney | upper hunter

# Table of Contents

# 1 Executive Summary

1.1 This supplementary privacy impact assessment (**PIA**) considers the impact the Department of the Treasury's (**Treasury**) rollout of the Consumer Data Right (**CDR**) to the non-bank lending (**NBL**) sector (the **Project**) will have on individuals' privacy.

1.2 This supplementary PIA builds on the privacy analysis completed by the Treasury to date in respect of the CDR.[1] This supplementary PIA only considers risks specific to the non-bank lending sector not analysed in previous PIAs undertaken by the Treasury.

1.3 This supplementary PIA is specifically focused on privacy risks identified:

(a) in response to consultation Treasury has undertaken in relation to the *Consumer data right in non-bank lending CDR rules and data standards design paper* dated December 2022 (**NBL sector Design Paper**)[2]

(b) our review of the *Competition and Consumer (Consumer Data Right) Amendment Rules (No 2) 2023* (**NBL CDR Rules**),[3] and

(c) in response to consultation Treasury has undertaken in respect to the NBL CDR Rules.

1.4 We consider the proposed amendment to the CDR to include the NBL sector provides appropriate safeguards in respect to the handling of personal information of individuals who are NBL sector consumers.

1.5 However, the inclusion of the NBL sector into the CDR does give rise to some unique privacy risks and it is these risks which are considered in this supplementary PIA and form the basis for our recommendations in Part 3.

1.6 Subject to the Treasury's consideration of our observations and the recommendations contained in this supplementary PIA, we consider that the privacy risks associated with the Project can be effectively managed such that the inclusion of the NBL sector in the CDR does not present a high privacy risk for customers.

[1] For PIAs prepared for Treasury to date, see Consumer Data Right | Treasury.gov.au and see paragraph 2.7 in this supplementary PIA.

[2] See Consumer data right in non-bank lending - CDR rules and data standards design paper (treasury.gov.au).

[3] See *Competition and Consumer (Consumer Data Right) Amendment Rules (No 2) 2023* as at 27 November 2023.

# 2 Background and rationale for the Project

### *(a) Overview*

2.1 The purpose of this supplementary PIA is to analyse the possible impacts on the privacy of individuals resulting from the inclusion of the NBL sector into the CDR.

2.2 This supplementary PIA builds on the privacy analysis completed by the Treasury to date in respect of the CDR,[4] including the PIA undertaken to support the development of the *Consumer data right: Non-bank lending sectoral assessment* final report dated August 2022[5] (**NBL Sector Report**) and the consultation process undertaken in respect to the NBL sector Design Paper.[6] We discuss the themes raised during that consultation process in Part 4 of this supplementary PIA.

2.3 This supplementary PIA is specifically focused on privacy risks identified in response to:

(a) consultation Treasury has undertaken in relation to the NBL sector Design Paper (conducted in December 2022)

(b) our review of the NBL CDR Rules, and

(c) consultation Treasury has undertaken in respect to the NBL CDR Rules (August 2023).

2.4 Privacy risks associated with the CDR generally and the designation of the banking, energy and telecommunications sectors[7] are not revisited in this supplementary PIA where they have already been assessed and are not affected by the proposed inclusion of the NBL sector in the CDR.

2.5 This supplementary PIA assesses the privacy risk of the Project with respect to the following legislative schemes:

(a) *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**)

(b) Part IVD of the *Competition and Consumer Act 2010* (Cth) (**Competition and Consumer Act**) (the **Privacy Safeguards**), and

(c) *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (**CDR Rules**).

2.6 Materially, by Division 5 of Part IVD of the Competition and Consumer Act, Privacy Safeguards 1, 10, 11, 13 and all of the APPs apply in respect to an entity's (data holders) handling of CDR data. While the APPs do not apply for accredited persons and accredited data recipients (**ADRs**), the Privacy Safeguards apply.[8] In order to assess the privacy impact of the Project, we have considered the Privacy Safeguards and APPs (as they apply).

---

[4] For PIAs prepared for Treasury to date, see Consumer Data Right | Treasury.gov.au and see paragraph 2.7 in this supplementary PIA.

[5] See Consumer Data Right – Sectoral Assessment for Non-Bank Lending – Final Report | Treasury.gov.au.

[6] See Consumer data right: Non-bank lending sectoral assessment - Final report (treasury.gov.au) Attachment A.

[7] A sector can be designated to be subject to the CDR under section 56AC of the Competition and Consumer Act.

[8] For ADRs, Privacy Safeguards 1, 2, and 5 to 13 (inclusive) apply. For accredited persons, Privacy Safeguards 1 to 4 (inclusive) apply (see Competition and Consumer Act section 56EC(4) and (5)).

### *(b) Previous PIAs*

2.7 Multiple PIAs have been completed for CDR and the progressive rollout of the CDR to new sectors. These PIA are:

(a) March 2019 – Implementing the CDR to give consumers better access and control over their data (**2019 CDR PIA**)

(b) November 2019 – Implementing the CDR to give consumers better access and control over their data (**2019 Banking PIA**)

(c) June 2020 – Supplementary PIA focusing on expanding the CDR to the energy sector (**2020 Energy PIA**)

(d) September 2021 – PIA update: 'version 3' CDR Rules amendments to expand participation pathways for businesses and give consumers better access and control over their data

(e) November 2021 – PIA update: 'version 4' CDR Rules amendments as they relate to the energy sector

(f) November 2021 – PIA update: examining the privacy impact of designating the telecommunications sector to the CDR

(g) August 2022 – PIA update: examining the privacy impact of designating the non-bank lending sector to the CDR (**NBL Sector PIA**) which is Attachment A to the NBL Sector Report, and

(h) July 2023 – PIA update 'version 5' operational enhancements to the CDR Rules'

(collectively, the **CDR PIAs**).

2.8 We have had regard to these CDR PIAs in undertaking this supplementary PIA.

### *(c) Current Status of the CDR Rollout*

2.9 The CDR is Australia's national data portability initiative. It gives individuals and businesses the ability to share their data with trusted and accredited third parties, along with limited types of data with non-accredited parties. In turn, these third parties can use this data to provide products, services and insights that benefit consumers.

2.10 The Treasury leads CDR policy and program delivery, including the development of the legislative framework. The CDR is regulated by the Office of the Australian Information Commissioner (**OAIC**) and the Australia Competition and Consumer Commission (**ACCC**). The Data Standards Body (**DSB**) develops the technical and consumer experience standards, which are made by the Data Standards Chair.

2.11 The CDR is being implemented on a sector-by-sector basis. The CDR is currently active in the banking and energy sectors.

### *(d) Rollout of the CDR to the NBL sector*

2.12 Following the release of the Treasury's 'Strategic Assessment Outcomes' report in January 2022, Treasury has assessed the expansion of the CDR to the NBL sector.

2.13 In August 2022, the Treasury released the final NBL Sector Report which recommends the designation of the NBL sector for the CDR. The NBL Sector Report identified that extending the CDR to the NBL sector would complement the rollout of the CDR in the banking sector,

allowing consumers to 'easily access and share a complete picture of their lending information'.[9]

2.14 Other benefits identified for the expansion of the CDR to the NBL sector (identified in the NBL Sector Report), include:

(a) empowering individuals and business consumers to make more informed decisions about non-bank lending products, leading to better outcomes for individuals and businesses. For example, comparator websites indicated they could provide better advice to consumers about lending products if they could take into account NBL products

(b) reducing barriers for consumers to switch between lender or lending products by providing an efficient and secure means for a consumer's financial data to be shared with an accredited lender and facilitate better lending decisions which take into account a more comprehensive assessment of the consumer's credit profile, history and risk

(c) facilitating investment in financial technology, which will give consumers a comprehensive picture of their day-to-day finances and better equip consumers to improve their financial planning

(d) promoting competition by making it easier for consumers to identify and evaluate alternative form of funding in competition with the banking sector, and

(e) leading to the development of new financial products and services for vulnerable customers experiencing financial hardship, for example, financial counsellors.

2.15 Relevant to this supplementary PIA, the NBL Sector Report notes that extending the CDR to the NBL sector is likely to present the same privacy risks as it did when rolled out to the banking sector.[10]

2.16 Following designation of the NBL sector (discussed below), the Treasury, in conjunction with the DSB, is developing CDR rules and data standards specific to the NBL sector.

2.17 See Part 4 of this PIA for a discussion of the consultation that has been conducted, to date, in respect of the Project and the consultation process(es) that have been considered as part of undertaking this supplementary PIA.

### *(e) NBL Sector Designation and NBL CDR Rules*

2.18 On 21 November 2022, the Minister formally designated the NBL sector by the *Consumer Data Right (Non-Bank Lenders) Designation 2022* (Cth) (**NBL Sector Designation**).[11]

2.19 The NBL Sector Designation provides that a "relevant non-bank lender" (being an entity providing finance or 'credit like' products other than excluded data holders) is required to comply with the CDR in respect to specifics classes of information designated as CDR data. Credit information is excluded.[12]

2.20 The NBL CDR Rules will amend the CDR Rules for the banking sector (Schedule 3 of the CDR Rules) and extend rules for the sharing of the same classes of information, being:

---

[9] See Consumer data right: Non-bank lending sectoral assessment - Final report (treasury.gov.au) page 7.

[10] *Consumer data right: Non-bank lending sectoral assessment – Final Report August 2022*, page 22.

[11] Consumer Data Right (Non-Bank Lenders) Designation 2022 (legislation.gov.au).

[12] See NBL Sector Designation clause 10 and Privacy Act section 6N(d), (i), (j) or (l) and section 6S(2).

(a) information about the user of a product ('customer data'),

(b) information about the operation of a user's account ('account data')

(c) information that describes the transactions of a user ('transaction data'), and

(d) information about the use of a product ('product-specific data'),

by a "relevant non-bank lender" other than excluded data holders.

2.21 Recognising that there are benefits to consumers, competition and innovation from small businesses and start-ups and the cost of compliance on small business, the NBL CDR Rules establish a *de minimis* threshold for mandatory data sharing.

2.22 Where the total value of the NBL sector lender's resident loans and finance leases:

(a) is over $500 million for the preceding calendar month,

(b) averages over $500 million for the previous 11 calendar months, and

(c) the lender has more than 500 customers,

the entity is a data holder for the purposes of the NBL CDR Rules and is required to comply.[13]

2.23 Finally, the NBL CDR Rules propose a phased application of the CDR to the NBL sector depending on the size of the provider, the complexity of the request and date for the relevant tranche being reached.[14] A phased approach to implementation balances the benefits of consumers receiving access to data sharing under the CDR while ensuring that smaller entities have adequate time to build the relevant IT systems under the CDR framework.

[13] see NBL CDR Rules definition of *large provider* Schedule 3 Part 6 Division 6.1 clause 6.1.

[14] see NBL CDR Rules Schedule 3 Part 6 Division 6.1.

# 3 Findings and Recommendations

3.1 We consider the extension of the CDR to the NBL sector will have a positive privacy outcome for consumers, particularly when compared to current data sharing arrangements in use by the sector. By requiring a "relevant non-bank lender" to share CDR data in accordance with the CDR framework, individuals get the benefit of the application of the Privacy Safeguards to the handling of their information, together with the requirement that consumer information be handled in accordance with specified data security requirements. The data minimisation principle also applies, as do the express consent provisions for data sharing and the requirements around accreditation. These changes reflect a more secure and transparent framework for data sharing.

3.2 We consider this improves the current position where NBL data is shared by sharing passwords, screen scraping, or by other less formal channels and without the benefit of the informed consent requirements imposed by Privacy Safeguard 3.

3.3 However, the inclusion of the NBL sector in the CDR does give rise to some unique privacy risks, which we consider can be mitigated by the implementation of the recommendations set out below.

***(a) Recommendations***

3.4 We have reviewed the NBL CDR Rules and the responses received by the Treasury, to date, in response to consultation on the NBL sector Design Paper (December 2022) and the NBL CRD Rules (August 2023).

3.5 Having regard to:

(a) the content of the NBL CDR Rules

(b) the extent to which the NBL CDR Rules propose amendments to the CDR Rules

(c) the extent to which issues have been addressed in previous CDR PIAs, and

(d) the issues raised in the consultation on the NBL sector Design Paper,

we make the following recommendations:

| No. | Recommendation |
|---|---|
| **Recommendation 1** | Treasury, together with the OAIC and ACCC, consider what instructions or guidance can be developed for credit providers to ensure credit providers comply with the CDR, Part IIIA of the Privacy Act and the CCR in relation to the handling of credit reporting information. |

| No. | Recommendation |
|---|---|
| **Recommendation 2** | Treasury consider whether the exclusion to financial hardship information and repayment history information from "customer data" |

| | |
|---|---|
| | is sufficient or whether the exclusion should be extended so as to protect the privacy of vulnerable consumers. |

| No. | Recommendation |
|---|---|
| **Recommendation 3** | Treasury monitor the regulation of certain NBL sector products, such as Buy Now, Pay Later products in order to identify any high privacy risks such that the NBL CDR Rules should be amended to address those risks (for example, in relation to the marketing of such products). |

| No. | Recommendation |
|---|---|
| **Recommendation 4** | Treasury consider ways to support non-bank lenders who do not meet the *de minimis* threshold understand the benefits of the CDR and encourage them to voluntarily participate in the CDR and comply with the obligations of a data holder. |

| No. | Recommendation |
|---|---|
| **Recommendation 5** | Treasury monitor the implementation of data holder's obligations to see if any privacy concerns arise.<br><br>Treasury should engage with industry and stakeholders to identify instances where the information security / privacy-related IT infrastructure is particularly difficult to implement and if so, consider whether the timing of obligations should be amended. |

# 4 Key issues raised in response to consultation

4.1 The Treasury and the DSB have undertaken a number of consultation processes as part of the Project.

***(a) Previous consultation processes in respect of the Project***

4.2 On 15 March 2022, the Treasury undertook a consultation process so as to assess whether to expand the CDR to the NBL sector, by the *Consumer Data Right Non-Bank Lending Sectoral Assessment: Consultation Paper*.[15] Responses to that consultation informed the NBL Sector Report, which recommended that the CDR be designated in the NBL sector.

4.3 Following the release of the NBL Sector Report, the Treasury consulted on the draft NBL Sector Designation. While designation does not of itself impose any data sharing obligations, this designation specified the classes of information that may be shared through the CDR, as well as the non-bank lenders that may be data holders.[16]

4.4 On 21 November 2022, the Minister formally designated the NBL sector for inclusion in the CDR.[17]

***(b) Consultation in relation to the NBL sector Design Paper***

4.5 In December 2022, the Treasury and DSB undertook a consultation to inform the Treasury and the DSB on the development of rules and data standards to implement the CDR in the NBL sector.[18] The NBL sector Design Paper was made available for stakeholders' consideration, which sought to elicit feedback on a range of issues in respect to the rules and data standards. That consultation closed on 31 January 2023.

4.6 We have considered the following responses to that NBL sector Design Paper consultation process:

(a) Adatree

(b) Australian Banking Association

(c) Australian Collectors & Debt Buyers Association

(d) Australian Competition and Consumer Commission

(e) Australian Finance Group

(f) Australian Financial Industry Association

(g) Australian Retail Credit Association

(h) Australian Securitisation Forum

(i) Australian Small Business and Family Enterprise Ombudsman

(j) Basiq

(k) Biza.io

[15] See Consumer Data Right Sectoral Assessment for Non-Bank Lending – Open Finance | Treasury.gov.au for a copy of the submissions received in response to the Department's consultation undertaken in respect of the NBL sector report. That consultation closed in April 2022.

[16] https://treasury.gov.au/consultation/c2022-300402

[17] https://www.legislation.gov.au/Details/F2022L01522

[18] See Consumer Data Right rules and data standards design paper for non-bank lending sector | Treasury.gov.au

(l) Block, Inc

(m) CDFP Limited

(n) Cuscal

(o) Finance Brokers of Australia Limited

(p) Financial Legal Rights Centre

(q) FinTech Australia

(r) Frollo

(s) Joint submission from Chartered Accountants Australian & New Zealand, CPA Australia, and the Institute of Public Accountants,

(t) Tech Council of Australia, and

(u) Officer level feedback from the OAIC.

4.7 We have also considered three additional submissions that were received on a confidential basis.

***(c) Consultation in relation to the NBL CDR Rules draft amendments, explanatory materials and draft of this PIA***

4.8 In August 2023, the Treasury and DSB subsequently undertook a public consultation on the following material:

(a) exposure draft amendments to the CDR Rules;

(b) explanatory materials; and

(c) draft version of this PIA.

4.9 This consultation closed on 6 October 2023.

4.10 We have considered the following responses received in response to this consultation process:

(a) Australian Competition and Consumer Commission

(b) Australian Finance Industry Association

(c) Australian Retail Credit Association

(d) Basiq

(e) Cuscal Limited

(f) FinTech Australia, and

(g) Office of the Australian Information Commissioner.

4.11 The consultation responses raised the following key issues:

(a) how the CDR and the Comprehensive Credit Regime (**CCR**) will interact in the NBL sector (**Issue 1**)

(b) the appropriateness of including or excluding Financial Hardship Information (**FHI**) from the scope of the CDR in the NBL sector (**Issue 2**)

(c) using non-credit information to inform credit assessments (**Issue 3**), and

(d) whether some products deemed to be 'high-cost' products should be excluded from the scope of the CDR in the NBL sector (**Issue 4**).

4.12 Our response to these issues is set out below and otherwise addressed in the Privacy Risk table.

### *(c) Response to consultation themes*

4.13 We discuss below our analysis of the privacy issues arising from the consultation.

#### *Issue 1 – interaction between NBL sector and CCR*

A number of responses to consultation raised issues in respect to the interaction between the NBL sector and the CCR. Those issues recommended Treasury consider the following:

(a) whether the extension of the CDR to the NBL sector may enable non-bank lenders to circumvent the CCR regime (for example, in relation to the disclosing of credit information in a manner that is inconsistent with the requirements of Part IIIA of the Privacy Act), and

(b) whether, for credit providers, the requirement to comply with three overlapping regulatory regimes (CDR for the NBL sector, Part IIIA of the Privacy Act and the CCR) will create risks that credit providers will fail to understand their obligations, increasing the risk of inadvertent breaches.

This issue was considered in the NBL sector PIA.[19]

Credit providers in the NBL sector may have obligations under each of the CDR for the NBL sector, the Privacy Act and the CCR as follows:

(a) In respect to the handling of credit information,[20] credit providers (and credit reporting bodies) are regulated by Part IIIA of the Privacy Act and must comply with Subdivision D of Division 3, Part IIIA of the Privacy Act in respect to the disclosure of credit eligibility information about an individual,

(b) A "relevant non-bank lender" who is a registered financial corporation and a credit provider may be a licensee for the purposes of the *National Consumer Credit Protection Act 2009* (Cth) (**NCCP Act**) and be required to comply with the CCR. The CCR provides limitations on sharing information about a person's credit history and how that information can be used,[21] and

(c) A credit provider who is a "relevant non-bank lender" will be required to comply with the CDR in relation to the sharing of CDR data.

The NBL Sector Designation provides that credit information is excluded as a specified class of information.[22] However, stakeholders have identified, as an example, a situation where a credit provider who receives credit reporting information from a credit reporting body in accordance with Part IIIA of the Privacy Act or holds information about a person's credit history in the performance of the CCR, receives a separate request from an ADR under the CDR to share that data (for

[19] See Consumer data right: Non-bank lending sectoral assessment - Final report (treasury.gov.au) at page Item 5 page 40.

[20] Defined in section 6N of the Privacy Act.

[21] See Part 3-2CA of the NCCP Act and Part 3.8 of the *National Consume Credit Protection Regulations 2010* (Cth).

[22] See Consumer Data Right (Non-Bank Lenders) Designation 2022 (legislation.gov.au) clause 10. We note this is also the case in relation to ADIs (see Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (legislation.gov.au) clause 9).

example, to the extent credit reporting information may form part of transaction data). If the credit provider was to share that information (in the form of transaction data) stakeholders consider there is a risk the information could be used in a way that is inconsistent with the limitations in the CCR (specifically, to disadvantage consumers by affecting their credit rating).

In terms of the privacy risk, we agree with the analysis set out in the NBL sector PIA that the CDR consent rules mitigate the privacy risk by requiring ADRs to obtain informed consent from consumers before their data is shared in response to a data request. Further, CDR Rule 3.5(1)(a) permits a data holder to refuse to disclose customer data in response to a request where, relevantly, the data holder considers this is necessary to prevent financial harm or abuse.

In relation to the risk of credit providers inadvertently breaching one or more of the requirements of Part IIIA of the Privacy Act, the CCR and / or the CDR for the NBL sector, we acknowledge non-compliance may give rise to a privacy risk for customers (depending on the nature of the non-compliance). For example, non-compliance with the consent provisions in the CDR Rules could have a substantial privacy impact if transaction data (which includes credit reporting information that is also personal information) is disclosed by a credit provider in a manner which is inconsistent with Part IIIA of the Privacy Act.

We consider that for credit providers who are a "relevant non-bank lender", compliance with the CDR for the NBL sector in addition to Part IIIA of the Privacy Act and the CCR will require a detailed understanding of the different regimes and how they operate in relation to credit reporting information that is held by the credit provider. Failure to understand how the obligations for the handling of credit reporting information apply may lead to a breach of one or more of the CDR, Part IIIA of the Privacy Act or the CCR, which could have a negative impact on the handling of an individual's personal information (in the form of their credit reporting information).

We make **Recommendation 1** accordingly.

**Recommendation 1 –** Treasury, together with the OAIC and ACCC, consider what instructions or guidance can be developed for credit providers to ensure credit providers comply with the CDR, Part IIIA of the Privacy Act and the CCR in relation to the handling of credit reporting information.

### *Issue 2 – excluding Financial Hardship Information from NBL sector*

A number of stakeholders have recommended that Treasury consider the risks and benefits of excluding FHI from the CDR for the NBL sector.

Some of the concerns about excluding FHI and "repayment history information" from the CDR for the NBL sector were as follows:

(a) that a broad exclusion of FHI and "repayment history information" from the CDR for the NBL sector could result in data holders adopting a broad interpretation of those terms in order to avoid sharing that data in response to a consumer data request (for example, when sharing information about a customer's transaction data), and

(b) by excluding FHI and "repayment history information", data holders would not have a complete picture of a consumer's financial position which may adversely affect the

consumer because certain types of products may not be offered to them (for example, financial counselling).

On the other hand, some stakeholders raised concerns that including FHI and "repayment history information" could lead to data holders exploiting the information to the detriment of vulnerable customers. For example, customers could be refused certain products, on the basis of their FHI.

One stakeholder also raised a concern that even if FHI and "repayment history information" is excluded from the CDR for the NBL sector, whether or not a customer is experiencing hardship can still be inferred from their transaction data. As an example, transaction data includes whether the transaction is a debit, a credit or a fee. If that transaction data indicated that a customer was regularly paying fees as a result of not making their minimum repayments, you could infer, however tenuously, that they were experiencing financial hardship. This could lead to a risk that the information could then be exploited to the detriment of the customer.

Financial hardship information is a customer's personal information (but not sensitive information).[23]

We note this issue was not considered in the 2019 CDR PIA or the 2019 Banking PIA given the timing of the commencement of the CCR. This issue was considered in the NBL sector PIA[24] and the 2020 Energy PIA.[25]

The NBL Sector Report discusses a number of policy reasons to support the inclusion of FHI in the NBL sector, including that inclusion of data of this nature may enable a lender to process hardship applications and aid customers more quickly and enable industry to develop tools to educate and assist individuals experiencing hardship. The contrary view is that inclusion of data of this nature may be misused by NBL sector participants to target vulnerable customers.

Taking into account the above, and balancing the policy considerations, "financial hardship information" and "repayment history information" as those terms are defined in the Privacy Act have been excluded from the meaning of "customer data", where such information was disclosed by or to a credit reporting body within the meaning of the Privacy Act.[26] Information about financial hardship and a consumer's repayment history is otherwise captured (for example, as transaction data).

We acknowledge this approach seeks to balance the risks and benefits discussed above, while being consistent with the overall objective of the CDR which is to enable consumers to consent to the sharing of their information in a secure manner and with enhanced privacy protections (in addition to the APPs).

By this approach, to the extent information about financial hardship could be inferred from transaction data, from a privacy perspective, we consider the CDR provides adequate protections in respect of the use and disclosure of that data noting:

(a) CDR Rule 4.11 requires an accredited person to obtain express consent from a CDR customer in relation to the disclosure of CDR data. This would include data which evidences financial hardship and / or repayment history. The consent may not be valid for a period of more than 12 months (CDR Rule 4.12(1)) and at the end of the consent period,

[23] See Privacy Act section 6AQ(4) (definition of "financial hardship information") and section 6V(1) (definition of "repayment history information").

[24] See Consumer data right: Non-bank lending sectoral assessment - Final report (treasury.gov.au) at pages 13 – 15 and Item 5 page 41.

[25] See Consumer Data Right in energy (treasury.gov.au) at page 42.

[26] See NBL CDR Rules Schedule 3 Part 2 clause 1.3 (definition of "customer data").

data needs to be de-identified or deleted (CDR Rule 7.12 and 7.13 and Privacy Safeguard 12).

(b) When seeking authorisation to disclose CDR data (or amend a current authorisation) a data holder must give the customer certain information including, relevantly, information about the types of data the data holder is seeking authorisation to disclose (CDR Rule 4.23(1)(c)). This would include transaction data which evidences financial hardship and transaction history information.

(c) CDR Rule 3.5(1)(a) permits a data holder to refuse to disclose customer data in response to a request where, relevantly, the data holder considers this is necessary to prevent financial harm or abuse. The data holder must also provide the customer with access to the customer dashboard if the data holder receives a request from an accredited person on behalf of an eligible customer (CDR Rule 1.15 and Schedule 3 Rule 2.3).

(d) We further note:

(i) the data minimisation principle (CDR Rule 1.8)

(ii) that accredited persons need to be accredited in accordance with Part 5 of the CDR Rules

(iii) that accredited persons can only use and disclose CDR data in accordance with the CDR Rules or otherwise in accordance with Privacy Safeguard 6, and

(iv) the *de minimis* principle will mean smaller players in the NBL sector will not be captured by the CDR Rules.

Notwithstanding the above, having regard to the concerns raised by stakeholders in response to consultation and the Treasury's policy objective, we make **Recommendation 2**.

**Recommendation 2 –** Treasury consider whether the exclusion to financial hardship information and repayment history information from "customer data" is sufficient or whether the exclusion should be extended so as to protect the privacy of vulnerable consumers.

***Issue 3 – use of non-credit information to inform credit assessments***

Consultation responses raised a concern about the use of non-credit information to inform credit assessments under the CDR.

Currently, by Part IIIA of the Privacy Act, an individual's creditworthiness is assessed based on the credit reporting information about the individual that was disclosed to a credit provider by a credit reporting body under Division 2 of Part IIIA.

Stakeholders raised a concern that under the CDR, aggregate data from different sources may be used to assess an individual's creditworthiness. For example, if transaction data evidences that an individual is a frequent users of BNPL products, which could then be used to adversely affect a customer's creditworthiness.

The issue of consumer data being collected from multiple sources was considered in the NBL sector PIA generally, but not specifically in relation to creditworthiness.[27]

As discussed in response to Issue 2 above, to the extent this concern raises a privacy issue, we consider the CDR provides a robust framework for the handling of CDR data with informed consent being the key mechanism by which customer privacy is protected (see CDR Rules 4.12(1), 4.23(1)(c), 7.12 and 7.13 and Privacy Safeguards 3, 5 and 6).

We consider these provisions adequately address the privacy risks associated with the combining various datasets in order to more accurately assess an individual's creditworthiness.

In circumstances where we consider the privacy risks are adequately addressed by the CDR, we make no recommendation in relation to Issue 3.

### *Issue 4 – excluding 'high-cost' products*

Consultation responses raised concerns about the inclusion of certain types of products in the NBL sector which may be marketed towards vulnerable customers, such as Buy Now, Pay Later (**BNPL**) products, given the impact of those products on vulnerable individuals. Some stakeholders suggested that Treasury should consult with industry about the specific types of products which are to be included in the list of "covered products" to assess any privacy risks that may arise by the inclusion of those products in the CDR for the NBL sector.

We note feedback from consultation on the NBL sector Design Paper was that the CDR data categories were appropriate for the NBL sector.

Further, it doesn't appear to us that a product-by-product review of covered products is required, from a privacy perspective, noting that the products that may be "covered products" by the NBL CDR Rules are the same products as those currently included in the CDR Rules (save for BNPL products)[28] and the CDR Rules apply consistently in respect of the handling of personal information collected and handled in the offering of those products by CDR participants.

To the extent the concern raised by stakeholders is that BNPL products may be used to target more vulnerable customers, we acknowledge that the profiling and targeting of vulnerable customers by providers of high-cost products could have serious privacy impacts and consequences for affected individuals.

However, we consider that privacy risk is appropriately mitigated in circumstances where the CDR requires an individual's consent prior to the disclosure of their data by a data holder, meaning individuals can refuse to consent to the disclosure of information which may make them a target for the marketing of 'high-risk' products (and noting our discussion in respect of Issue 2 above that "financial hardship information" and "repayment history information" has been excluded from the meaning of "customer data").

Some stakeholders have expressed concern regarding reliance on consent as the main strategy for mitigating risk, and have submitted that protections offered by the CDR consent framework should be supported by other mechanisms to protect consumers, noting that consumers are not always well-placed to assess the risks and benefits of sharing their data, particularly in circumstances where the consumer is experiencing vulnerability. We do not share this sentiment. Consent is a

[27] See Consumer data right: Non-bank lending sectoral assessment - Final report (treasury.gov.au) at Item 6 page 42.

[28] See CDR Rules Schedule 3 clause 1.4.

key feature of the CDR (the consent framework often being described as "rigorous" and being the "bedrock of the CDR system"). It does not follow, in our view, that because a customer is vulnerable they are not in a position to give their informed and express consent to the use and disclosure of their CDR data. Indeed, for the reasons discussed above in respect of Issue 2, there are genuine policy reasons for sharing a more complete picture of a customer's financial position (for example, so customers can be offered financial counselling services).

We think the preferable approach is that the CDR framework have adequate protections to protect consumers, whether vulnerable or not, such that information that prejudices or unfairly targets vulnerable consumers ought not be disclosed.

We note that the Treasury and DSB are currently undertaking a consent review and authentication uplift in respect of the CDR. While the outcome of this process is not known at the time of the preparation of this PIA, this process may make specific recommendations in relation to consents for certain types of products, such as BNPL products.[29] Some stakeholders recommended that Treasury consider the impact of any proposed changes to the consent framework to the regulation of higher cost products in the NBL sector.

We further note that, as identified in the NBL Sector Report,[30] the CDR operates alongside regulatory frameworks for the banking sector, including the Credit Act, which contains a range of protections to prevent lenders from targeting consumers with inappropriate lending products. The regulation of those products is arguably better managed under those specific legislative schemes.

In relation to BNPL products, pay day loans and consumer leases, the Commonwealth is currently taking steps to better regulate those products, with one option being that BNPL products will be treated as credit contracts and subject to the Credit Act.[31] Further reforms are also proposed by the *Financial Sector Reform Bill 2022* (Cth)[32] which includes, relevantly, an amendment to the Credit Act to impose additional protections on the offering of small amount credit contracts including the marketing of those contracts. For example, section 133CF of the *Financial Sector Reform Bill* prohibits a licensee from direct marketing (unsolicited communications) in relation to a small amount credit contract.

In circumstances where BNPL products are being actively considered by the Commonwealth for regulation (by the Credit Act and *Financial Sector Reform Bill*), we make **Recommendation 3** below.

**Recommendation 3 –** Treasury monitor the regulation of certain NBL sector products, such as Buy Now, Pay Later products in order to identify any high privacy risks such that the NBL CDR Rules should be amended to address those risks (for example, in relation to the marketing of such products).

[29] See Noting Paper 273 - Consent Review · Issue #273 · ConsumerDataStandardsAustralia/standards · GitHub and Noting Paper 280: The CX of Authentication Uplift · Issue #280 · ConsumerDataStandardsAustralia/standards · GitHub.

[30] See Consumer data right: Non-bank lending sectoral assessment - Final report (treasury.gov.au) page 23.

[31] See Address to the Responsible Lending & Borrowing Summit | Treasury Ministers and Regulating Buy Now, Pay Later in Australia | Treasury.gov.au accessed 1 June 2023.

[32] See 22087b01.pdf;fileType=application/pdf (aph.gov.au).

# 5 Analysis of privacy impacts and risks

***(a) Documentation considered as part of this supplementary PIA***

5.1 This supplementary PIA is informed by the following documentation:

(a) NBL Sector Report

(b) NBL sector Design Paper

(c) NBL CDR Rules

(d) NBL Designation

(e) the CDR PIAs

(f) OAIC's *Report on the draft Consumer Data Right (Non-bank Lenders) Designation 2022*[33]

(g) Consent flow public design document[34]

(h) CDR consent flows[35]

(i) Consent management for Data Holders[36]

(j) Consumer experience guidelines[37]

(k) CX Guidelines for collection and use consents[38]

(l) CX Artefacts Design Paper for the Telecommunications Sector

(m) Privacy Act and the APPs

(n) Part IVD of the Competition and Consumer Act

(o) CDR Rules

(p) *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019*

(q) *Consumer Data Right (Energy Sector) Designation 2020*

(r) OAIC's *APP Guidelines*[39]

(s) OAIC's *Guide to Undertaking Privacy Impact Assessments*[40]

(t) OAIC's *CDR Privacy Safeguards Guidelines*,[41] and

(u) *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth).

5.2 We have also incorporated into this supplementary PIA:

(a) feedback from the Treasury, and

---

[33] See Report on the draft Consumer Data Right (Non-bank Lenders) Designation 2022 (oaic.gov.au)

[34] Available at https://miro.com/app/board/uXjVPD76GlY=/.

[35] Available at https://www.figma.com/proto/jHG3HstULWcr7KfCUWxFtD/WIP-%7C-Design-paper-%7C-NBL?page-id=0%3A1&node-id=18%3A4734&viewport=1717%2C927%2C0.25&scaling=scale-down&starting-point-node-id=1%3A3263.

[36] Available at https://d61cds.notion.site/Consent-Management-Data-holder-33ff846f68f3466ab189d97c6c0afd28.

[37] Available at https://d61cds.notion.site/.

[38] Available at https://d61cds.notion.site/Collection-and-use-consents-fcf5e47455274d26b028d218b22f017a.

[39] Available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines.

[40] Available at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments.

[41] Available at https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines.

(b) responses to the consultation undertaken in respect of the NBL CDR Rules (see Part 4 of this PIA) and this draft supplementary PIA.

### *(b) Scope of this PIA*

*In scope of this supplementary PIA*

5.3 This supplementary PIA considers risks specific to the NBL sector not analysed in previous PIAs undertaken by the Treasury regarding the CDR.

*Out of scope of this supplementary PIA*

5.4 This supplementary PIA does not consider:

(a) the privacy risks previously assessed in the previous CDR PIAs

(b) applicability or impact of any proposed amendments to the Privacy Act that have not received Royal Assent as at the date of this supplementary PIA, and

(c) other risks on individuals, businesses or government departments or agencies, for example commercial or competition law risks.

### *(c) How should this PIA be used?*

5.5 This supplementary PIA:

(a) examines how the CDR rollout to the NBL sector will affect individuals from a privacy perspective

(b) identifies risk areas that the CDR will likely pose to the NBL sector in relation to compliance with privacy laws and community expectations, and

(c) suggests strategies to address identified risks by minimising privacy intrusions, and maximising privacy protections for the implementation and operation of the Project.

5.6 This supplementary PIA can also be used to further inform and educate those involved in, or affected by, the initiative as it is implemented, for example, in the design of guidelines, educational materials for users, staff training, system design and program evaluation.

### *(d) Methodology*

5.7 To develop this supplementary PIA, we have had regard to the documents and discussions specified in paragraphs 5.1 and 5.2 above.

5.8 Our process for assessing privacy impacts is as follows:

(a) identifying privacy impacts and risks involves an examination of how the Project will:

> *[a]ffect the choices consumers have regarding how information about them is handled, the potential degree of intrusiveness into the private lives of consumers, compliance with privacy law, and how the project fits into community expectations.*[42]

(b) the Project is therefore assessed for compliance with privacy laws, and whether the Project can meet community expectations, and

(c) the Privacy Risk table (set out below) outlines specific recommendations to minimise privacy risks relating to the Project.

[42] OAIC, Privacy impact assessment guide dated August 2006, at page xxi.

### *(e) Privacy laws considered by this supplementary PIA*

5.9 This supplementary PIA considers privacy impacts by reference to the Privacy Act, including the APPs set out in Schedule 1 to the Privacy Act, the 13 Privacy Safeguards within Division 5, Part VID of the Competition and Consumer Act and the extent to which the Privacy Safeguards are further discussed in the CDR Rules (Part 7, Division 7.2).

### *(f) Making recommendations*

5.10 A PIA should identify avoidable risks and recommend measures to remove or reduce them to an appropriate level.

5.11 However, recommendations should seek to achieve a balance between the interests of the Treasury in making the proposal, and the people affected by that proposal.

5.12 Our recommendations in this supplementary PIA reflect the above principles.

### *(g) Information flows for the Project*

5.13 The NBL sector information flows are discussed in the following documents:

(a) the 2019 CDR PIA[43]

(b) the 2019 Banking PIA,[44] and

(c) the OAIC PS Guidelines.[45]

5.14 The same information flows will apply for the NBL sector by the operation of the NBL CDR Rules. We have not repeated the data flows in this supplementary PIA on that basis.

### *(h) Privacy Risk table*

5.15 The Privacy Risk table sets out our analysis of the privacy risks identified for the Project against the Privacy Safeguards and the APPs (if applicable). These privacy risks have been identified based on our review of the NBL CDR Rules with a focus on what is intended to change as a consequence of the inclusion of the NBL sector in the CDR.

5.16 Where privacy risks have been adequately assessed in previous CDR PIAs, we have not further considered the issue. In particular, we have not revised the privacy assessment of the overall operation of the CDR (addressed in the 2019 CDR PIA) nor the operation of the CDR to the banking sector (addressed in the 2019 Banking PIA).

5.17 In summary, and in circumstances where the NBL CDR Rules will require those relevant non-bank lenders (other than excluded entities) to share the same datasets those shared by the banking sector, in the same way as data is shared in the banking sector, we consider the overall effect of the designation of the NBL sector to provide appropriate safeguards for the handling of the personal information of NBL sector customers.

5.18 However, where the operation of the CDR in the NBL sector raises privacy risks, we have discussed those in the Privacy Risk table and made a number of recommendations for Treasury's consideration at this stage in the Project.

---

[43] See Privacy Impact Assessment (treasury.gov.au) page 53 to 58 (inclusive).

[44] See Consumer Data Right Regime PIA (treasury.gov.au) Part G page 71.

[45] See Privacy-Safeguard-Guidelines-v4-Nov-2022-rev2.pdf (oaic.gov.au) Chapter C page 37.

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| **Excluded entities** | | | |
| 1 | The NBL CDR Rules establish a *de minimis* threshold to limit mandatory data sharing obligations to relevant non-bank lenders.[46]<br><br>Where, on a particular day, the total value of the relevant non-bank lender's resident loans and finance leases:<br><br>(a) is over $500 million for the preceding calendar month,<br><br>(b) averages over $500 million for the preceding 11 months, and<br><br>(c) the lender has more than 500 customers,<br><br>the entity is an excluded entity for the purposes of the NBL CDR Rules and not required to comply (although they may do so voluntarily). | Non-bank lenders who will not met the *de minimis* threshold will not be subject to the CDR for the NBL sector.<br><br>Depending on the nature and size of a non-bank lender, they may be regulated by the Credit Act and the Privacy Act (in terms of their being an APP entity). Credit providers will also be regulated by Part IIIA of the Privacy Act. | The NBL Sector Report and the NBL sector Design Report discuss the rationale for the *de minimis* threshold.<br><br>The *de minimis* threshold has an impact from a privacy perspective because the NBL sector has a long tail of smaller providers who will not meet the *de minimis* threshold, meaning their collection and handling of information will not be required to comply with the CDR and the Privacy Safeguards. They will also be exempt from the requirement to comply with the internal and external dispute resolution requirements set out in the CDR for the banking sector.<br><br>Some NBL sector providers will be regulated by other laws, including the Credit Act and the Privacy Act (generally as an APP entity, and Part IIIA in relation to credit providers) while others (for example, providers of BNPL products) are not currently regulated by the Credit Act for the provision of 'credit-type' products.<br><br>We consider the extension of the CDR to the NBL sector will improve privacy protections for consumers when compared to current data sharing arrangements being used by NBL sector entities. However, we acknowledge Treasury's concern that the CDR requirements should be balanced against the substantial costs of compliance with the CDR, especially for smaller players in the NBL sector, and the important role those entities have in facilitating innovation and encouraging competition.<br><br>We note that Treasury has sought feedback from industry as part of the consultation about the *de minimis* threshold and, based on the feedback we |

[46] See NBL CDR Rules definition of *excluded data holder* Schedule 3 item 1.2 (clause 1.1A).

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | | | have reviewed (see paragraphs 4.6 to 4.7) industry is generally supportive of a *de minimis* threshold, although the financial threshold proposed varies.<br><br>Some stakeholders recommended Treasury consider what guidance it can provide to non-bank lenders who will not meet the *de minimis* threshold, to support voluntary compliance with the CDR.<br><br>Non-bank lenders who do not met the *de minimis* threshold will be able to elect to share data through the CDR on a voluntary basis. For example, a non-bank lender may voluntarily elect to share "product data" without also needing to share "consumer data". Sharing product data allows entities to have their products considered as part of product comparison services and can be provided at a lower cost than consumer data which requires authentication.<br><br>Participation in the CDR, even on a voluntary basis, increases the safety and security of data sharing.<br><br>In her *Report on the draft Consumer Data Right (Non-bank Lenders) Designation 2022*[47] the Information Commissioner recommended the Treasury consider ways to support NBL sector lenders who choose to voluntarily participate in the CDR to help the understand and comply with their obligations as a data holder (see Recommendation 1(b)).<br><br>We agree that such assistance will help develop the maturity of the NBL sector and improve privacy outcomes for consumers who engage with those NBL sector lenders without the protection of the CDR.<br><br>We make **Recommendation 4** on that basis. |

[47] See Report on the draft Consumer Data Right (Non-bank Lenders) Designation 2022 (oaic.gov.au)

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | | | **Recommendation 4** – Treasury consider ways to support non-bank lenders who do not meet the *de minimis* threshold understand the benefits of the CDR and encourage them to voluntarily participate in the CDR and comply with the obligations of a data holder. |
| ***Categories of CDR data*** | | | |
| *2* | Four (4) categories of information are CDR data sets for the purposes of the NBL CDR Rules being *customer data*, *account data*, *transaction data* and *product specific data*.[48] | The four (4) categories of CDR data identified in the NBL CDR Rules are identical to the categories of CDR data already captured by the CDR Rules for the banking sector (Schedule 3) save for the express exclusion of FHI or repayment history information (as those terms are defined in the Privacy Act) from the definition of *customer data*.<br><br>This CDR data is also broadly consistent with the required data in the energy sector. | Some of the categories of CDR data in the NBL CDR Rules clearly relate to the personal information of consumers. For example, *customer data* which requires the collection of identifying information of a person. Other categories will also include the personal information of customers. For example, *account data* includes information such as "account name" (NBL CDR Rules Schedule 3 item 2(b)(ii)) and "details of payees stored with the account" (NBL CDR Rules Schedule 3 item 2(b)(C)). *Transaction data* includes, relevantly, "any description of the transaction" (NBL CDR Rules Schedule 3 item 3(b)(v)).<br><br>Where this CDR information identifies (or reasonably identifies) at least one person, the Privacy Safeguards apply.[49] This includes Privacy Safeguard 3 in relation to the soliciting of CDR data from a consumer. The data minimisation principle also applies.[50] This principle requires that an accredited person must not seek to collect data beyond what is reasonably needed to provide the good or service to which a consumer has consented, or for a longer time than is reasonably needed.[51] |

[48] See NBL CDR Rules Schedule 1 item 1.3.

[49] See Competition and Consumer Act section 56AI(3)(c)).

[50] See Competition and Consumer Act section 1.8.

[51] See Chapter 3: Privacy Safeguard 3 – Seeking to collect CDR data from CDR participants (oaic.gov.au).

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | | | The basis for the inclusion of categories of information as CDR data was considered in the Banking PIA (save for the express exclusion of FHI or repayment history information from the definition) and broadly consistent with the required data in the energy sector.<br><br>We note feedback from consultation was that the CDR data categories were appropriate for the NBL sector.<br><br>In circumstances where the Treasury (in consultation with the OAIC, ACCC and industry) are satisfied that the CDR data categories continue to reflect data required to be collected for the performance of the sector, we make no recommendations in relation to the CDR data sets.<br><br>See below for a discussion about FHI or repayment history information from the *customer data* CDR data set. |
| *3* | Express exclusion of FHI and repayment history information from the *customer data* CDR data set. | The CDR Rules for the banking sector do not currently exclude FHI and repayment history information (as defined in the Privacy Act) from the *customer data* CDR data set.<br><br>By the NBL CDR Rules this category of data will be excluded from the CDR and the application of the Privacy Safeguards. | See our discussion at Issue 2 above (page 13) in relation to the exclusion of FHI and repayment history information from "customer data" but noting that financial history information and repayment history information may be inferred from transaction data.<br><br>See **Recommendation 2** above. |
| *4* | The NBL CDR Rules will implement the same approach to historical data and closed accounts as is currently set out | The CDR for the banking sector deals with historical data and closed accounts in Schedule 3, clauses 3.2(4) and 3.2(5). It provides that the following data is not *required* | By the NBL CDR Rules[52] the Treasury will take the same approach as it has taken in the CDR Rules for the banking sector in relation to historical data sharing. |

[52] NBL CDR Rules Schedule 3 item 3.2 (clause 3.2(5) and (6)).

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | in the CDR Rules for the banking sector. | *customer data* for the purposes of the CDR in the following circumstances:<br>(a) where an account is open: transaction data that is more than 7 years old, and data on direct debits more than 13 months old<br>(b) where an account has been closed for more than 24 months: account data, transaction data, and product specific data<br>(c) where an account has been closed for any period of time: all data on direct debits, and<br>(d) where an account has been closed for less than 24 months: transaction data for a transaction that occurred more than 12 months before the account was closed. | Feedback from consultation was that the treatment of historical data and closed accounts was appropriate for the NBL sector.<br>Some feedback received on the NBL sector Design Paper recommended the Treasury consider the approach taken in the CDR to the handling of historical data sets, in view of recent high profile data breaches and changing community attitudes about the retention of historical data. In these circumstances, certain stakeholders recommended Treasury consider whether the limitations in terms of historical data sharing are sufficient and adequately address the privacy risks to consumers in the sharing of historical data. Other stakeholders noted the value of historical data in providing a complete picture of the consumer's financial position so that a data holder can provide goods / services tailored to their needs.<br>This recommendation goes beyond the scope of this supplementary PIA on the CDR for the NBL sector. However, we consider that the existing rules around historical account data are sufficient to mitigate this privacy risk. |
| ***Types of products*** | | | |
| *5* | Inclusion of BNPL products in the definition of *covered products*. | The CDR Rules for the banking sector do not currently include BNPL products in the definition of *phase 1* | The NBL CDR Rules proposes to include BNPL products as *covered products* for both the banking and NBL sector. This inclusion will add a new product category to the CDR. |

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | | *product*, *phase 2 product* or and *phase 3 product*.[53]<br><br>By the NBL CDR Rules, BNPL products will be included in the definition of *covered products* in both the NBL sector and the banking sector and the collection and handling of those BNPL products will be subject to the CDR and the Privacy Safeguards. | See our comments in relation to Issue 4 (page 16) and **Recommendation 3** above. |
| *6* | White labelling has been identified as a practice which presents unique privacy risks given it involves multiple businesses providing a product, so it is not always clear who is the relevant CDR participant and which entity will receive and use a customer's data. This risk is magnified in the NBL sector, given the number of smaller entities offering white labelled products. | | No specific provisions are made in the NBL CDR Rules for data holders with respect to white labelling. Accordingly, the approach taken in the CDR applies which allows for data holder obligations to be managed between the white labeller and brand owner to ensure the entity most suitable for meeting data holder obligations can provide the required data.<br><br>Some stakeholders have raised the concern that the use of white labelling can give rise to unique privacy risks in circumstances where it is common practice in the banking sector and that this risk is magnified in the NBL sector, given the number of smaller entities. Some stakeholders are concerned that this practice has the potential to undermine informed and specific consent. In light of this, some stakeholders recommended that Treasury should consider whether additional protections are required for the NBL sector, given the prevalence of white labelling in the NBL sector.<br><br>It is not clear to us how the practice of white labelling gives rise to privacy risks in the context of a customer data request in circumstances where arrangements are made between parties to a white labelling arrangement as to who has responsibility for responding to a data request (accordingly, |

[53] See *Competition and Consumer Act 2020* (Cth) Schedule 3 clause 1.4.

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | | | the data sharing principle is still achieved) and the customer's consent is required.<br><br>Further, in respect of a product data request, we do not consider white labelling arrangements give rise to a privacy risk in circumstances where product data is not personal information (but information about the product, its features, fees, charges and eligibility criteria).<br><br>We note that white label brands need to be published on the CDR Register which is consistent with transparency requirements.<br><br>We make no recommendations in respect to white labelling on that basis. |
| 7 | Inclusion of arrangements for trial products. | The CDR Rules for the banking sector do not currently make provision of trial or pilot products. | The NBL CDR Rules defines a 'trial product' as a product which is:<br><br>(a) described as a 'trial or pilot'<br><br>(b) not offered for more than 6 months (trial period)<br><br>(c) is limited to not more than 1,000 customers, and<br><br>(d) includes a statement that the product may be terminated before the end of the trial period in which case the CDR data in relation to the trial product may not be available,<br><br>unless the trial product is a *covered product*, in which case once it ceases to be a trial product the CDR data generated while the product was a trial is taken to be *required consumer data*, *required product data*, or *voluntary consumer data* for the purposes of the CDR.[54]<br><br>Trial product data will continue to be protected by the Privacy Safeguards for the duration of the trial.<br><br>While we note that some stakeholders had concerns about the length of the trial period and the customer threshold number not being high enough, we |

[54] See NBL CDR Rules Schedule 3 item 1.5.

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | | | consider the proposed approach to trial products to be appropriate from a privacy perspective and balances the privacy needs of customers with encouraging NBL sector entities to continue to innovate and offer new products to the market.<br><br>We make no recommendation in relation to trial products on that basis. |
| ***Other issues*** | | | |
| *8* | The phased implementation of the CDR to the NBL sector. | This is a new concept for the NBL CDR Rules. | The NBL CDR Rules propose the phased implementation of the CDR to the NBL sector as detailed in Schedule 3, Part 6 clause 6.1.[55]<br><br>Treasury has indicated in its NBL sector Design Paper that the basis for the phased implementation of the CDR to the NBL sector is to allow sufficient time for relevant non-bank lenders to comply with the CDR. This also gives data holders time to build for their data sharing obligations and develop more sophisticated and secure CDR systems (including IT systems). While not strictly a privacy issue, we consider this approach is sensible having regard to the diversity of players in the NBL sector.<br><br>Some stakeholders are supportive of the phased implementation of the CDR to the NBL sector and have suggested that this phasing period be no less than 12 months from the making (amendment) of the NBL CDR Rules to ensure data holders have an opportunity to understand the requirements and their compliance obligations and have sufficient time to prepare to comply.<br><br>Some stakeholders have expressed concern that, due to the significant technical and compliance uplift required, a longer transition period is necessary, and that reconsideration of the proposed timelines for implementation should be undertaken. Stakeholders have also expressed concerns regarding awareness of the CDR expansion to the NBL sector |

[55] See Draft NBL CDR Rules Schedule 3 clause 6.1.

| No. | Issue/Risk | Existing mitigation strategies | Gap analysis and privacy recommendation |
|---|---|---|---|
| | | | among non-bank lender, suggesting that further awareness campaigns may be required.<br><br>We consider the proposal to phase the implementation of the CDR to the NBL sector does not give rise to any high privacy risks and recognises the scale of the regulatory change for the NBL sector.<br><br>Having said that, having regard to stakeholder feedback about the NBL sector awareness (and preparedness) for compliance with the CDR, we make **Recommendation 5**.<br><br>**Recommendation 5** – Treasury monitor the implementation of data holder's obligations to see if any privacy concerns arise.<br><br>Treasury should engage with industry and stakeholders to identify instances where the information security / privacy-related IT infrastructure is particularly difficult to implement and if so, consider whether the timing of obligations should be amended. |

# 6 Overall Analysis

6.1 We have made several recommendations in order to mitigate the privacy risks associated with the Project.

6.2 Subject to the Treasury's consideration of our recommendations and observations in this supplementary PIA, we believe that the privacy risks associated with the Project can be effectively managed and mitigated against.

6.3 We otherwise remind the Treasury of the importance of ensuring that as the Project advances, further privacy risks may arise. As such we recommend reviewing this supplementary PIA to address emerging risks and issues.

# 7 Next Steps

7.1 We would be pleased to discuss our draft recommendations with you and discuss the next steps.

Chantal Tipene, Partner
t: +61 2 9260 2542
e: Chantal.Tipene@sparke.com.au

# Attachment A Glossary

In this supplementary PIA, terms defined in **bold** have the following meaning:

| | |
|---|---|
| **2019 Banking PIA** | November 2019 – Implementing the CDR to give consumers better access and control over their data available at Consumer Data Right \| Treasury.gov.au |
| **2019 CDR PIA** | March 2019 – Implementing the CDR to give consumers better access and control over their data available at Consumer Data Right \| Treasury.gov.au |
| **2020 Energy PIA** | June 2020 – Supplementary PIA focusing on expanding the CDR to the energy sector available at Consumer Data Right \| Treasury.gov.au |
| **ACCC** | Australia Competition and Consumer Commission |
| **APPs** | Australian Privacy Principles |
| **BNPL** | Buy Now, Pay Later |
| **CCR** | Comprehensive Credit Regime |
| **CDR** | Consumer Data Right as set out in Part IVD of the Competition and Consumer Act |
| **CDR Rules** | *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) including Schedule 3 in respect to the banking sector |
| **Competition and Consumer Act** | *Competition and Consumer Act 2010* (Cth) |
| **Credit Act** | *National Consumer Credit Protection Act 2009* (Cth) |
| **DSB** | Data Standards Body |
| **FHI** | Financial hardship information as defined in section 6QA(4) of the Privacy Act |
| **NBL Sector Designation** | *Consumer Data Right (Non-Bank Lenders) Designation 2022* (Cth) |
| **NBL CDR Rules** | *Competition and Consumer (Consumer Data Right) Amendment Rules (No 2) 2023* as at 27 November 2023 |
| **NBL sector Design Paper** | *Consumer data right in non-bank lending CDR rules and data standards design paper* dated December 2022 accessed at Consumer data right in non-bank lending - CDR rules and data standards design paper (treasury.gov.au). |

| | |
|---|---|
| **NBL Sector PIA** | PIA update: examining the privacy impact of designating the non-bank lending sector to the CDR dated August 2022 (see Attachment A to the NBL Sector Report) |
| **NBL Sector Report** | *Consumer data right: Non-bank lending sectoral assessment* final report dated August 2022 available at Consumer Data Right – Sectoral Assessment for Non-Bank Lending – Final Report \| Treasury.gov.au |
| **OAIC** | Office of the Australian Information Commissioner |
| **PIA** | Privacy Impact Assessment undertaken in accordance with the OAIC's *Guide to undertaking privacy impact assessments* |
| **Privacy Act** | *Privacy Act 1988* (Cth) |
| **Privacy Safeguards** | the privacy safeguards set out in Part IVD of the Competition and Consumer Act and the application of those privacy safeguards to the CDR in Division 7.2 of Part 7 of the CDR Rules |