Australian Government

Office of the Australian Information Commissioner

Submission to Treasury's Consumer Data Right Non-bank Lenders Rules Consultation 2023

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

5 October 2023

OAIC

Contents

Part 1: Introduction

1.1 The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on Treasury's exposure draft of the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2023* (draft rules). In making this submission, we considered the draft explanatory materials, amending instrument and draft supplementary Privacy Impact Assessment (draft PIA) published as part of public consultation.

1.2 Under Part IVD of the *Competition and Consumer Act 2010* (CCA), the Secretary to the Treasury must consult the Information Commissioner before rules are made on the likely effect of making the instrument on the privacy or confidentiality of consumers' information.[1]

1.3 The Information Commissioner's report on the draft designation instrument for the non-bank lenders (NBL) sector (s 56AF report) identified privacy risks and made three recommendations to mitigate those risks. This submission examines whether our recommendations have been addressed and the extent to which the draft rules adequately mitigate the identified privacy risks. We conclude that further work needs to be undertaken in this regard. This submission also considers other privacy and confidentiality impacts arising from the draft rules. We are available to discuss our submission with Treasury.

Expansion to the NBL sector and associated privacy risks

1.4 We generally support Treasury's proposed approach to align, where appropriate, the rules in the NBL sector with the existing banking sector. However, there are key differences in the data holder and consumer cohorts in these sectors requiring separate consideration of the privacy and confidentiality impacts that may arise from extending the Consumer Data Right (CDR) to the NBL sector.

1.5 The draft rules expand the CDR to the NBL sector by amending Schedule 3 of the *Competition and Consumer (Consumer Data Right) Rules 2020* (CDR Rules), which currently applies to banking, to both the banking and NBL sectors. The draft rules make changes to the CDR for the banking sector, including a schedule for staged implementation of obligations and arrangements for entities transitioning to the banking sector.[2]

1.6 The draft rules apply the following elements of Schedule 3 to non-bank lenders:

- eligibility requirements for consumers seeking to make requests for CDR data
- the products covered by the CDR and data sets that may, or must, be provided on request
- the NBL data holders required to share CDR data, and
- requirements for internal and external dispute resolution.

[1] See ss 56BQ and 56BR of the *Competition and Consumer Act 2010 (Cth)* (CCA).

[2] The draft rules also introduce an obligation for energy retailer data holders regarding the transfer of product data requests in the energy sector.

1.7 The draft rules also apply changes to the obligations of data holders in both the banking and NBL sector. These include:

- introducing buy now pay later (BNPL) products into the CDR
- excluding from the meaning of 'account data' information relating to 'financial hardship information' and 'repayment history information' as defined in the *Privacy Act 1988* (Privacy Act)
- excluding consumer data relating to debts bought by debt buyers or debt collections from the definitions of voluntary consumer data and required consumer data.

1.8 Treasury expects that extending the CDR to the NBL sector will facilitate more informed consumer engagement with both banks and non-bank lenders. Treasury's view is this will lead to improved financial outcomes for individuals and businesses and increase the availability of data, encouraging innovation in financial technology and helping consumers to better understand and manage their finances.[3]

1.9 We acknowledge the potential benefits of expanding the CDR to the NBL sector including benefitting consumers by enabling them to form a better understanding of their financial situation and make more informed decisions about suitable financial products. However, expansion of the CDR to the NBL sector also:

- introduces more entities into the CDR system. These entities may operate under varying business models and may be subject to varying degrees of regulation which can impact regulatory, privacy and security maturity and potential compliance with CDR obligations
- increases the volume of consumer data able to be shared in the CDR especially financial information from banking and NBL sectors.

1.10 This may give rise to increased privacy risks for consumers. For example:

- financial information sourced from the NBL and banking sectors provide a comprehensive picture of an individual's financial circumstances, including if they are experiencing financial hardship
- financial information can also reveal information about an individual which may be derived from their spending habits, such as health information contained in their transaction history where an individual has sought health services, or other sensitive information about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations.[4]

1.11 Expanding the CDR into the NBL also will potentially introduce new consumers to the CDR system. While not exclusively, the NBL sector offers a range of products to borrowers who may not meet the traditional lending criteria of banks. There may be a higher proportion of consumers in the NBL sector who may be experiencing financial hardship or vulnerability

[3] See Exposure draft explanatory materials, pg 1

[4] Section 6 of the Privacy Act defines 'sensitive information'.

and rely on access to certain credit products offered by the NBL sector, such as short-term consumer credit contracts (also known as pay day loans) and BNPL products.

1.12 While the CDR may allow consumers to build a more complete picture of their financial situation and access products better tailored to their circumstances, it is important to ensure that increased data sharing does not increase the risks of products being marketed to consumers that are inappropriate for their circumstances.

1.13 Treasury released a draft PIA with its consultation on the draft rules to support its consideration of privacy risks with the introduction of the NBL sector. The Information Commissioner's s 56AF report recommended that Treasury undertake a PIA to inform the development of the rules, and identified several relevant matters the PIA should consider.[5] The OAIC considers that several relevant matters recommended by the s 56AF report have not been fully addressed in the PIA. Further, earlier preparation of the PIA would have provided greater assurance that privacy risks arising from the expansion of the CDR to the NBL sector have been considered through both the design and rules drafting stages. This includes ensuring that the rules reflect and, where possible, effectively mitigate privacy risks for consumers.

Part 2: About the OAIC and our role in the CDR system

2.1 The OAIC is Australia's independent regulator for privacy and freedom of information. The OAIC co-regulates the CDR system together with the Australian Competition and Consumer Commission (ACCC). The OAIC enforces the Privacy Safeguards contained in Part IVD of the CCA as well as the privacy and confidentiality related CDR Rules. The OAIC also has a number of statutory and guidance functions under the CDR framework. For example, the OAIC provides advice to the Minister and CDR agencies on the privacy implications of designation of a potential sector and making CDR Rules,[6] recognising an external dispute resolution scheme,[7] and makes guidelines on the operation of the Privacy Safeguards.[8]

2.2 The OAIC is also responsible for undertaking strategic regulatory and enforcement action in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of CDR data.

---

[5] To be effective, a PIA should be an integral part of the project planning process not an afterthought. It should be undertaken early enough in the development of a project that it is still possible to influence the project design. A PIA works most effectively when it evolves with and helps to shape the project's development, ensuring that privacy is considered throughout the planning process.

[6] The OAIC has a number of formal statutory functions under Part IVD of the CCA in relation to the making of CDR Rules and designation of a potential sector. For example, being consulted about the making of proposed CDR Rules and potential designated sectors (sections 56AD(3) and 56BQ), analysing the privacy impacts in relation to the making of proposed CDR Rules and potential sectors to be designated when consulted (sections 56BR and 56AF), and producing a report about an instrument to designate a sector (section 56AF).

[7] Section 56DA(4) of the CCA requires the Minister to consult with the Information Commissioner before recognising an external dispute resolution scheme under s 56DA(1).

[8] Under section 56EQ of the CCA, the Information Commissioner must make guidance for the avoidance of acts or practices that may breach the privacy safeguards.

2.3 Our goal as regulator of the privacy aspect of the CDR system is to ensure that there is a robust data protection and privacy framework and effective accountability mechanisms to ensure consumers' CDR data is protected.

Part 3: Comments on issues raised by draft rules

Products in scope and risks to privacy

3.1 The NBL sectoral assessment report indicated the inclusion of particular NBL products and operation of direct marketing consents on high-cost products would be considered at the rule making stage.

Covered product

3.2 The draft rules define 'covered product', specifying products for the banking and NBL sectors as well as the banking sector only.[9] The products in the draft rules that may be a 'covered product' mirror those currently specified in banking except for the addition of BNPL. The draft rules do not specifically exclude any NBL products.

High-cost products

3.3 The draft PIA identifies three high-cost products but does not provide analysis of the risks and benefits of including these products in the CDR. It notes:

- a product-by-product review of NBL products is not required because the products that may be 'covered products' are the same as are currently covered in banking (except for BNPL)
- 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
- the CDR operates alongside regulatory frameworks for the banking sector, including the *National Consumer Credit Protection Act 2009* (the Credit Act), which provide a range of protections to prevent lenders from targeting consumers with inappropriate lending products. There are also anticipated reforms to regulate BNPL products.

3.4 The NBL sector is comprised of a different cohort of participants and consumers and carries different risks from those in the banking sector which should be considered separately. For example, the NBL sector will potentially include a greater proportion of consumers experiencing financial hardship or other types of vulnerability than the banking sector, and consumers who may rely on access to high-cost products offered by the NBL sector.

3.5 We reiterate the Information Commissioner's recommendation 1(d) from the s 56AF report to consider the impact of products offered by the NBL sector including through

[9] See draft clause 1.4 of Schedule 3

consultation with consumer advocacy groups who will have knowledge/experience with high-risk products and how they may impact consumers experiencing vulnerability.

Monitoring reforms to regulation of certain products

3.6 In relation to high-cost products, the draft PIA refers to recent reforms to the Credit Act and the proposed regulation of BNPL products.

3.7 We are aware the Government is taking steps to regulate BNPL and recently announced BNPL will be subject to regulation under the Credit Act.[10] Under the proposed changes, providers would be required to have a credit license, hardship requirements and minimum standards for conduct. The *Financial Sector Reform Act 2022* also introduced changes to the regulation of pay day loans and consumer leases, including limits on fees and repayments, mandatory information for consumers, and assessments around product suitability.

3.8 The draft PIA recommends Treasury monitor where high-cost products are being actively considered by the Commonwealth for regulation. Recommendation 2 of the draft PIA states:

> *Treasury monitor the regulation of 'high-cost' products in order to determine whether the inclusion of **BNPL products** in the CDR is consistent with those reforms. If those reforms strengthen the privacy position in relation to 'high-cost' products beyond the Privacy Safeguards and the CDR (for example, in relation to the marketing of 'high-cost' products), we recommend the Draft NBL CDR Rules be revisited to ensure the CDR does not reduce the effectiveness of those reforms.*[11]

3.9 We think this recommendation should be expanded so Treasury also reviews the impact of the recent financial sector reforms on the regulation of pay day loans and consumer leases. Prior to the draft rules being finalised, the PIA should assess if there is consistency and alignment in the policy intent of the reforms and their inclusion in the CDR, including whether the draft rules should be revisited.

3.10 The Information Commissioner's s 56AF report noted that BNPL products represent a potential regulatory gap as not all BNPL providers are subject to responsible lending obligations under the Credit Act. Noting recommendation 2 of the draft PIA and anticipated reforms to BNPL regulation, the OAIC recommends that Treasury delay the introduction of BNPL into the CDR until finalisation of the proposed BNPL reforms.

Direct marketing

3.11 The draft rules introduce no restrictions to the operation of direct marketing consents. The draft PIA acknowledges the profiling and targeting of vulnerable customers by providers of high-cost products could have serious privacy impacts and consequences for affected individuals. However, it considers the risks are appropriately mitigated by the CDR consent

[10] Address to the Responsible Lending & Borrowing Summit | Treasury Ministers

[11] Draft supplementary PIA to expand Consumer Data Right to the Non-Bank Lending sector (19 July 2023), page 16

framework as consumers can refuse to disclose data which may make them a target for the marketing of high-risk products.

3.12 We consider the CDR system should be set up and maintained with protections in place for consumers, without having undue reliance on consent as the main strategy for mitigating risk. Protections offered by the CDR consent framework should be supported by other mechanisms to protect consumers, particularly in relation to specific or identifiable risks, such as may arise where the CDR is facilitating consumers entering into high-cost products. Consumers are not always well-placed to assess the risks and benefits of allowing their data to be shared and analysed in more complex circumstances, and this risk increases where a consumer may be experiencing vulnerability. In particular, consumers experiencing vulnerability may feel reliant on services or payments, may feel a loss of control over their personal information and may feel unable to make meaningful choices about the collection, use and disclosure of their data. When considering measures to mitigate risk, a balance should be maintained between privacy self-management and the obligations on entities to ensure CDR data is handled, used and disclosed appropriately.

3.13 Treasury is separately conducting a review of the CDR's consent framework with a view to identifying opportunities to simplify the CDR Rules and standards in relation to consent.[12] In its submission to the CDR consent review, the OAIC has expressed concern regarding the potential impact of certain proposals on consumer privacy. When relying on the consent framework to mitigate risks, Treasury should consider the impact of proposed changes to the consent framework and how any changes impact the analysis in the PIA for the NBL sector.

Consumer leases and small amount credit contracts

3.14 Reforms to the Credit Act in 2022 introduced a prohibition on providers making unsolicited offers or engaging in unsolicited communications about credit or consumer lease products. However, it is not clear that these reforms will entirely prevent direct marketing of these high-cost products to consumers in the CDR.

3.15 In relation to small amount credit contracts (also known as pay day loans), the Credit Act reforms prohibit a licensee from making, or arranging for the making of, unsolicited communication to a consumer that contains an offer or an invitation for the consumer to apply for a small amount credit contract.[13] The prohibition applies to oral, written or electronic communications where a consumer has previously had, or applied for, a debt or small amount credit contract with the licensee. It will also apply where a consumer had or applied for a small amount credit contract or debt with another credit provider and a reasonable licensee would, if they made reasonable inquiries, be aware of that.

3.16 The Credit Act defines unsolicited communication as a direct communication with a consumer or their agent where no prior request has been made by the consumer for that communication, or where a prior request was solicited by the licensee or their agent.

[12] Treasury is consulting on the Consent Review rules and data standards design paper which proposes changes to the CDR Rules regarding consent.

[13] See s 133CF of the Credit Act

3.17 In relation to consumer leases, the reforms prohibit a lessor from engaging in unsolicited communication with a consumer for the purpose of inducing the consumer to apply for or obtain a consumer lease for household goods.[14] The prohibition is specifically directed at person-to-person 'canvassing', where the communication occurs in the physical presence of the consumer.

3.18 It appears these reforms to the Credit Act would prohibit unsolicited communication, as defined in the Credit Act, in relation to small amount credit contracts and consumer leases in the CDR. However, provided the communication does not contain an offer or an invitation for the consumer to apply for the product, and a consumer has given a direct marketing consent, there appear to be circumstances where direct marketing of these high-cost products would be permissible in the CDR. This may include:

- providing information about upgraded or alternative goods or services to existing goods or services
- providing information about the benefits of existing goods or services
- providing information about other goods or services provided by another accredited data recipient (ADR)
- using CDR data, including by analysing CDR data, in order to send the consumer the above types of information.[15]

3.19 Further, in relation to consumer leases, it appears the Credit Act reforms would not prevent an ADR from engaging in direct marketing via written or electronic communications, in circumstances where the consumer has provided a direct marketing consent under the CDR Rules.

3.20 There is also a question as to whether communications with a consumer provided in accordance with a direct marketing consent under the CDR Rules[16] can be 'unsolicited' for the purposes of the Credit Act. To the extent that a consumer agrees or consents to receiving information or offers about different products or services, Treasury should consider whether this will render such communications permissible under the Credit Act and whether specific prohibitions on direct marketing of these high-cost products are required under the CDR.

3.21 Noting these matters, Treasury should consider potential gaps in the regulation of direct marketing of high-cost products in the CDR and the need for additional safeguards or mitigating measures. Consideration should include whether:

- communications in the CDR that do not contain a direct offer or invitation to apply for a product may not be caught by the Credit Act prohibitions
- prohibitions in the Credit Act in relation to consumer leases would prevent direct marketing of these products in the CDR, and

[14] See Schedule 1, s 179VA of the Credit Act

[15] See r 7.5(3) of the CDR Rules

[16] See r 1.10A(1)(d) of the CDR Rules

- a consumer giving a direct marketing consent in the CDR may overcome the prohibition on unsolicited communication in the Credit Act.

Direct marketing of BNPL

3.22 As noted above, the Government has also announced its intention to regulate BNPL products as credit products, requiring providers to hold Australian Credit Licences and requiring providers to abide by restrictions on marketing.

3.23 Treasury should consider how these proposed reforms are likely to interact with BNPL providers operating in the CDR. Specifically, Treasury should consider whether any restrictions on direct marketing in the Credit Act for BNPL providers would prevent such providers from engaging the same, or similar, conduct in the CDR, and whether any additional safeguards are required in the CDR to protect vulnerable consumers.

Recommendation 1: Treasury should consider the impact of products offered by the NBL sector including through consultation with consumer advocacy groups who will have knowledge/experience with high-risk products and how they may impact consumers experiencing vulnerability.

Recommendation 2: Treasury should review the impact of the financial sector reforms on the regulation of pay day loans and consumer leases to ensure an alignment of policy intent and delay the introduction of BNPL into the CDR until finalisation of the proposed BNPL reforms.

Recommendation 3: Treasury should consider gaps in the regulation, and proposed regulation, of direct marketing for high-cost products in the CDR and identify additional safeguards or mitigating measures.

Excluding information about consumers in financial hardship

3.24 The s 56AF report noted Treasury should closely consider the benefits and risks associated with the designation of financial hardship information at the rule-making stage. There may be circumstances where including this information in the CDR may help consumers experiencing hardship or vulnerability access financial products and services that suit their specific circumstances. However, information about financial hardship and financial vulnerability is particularly sensitive. Given this, and the fact that the NBL sector introduces a separate cohort of consumers to the CDR, some of whom are more likely to be experiencing vulnerability or financial hardship, the extent to which financial hardship information is excluded under the CDR Rules should be clear.

3.25 The draft rules propose excluding from the meaning of ‘required consumer data’ and ‘voluntary consumer data’, CDR data relating to a debt of a CDR consumer, if the data was acquired by a data holder acting in its capacity as a debt collector or debt buyer. The explanatory materials notes this exclusion aims to exclude balances bought from other lenders where the customer is in financial hardship and has defaulted on their payments. Accordingly, the fact that an individual’s debt is with a debt collector is considered likely to signal financial hardship. To protect such individuals, such data is outside the scope of the CDR in the banking and NBL sectors.

3.26 In the sectoral assessment report for the NBL sector, Treasury expressed an intention to exclude financial hardship information,[17] noting this would be consistent with the energy sector and the approach being consulted on, at the time, in telecommunications. The draft rules exclude from the meaning of account data, in the NBL and banking sectors, financial hardship information (FHI) and repayment history information (RHI) as defined by the Privacy Act.

3.27 FHI and RHI are specific categories of credit information[18] created for the purposes of credit reporting under Part IIIA of the Privacy Act, and not all entities participating in the CDR would also participate in credit reporting and be required to create and hold this type of information:

- FHI relates to an arrangement between a credit provider and an individual affecting the monthly repayment obligations of an individual. It is denoted by the presence of a sign next to a repayment on an individual's repayment history in their credit report indicating the individual has a temporary or permanent financial hardship arrangement with a credit provider.[19]
- RHI is information about whether a consumer has met their consumer credit payment obligations in a particular month.[20]

3.28 The Financial Rights Legal Centre submission to the design paper, in discussing the issue of proxy or equivalent indicators of FHI and RHI, suggested it would be 'easy' to look at a consumer's transaction history and product data and identify whether a financial hardship arrangement was in place outside of the 12 month period that FHI is meant to be limited to. For example, this could be done by reviewing mortgage repayments that halved for 6 months three years ago, and then returning to normal, or a mortgage repayment permanently varying.[21]

3.29 Further consideration should be given to the proposed exclusion of FHI noting not all entities operating in the CDR participate in credit reporting, and a financial hardship arrangement may be inferred by a consumer's transaction history and product data. This suggests the proposed exclusion of FHI in the draft rules would not be effective at excluding all types of information which are likely to signal that a consumer is in a financial hardship arrangement.

3.30 The draft PIA uses the acronym 'FHI' when referring to both the exclusion in the draft rules of FHI as defined by the Privacy Act and information about a consumer experiencing financial hardship which could be inferred from a consumer's transaction data. We think it

[17] The Sectoral Assessment Report noted the intention to exclude financial hardship information as defined under the Comprehensive Credit Reporting regime (CCR). We note financial hardship information is defined in s 6QA(4) of the Privacy Act.

[18] See ss6N for the meaning of credit information and 6QA(4) for the meaning of FHI and 6V(1) for the meaning of RHI

[19] See s 6QA of the Privacy Act and OAIC website for What is financial hardship information.

[20] A credit provider can list information about a consumer's repayment history on their credit report including if payments are on time or have been missed. The information is reported as a number on the credit report.

[21] FRLC submission to the CDR design paper: 230201_CDR_NonBankLending_FINAL.pdf (financialrights.org.au)

is important to highlight the distinction between these categories of data in considering the risks of transaction data.

3.31 The draft PIA discusses the risk that information about financial hardship can be inferred from a consumer's transaction data and states:

'… 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.'[22]

3.32 The draft PIA concludes that, to the extent financial hardship information can be inferred from transaction data, the CDR provides adequate protections in respect of the use and disclosure of that data, citing, amongst other things, the requirement for a consumer to consent to the sharing of their data, and the data minimisation principle.[23] As discussed earlier, Treasury should consider how measures under consideration in the CDR consent review to simplify consent are likely to impact the role of consent in providing protections for consumers in the CDR.

3.33 Transaction data can reveal significant information about a person's circumstances. The CDR facilitates the collection of granular and in some instances sensitive personal information. This information can be used to build a detailed profile of an individual, including in relation to their lifestyle, health and habits. Expansion of the CDR to the NBL sector significantly increases the volume of granular information about a consumer able to be collected, used and disclosed.

3.34 While there are existing protections for consumers in the CDR, such as consent, requiring a consumer to understand and manage these risks through the CDR's consent settings may place an undue burden on the consumer. This is particularly the case where risks are complex or relate to uses of CDR data that a consumer might not anticipate or where the consequences for consumers, for example of entering into a pay day loan, are material.

3.35 Noting the introduction of the NBL data to the CDR will enable recipients of CDR data to gain a comprehensive picture of an individual's financial circumstances, Treasury should consider undertaking more analysis of information able to be shared in the CDR which could signal financial hardship, such as transaction data.

3.36 We note that in the energy sector, the CDR Rules exclude from the meaning of account data information about whether the account is associated with a hardship program.[24] The concept of 'associated with a hardship program' is arguably substantially broader than the proposal in the draft rules for the NBL sector which defines financial hardship information by reference to the Privacy Act definition.

---

[22] Draft supplementary PIA to expand Consumer Data Right to the Non-Bank Lending sector (19 July 2023), page 13

[23] In examining how the risks to consumers may be mitigated, the draft PIA also refers to r 3.5(1)(a), which enables a data holder to refuse to disclose required consumer data in response to consumer data request where 'the data holder considers this to be necessary to prevent physical, psychological or financial harm or abuse'. We understand this sub rule has limited operation and is intended to accommodate data holder procedures to protect consumers who may be experiencing family violence. See para 76, Explanatory Statement Competition and Consumer (Consumer Data Right) Rules 2020.

[24] Item 2, r 1.3 of Part 1, Schedule 4 of the CDR Rules

3.37 In our view, Treasury should revisit its policy intent in relation to the exclusion of financial hardship information. Treasury should consider whether the current approach achieves its policy intent, noting that the proposed exclusion of data held by debt collectors or debt buyers suggests an existing intent to exclude information likely to be indicative of financial hardship, beyond the definition of FHI in the Privacy Act. This assessment may include whether a similar approach to that taken in the energy sector, relating to information 'associated with financial hardship', may also be appropriate for NBL and banking.

Recommendation 4: Treasury revisit the approach to excluding financial hardship information in the draft rules. This could include engaging with industry and consumer protection groups about whether there is a suitable NBL and banking sector equivalent of whether an account is associated with a hardship program, consistent with Treasury's intent to adopt the approach implemented in the energy sector.

Recommendation 5: Undertake further analysis of the impact of allowing information from the NBL sector to be shared in the CDR which could signal financial hardship and risk potential consumer harm. The approach to financial hardship in the draft rules should be clearly explained in the explanatory statement.

Interaction between Part IIIA of the Privacy Act and the CDR

3.38 The interaction between the CDR and Part IIIA of the Privacy Act has been subject to some consideration by Treasury in the NBL designation and over the course of the development of the CDR.[25]

3.39 Part IIIA of the Privacy Act and the Privacy (Credit Reporting) Code 2014 regulate the handling of personal information in the credit reporting system. The credit reporting system is a closed system which limits the sharing of credit reporting information between credit providers and credit reporting bodies. By prescribing and limiting the types of information that may be collected and the bodies who may access the information,[26] Part IIIA aims to balance entities' legitimate need to access credit information and the protection of consumer privacy. By contrast, the CDR enables, with consumer consent, sharing of consumer information including financial information to a wider range of CDR accredited or trusted entities.

3.40 Section 56EC(3) of the CCA provides that the CDR does not limit Part IIIA of the Privacy Act, although there is the potential for CDR Regulations to limit specified provisions of Part IIIA. In principle, the two systems can operate concurrently. The CDR Rules cannot permit credit providers or credit reporting bodies to collect, use or disclose CDR data for credit reporting purposes (except in ways where they are already permitted to use that same information under Part IIIA).

[25] See Attachment A of the Consumer data right: Non-bank lending sectoral assessment, Privacy Impact Assessment – Consumer Data Right – March 2019

[26] A CRB may only provider a consumer's credit report to another CRB, a credit provider, a mortgage insurer, a trade insurer, a debt collector acting for a credit provider.

3.41 Subject to some exceptions, the NBL designation provides for consumers to share their credit information in the CDR, mirroring the current arrangements in banking.[27] While credit information may be shared in the CDR in the banking sector, the designation of the NBL sector is likely to amplify risks arising from the interaction of the two systems.

Compliance

3.42 The Information Commissioner's s 56AF report noted that the two regimes are able to operate concurrently. However, the designation of the NBL sector is likely to result in an increased number of credit providers and credit reporting bodies participating in the CDR, and an increased amount of credit reporting information being shared in the CDR and combined with CDR data not subject to Part IIIA. Accordingly, there is a risk that credit providers and credit reporting bodies may face difficulties complying with the differing obligations of each system and will find compliance a more onerous and complex exercise.

3.43 For example, there is a potential for confusion to arise when CDR data and Part IIIA data is mixed and credit providers or CRBs operating in the CDR need to comply with both regimes. In these circumstances, an entity may face the challenge of meeting different regulatory requirements for CDR data, depending on whether it is subject to Part IIIA or not.

3.44 Recommendation 1 of the draft PIA recommends that 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.

3.45 We support, in principle, the development of guidance to assist stakeholders understand their compliance obligations. However, before this recommendation can be considered, additional work is required to identify and articulate the risks associated with the data handling obligations under the two systems and the circumstances in which these obligations are likely to create a burden for entities.

Inconsistency of policy intent

3.46 The OAIC has previously identified potential inconsistencies between the policy objectives of the CDR and credit reporting system.[28]

3.47 While s 56EC(3) of the CCA makes clear that the operation of Part IIIA is not to be directly affected by the CDR and the sharing of credit information in the CDR must conform with Part IIIA, the CDR creates avenues to share similar types of financial information beyond what is currently prescribed and limited under the Part IIIA framework. It also allows insights from more granular information to be drawn and this may be equivalent or similar information to credit reporting information. For example, insights from granular transaction data may be drawn by an ADR about a consumer's financial situation. This may

[27] As with banking, the NBL designation excludes credit information defined under s 6N(d), (i), (j), (l), and s 6S(2) of the Privacy Act. The draft rules also propose to exclude FHI and RHI, which are also categories credit information under s6N, from the meaning of account data.

[28] OAIC submission to the CDR Rules Expansion Amendments consultation | OAIC

occur without the consumer's consent or knowledge – while the consumer is required to consent to sharing their transaction information with an ADR, they may not anticipate how the ADR may use the data to analyse and draw interferences about their financial situation.

3.48 Given the potential expansion of the amount of credit-related information being shared in the CDR with introduction of the NBL sector, Treasury should ensure that the rules are consistent with Part IIIA of the Privacy Act and that credit information is not being shared in the CDR in a manner that undermines or is inconsistent with entities' Part IIIA obligations. Further consideration should be given to the tension between the framework and policy objectives of the two systems and outcomes for consumers.

3.49 The Information Commissioner's s 56AF report recommended that Treasury engage with the Attorney-General's Department in relation to the consultation for the independent review of Part IIIA. We reiterate this recommendation, noting this would support Treasury's consideration of the interaction between the CDR and Part IIIA of the Privacy Act, and the impact of increasing volumes of credit reporting information being shared in the CDR.

Recommendation 6: Treasury should undertake targeted consultation with consumer and industry stakeholders to better understand the compliance challenges and risks associated with the differing data handling obligations for entities operating under the two systems.

Recommendation 7: We reiterate recommendation 3 of the Information Commissioner's s 56AF report in relation to the interaction between CDR and Part IIIA of the Privacy Act and recommend Treasury ensure the rules are consistent with Part IIIA of the Privacy Act.

Excluded data holders and application of a de minimis threshold for mandatory data holders

3.50 During consultation on the sectoral assessment and draft designation instrument, we raised the importance of ensuring non-bank lenders in the CDR system have privacy and data security awareness and the regulatory maturity and capability to comply with obligations as a mandatory data holder as well as broader privacy awareness. This is critical to upholding consumer privacy and security and maintaining trust in the CDR system.

3.51 The draft rules establish definitions for initial and large providers who will be subject to mandatory data sharing obligations. We generally support the establishment of a de minimis threshold that would exclude entities that are unlikely to have an appropriate level of privacy and data security awareness and the regulatory maturity and capability to comply with the CDR Rules. We note the proposed de minimis threshold for large providers is likely to capture mandatory data holders subject to the Privacy Act with the regulatory maturity and capability for complying with CDR obligations.

3.52 The Information Commissioner's s 56AF report recommended that the PIA consider ways to support non-bank lenders who choose to voluntarily participate in the CDR to help them understand and comply with their obligations as a data holder. The draft PIA recommends 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.

3.53 In addition to considering ways to encourage voluntary participation, Treasury should ensure adequate support is provided to entities who wish to voluntarily become data holders and who may lack the regulatory maturity and capability of entities captured by the de minimis threshold. Additional support or guidance to smaller voluntary data holders will help to ensure that the CDR system can be more easily understood and operationalised. This may also help guard against misuse of information or risk of error in the application of the privacy safeguards by entities, especially by NBL sector entities voluntarily participating in the CDR who are not subject to the Privacy Act.

Staged implementation

3.54 The draft rules propose dates for the staged implementation of data sharing obligations for initial and large non-bank lenders. These are further divided into product data requests, consumer data requests (excluding complex data requests) and complex consumer data requests.

3.55 The explanatory materials note the proposed dates may be adjusted in response to stakeholder feedback. We strongly recommend Treasury ensure the timeframe for implementation is adequate to ensure data holders can meet their obligations under the rules. Noting the complexities that may arise for participants in ensuring they have systems in place to meet their CDR obligations, we suggest the timeframe should be no less than 12 months from the making of the rules and commencement of obligations. This should be subject to stakeholder input and the impact of other proposed changes to the CDR system.

3.56 We also note two issues for consideration in relation to compliance arrangements for large providers and BNPL products in the banking sector:

- **Deferred compliance for large providers**: the draft rules include deferred compliance arrangements for large providers depending on when they meet the definition of a large provider. Entities who become a large provider after 1 November 2023 will begin having obligations on the date they meet the definition of a large provider. This approach may result in complexity from a regulatory oversight perspective as entities may meet the definition of large provider on different dates.

- **BNPL compliance schedule**: the draft rules include a compliance schedule for the commencement of data sharing obligations by banking data holders that offer BNPL products. Treasury proposes that if a banking data holder starts to offer a product after 1 November 2024, obligations for product, consumer data and complex consumer data requests will commence after specific timeframes set out in the draft rules. Given commencement of obligations are based on the date the data holder started to offer that product, this could result in complexity in ascertaining when a banking data holder is subject to data sharing for BNPL. We recommend Treasury consider stakeholder feedback and examine the viability of alternative approaches for streamlining obligations.

3.57 We suggest Treasury engage with stakeholders, including relevant CDR agencies, to assess the impact of this approach to compliance obligations and whether alternative approaches to streamline obligations may be available. Treasury should also consider whether

additional record keeping obligations may be necessary to support visibility of the commencement of compliance obligations for individual data holders.

Historical data sharing

3.58 The draft rules apply the same limitations on required consumer data as contained in the banking rules. This enables consumers to share account data, transaction data and product specific data generated over the preceding 7 years. This contrasts with the energy sector, where sharing of transaction data is limited to the preceding 2 years.

3.59 The draft PIA notes that the approach to historical data sharing was consulted on in the design paper but finds that the issue is outside the scope of the PIA. It also concludes that the CDR Rules around historical account data are sufficient to mitigate the privacy risk. The explanatory materials do not identify why this approach to historical data sharing has been adopted and is appropriate for the NBL sector.

3.60 We note there may be benefits in achieving consistency across the banking and NBL sectors, however in light of recent data breaches and increasing community concern over retention of historical data, closer examination is required to ensure that the approach is fit-for-purpose and adequately balances, and addresses, the risks and benefits to consumers. This assessment should include the types of data shared in NBL and the data reasonably required by participants to support their use cases, as well as any potential gaps, noting certain categories of data in the banking sector do not appear to be subject to any limitations in terms of historical data sharing in the CDR Rules.

Recommendation 8: Treasury should examine the benefits and risks to consumers of the proposed approach to historical data sharing, including the types of data being shared in NBL, the amount of data required by participants to support their use cases and whether any gaps in the limitations on historical data sharing are likely to present privacy risks for consumers.

Recommendation 9: To support consistency and transparency, the proposed approach to historical data sharing should be explained in the explanatory materials.