Australian Government

Office of the Australian Information Commissioner

2021 Independent review of the Privacy (Credit Reporting) Code

September 2022

20 September 2022

OAIC

Contents

Foreword from the Commissioner

Credit reporting in Australia is fundamental to a functioning economy. The credit reporting system has been subject to significant changes over the past two years including through the introduction of mandatory comprehensive credit reporting, and amendments to Part IIIA of the *Privacy Act 1988* (the Privacy Act).

Protecting the way Australian's personal information is collected, handled and stored is more than ever, an important objective as the credit reporting landscape has expanded and shifted.

As a contemporary regulator, the OAIC seeks to respond to government and community public expectations when exercising our regulatory responsibilities and powers under the Privacy Act.

The OAIC has undertaken a major review of the *Privacy (Credit Reporting) Code 2014* (the CR Code) to ensure it remains fit for purpose - that it provides appropriate guardrails for regulated entities in complying with Part IIIA of the Privacy Act and that it provides adequate privacy protections for individuals. Under the CR Code the OAIC is required to commence an independent review of the practical operation of the CR Code every 4 years.

I am pleased to present the outcomes of the review in this report. These findings are the result of significant engagement by the OAIC with informed and committed stakeholders on how the CR Code is operating in practice, and ways in which it can be improved to ensure the privacy of individuals is respected, while facilitating an efficient credit reporting system in Australia. Regular review of the CR Code provisions, and their operation is fundamental to ensuring the CR Code is achieving these important objectives.

The Review resolved a number of issues occurring within industry and found that further changes need to be made. It makes proposals to better protect the rights and interests of consumers and provide greater clarity for industry on their obligations.

The OAIC plans to implement the proposals outlined in this report in the next 2 years and to take proactive steps to ensure issues identified with Part IIIA of the Privacy Act are brought to the attention of the Attorney-General for the independent review required by statute to be completed in 2024. The OAIC looks forward to continued engagement from stakeholders in the implementation of these proposals for the benefit of all Australians.

Angelene Falk
Australian Information Commissioner
Privacy Commissioner
20 September 2022

Executive summary

The *Privacy (Credit Reporting) Code 2014* (the CR Code) is a legislative instrument under the *Privacy Act 1988* (the Privacy Act). Its objective is to provide further particularisation to regulated entities as to how they should comply with their obligations set out in Part IIIA of the Act. The CR Code includes an important governance mechanism, which requires the OAIC to commence an independent review of the practical operation of the CR Code every 4 years. In 2021, the OAIC commenced its second independent review (the Review) of the CR Code.

The Review presented an important opportunity to reflect on the practical operation and effect of the CR Code, and to evaluate whether it continues to deliver its intended objective. It also provided an opportunity to consider the operation of the CR Code amid social, technological, and regulatory developments. The Review sought stakeholders' feedback on their practical experiences with the CR Code, including what is working well and what could be improved. The Review also sought stakeholders' views on whether there were any opportunities to improve the operation of the CR Code more broadly, and if so, how those could be implemented.

In finalising the Review, the OAIC gave significant consideration to the views provided by stakeholders during the consultation process. We thank all stakeholders for their robust engagement in this process. This engagement has allowed the OAIC to holistically consider the operation of the CR Code. The OAIC recognises that credit reporting information is a significant kind of personal information that has real impacts on an individual's life – their ability to obtain credit affects livelihoods and the ability to engage in society.[1] The OAIC is committed to fulfilling its role in regulating the credit reporting provisions of the Privacy Act to ensure the privacy of individuals is respected.

This report seeks to deliver real, tangible outcomes to address the issues raised by stakeholders. As a result, we focused on steps that can be taken now to resolve issues raised in the review. We consider that the implementation of the remaining issues fell into four categories:

- proposals which require an amendment to the CR Code
- proposals to increase education and awareness
- proposals focused on compliance and monitoring, and
- proposals where legislative amendment to Part IIIA of the Privacy Act would be needed to address the issues raised. The Attorney-General is required to cause an independent review to be conducted of the operation of Part IIIA by October 2024.[2]

All issue resolutions and proposals are summarised, by category, in the below table.

OAIC resolutions of practice issues

During the consultation process, several issues were raised by stakeholders which went to the application of the Privacy Act and the CR Code in certain scenarios. The OAIC has provided a view on a

[1] See Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012 under 'Clause 20R'.

[2] See Privacy Act, s 25B.

number of these issues through this Review process, and these are presented throughout this report as OAIC Resolutions of Practice Issues.

The OAIC will consider further whether these issues need to be drawn out in comprehensive guidance issued to industry to encourage consistency.

These resolutions of akin to Guidance notes and have been made to encourage industry best practice in relation to the specific circumstances as outlined in this Review report. They are case and time specific to this report and do not constitute legal advice. They will not apply to all scenarios or situations, and an entity should check the accuracy, currency, and relevancy of the Guidance notes in relation to their circumstances before taking any action based on these Notes. An entity may wish to seek independent legal advice where appropriate.

Proposals to amend the CR Code

A number of issues raised by stakeholders could be resolved through amendments to the CR Code. These amendments range from minor adjustments to ensure the smooth functioning of the CR Code, through to significant changes that enhance individual rights (e.g. expanded correction provisions) and the operation of credit reporting (e.g. introduction of 'soft enquiries').

Where proposals relate to CR Code amendments, these amendments will be subject to further consultation from all stakeholders in accordance with the variation process.

The Review has also presented a complementary proposal that the OAIC will review and update its *Guidelines for Developing Codes* to provide further particularity and clarity around the OAIC's expectations on how variations to the CR Code will be developed. This includes consideration of the need for all stakeholder groups to have early input on the framing of issues before drafting commences. It is expected that the CR Code amendments proposed in this report will follow these updated guidelines.

Proposals to improve overall education and awareness

The Review recognises that the OAIC plays an important role in providing education and guidance to the Australian community. To achieve this, the OAIC has published a number of resources related to credit reporting on its website. However, feedback from the Review has indicated that there is a need among consumers for further education and clarity about the operation of the CR Code, particularly when it comes to advocating for their privacy rights.

To address this, the report presents a series of proposals aimed at education for individuals and their advocates. In particular, the Review proposes that the OAIC review its existing material, and where appropriate, develop additional targeted resources on the issues identified in this Review. The OAIC will also consider changes that can be made to how it provides materials to stakeholders and the form of this material, to ensure that they are promoted and easily accessible.

Proposals focussed on compliance and monitoring

Stakeholders raised concerns about industry compliance with the credit reporting system, along with the importance of the OAIC being appropriately resourced to undertake monitoring and enforcement activities. The report presents proposals which are focused on the Information Commissioner's role in regulating credit reporting and are aimed at most effectively and efficiently utilise the tools currently

available in the OAIC's regulatory toolkit. The Review notes that the broader ongoing review of the Privacy Act may present opportunities to further enhance these proposals.

Proposals to raise Part IIIA issues with Government

Stakeholders raised concerns about the operation of certain regulatory provisions, as well as aspects of credit reporting more broadly, which are beyond the scope of the CR Code because they require amendments to Part IIIA of the Privacy Act. In these circumstances, the OAIC will write to the Attorney-General about these issues, so that they can be considered by the reviewer in the required independent review of Part IIIA of the Privacy Act due to be completed by 1 October 2024.[3]

[3] Privacy Act, s 25B.

OAIC resolutions of practice issues

OAIC resolution	Report reference
Resolution of practice issue	
Resolution 1 – CRBs should have appropriate controls in place to quarantine information from future use or disclosure, where necessary	3.2.2
Resolution 2 – CRBs should only disclose current information when disclosing CCLI	4.1.4
Resolution 3 – CRBs can collect and use personal information for the purposes of communicating with individuals to whom the information relates, regarding credit bans	5.2.2
Resolution 4 – CRBs must provide access seekers with a copy of credit reports free of charge, once every 3 months	5.3.3
Resolution 5 – CRBs should recognise standard authorities from advocates	5.3.4
Resolution 6 – CRBs must provide access to advocates during a ban period where consent provided	5.3.4
Resolution 7 – Real estate agencies and employers must not seek access to an individual's credit reporting information	5.3.5
Resolution 8 – CRBs and CPs can share contact information for the purposes of actioning a correction request	5.4.1
Resolution 9 – CRBs and CPs should actively resolve correction requests as soon as practicable	5.4.5
Resolution 10 – CPs and CRBs should make individuals aware of their options, such as where customer-based reporting may be available, when experiencing domestic abuse	5.6.2
Resolution 11 – Mortgage brokers should use the access seeker provisions to access CEI on behalf of an individual	6.2
Resolution 12 – Acquiring CPs must not access credit information where they are not permitted to do so	6.4

OAIC proposals by category

Proposal	Report reference
CR Code amendments	
Proposal 4 – Amend CR Code source notes column and blue row lines	2.1
Proposal 6 – Amend CR code to accommodate other entities reporting CCLI (paragraph 6)	2.3.1
Proposal 13 – Amend CR Code to require CRBs to publish their CP audits and submit these to the OAIC (paragraph 23)	3.2.1
Proposal 15 – Amend CR Code to clarify the definition of 'account close' in respect of CCLI (paragraph 6)	4.1.2
Proposal 17 – Amend CR Code to clarify definition of 'month' to more flexibly accommodate CP reporting practices (paragraph 1)	4.2.1
Proposal 19 – Amend CR Code to introduce positive obligations on CRBs to remove statute barred debts and on CPs to inform CRBs when a debt has or will become statute barred (paragraph 20)	4.3.1
Proposal 21 – Amend CR Code to specify that s 21D(3)(d) notice must be a standalone notice (paragraph 9)	4.3.3
Proposal 24 – Amend CR Code regarding notification obligations (paragraph 4)	5.1
Proposal 28 – Amend CR Code to allow CRBs to offer individuals an automatic extension to the ban period when they make their initial request, where appropriate (paragraph 17)	5.2.1
Proposal 29 – Amend CR Code to provide further clarity on the expected level of evidence that a CRB needs to implement a ban and/or extension (paragraph 17)	5.2.2
Proposal 31 – Amend CR Code to require a CRB to record and alert an individual of access requests during a ban period (paragraph 17)	5.2.3
Proposal 32 – Amend CR Code to require CRBs to provide information to individuals on how they can access their credit reports held by other CRBs (paragraph 19)	5.3.1
Proposal 33 – Amend CR Code to specify that CRBs must provide physical copies of credit reports upon request (paragraph 19)	5.3.2
Proposal 37 – Amend CR Code to introduce a mechanism to correct multiple instances of incorrect information stemming from one event (paragraph 20)	5.4.2
Proposal 39 – Amend CR Code to include domestic abuse as an example of circumstances beyond the individual's control (paragraph 20.5)	5.4.4
Proposal 40 – Amend CR Code to extend correction requests to include CPs (paragraph 20.5)	5.4.4

Proposal 41 – Amend CR Code to expand the categories of information that can be corrected (paragraph 20.5)	5.4.4
Proposal 43 – Amend CR Code to introduce soft enquiries framework	6.1.1
Proposal 44 – Amend definition of 'capacity information' to include an individual in their capacity as a trustee (paragraph 1.2)	6.2
Education and awareness	
Proposal 1 – OAIC to review and update existing credit guidance with a particular focus on guidance for individuals and their advocates	2.1
Proposal 2 – OAIC to consider mechanisms to promote its credit reporting resources	2.1
Proposal 23 – OAIC to develop guidance about 'court proceedings information' and 'publicly available information'	4.4
Proposal 26 – OAIC to provide guidance to individuals on which circumstances require notice and which require consent	5.1
Proposal 30 – OAIC to develop guidance for individuals to explain the credit ban application and extension process	5.2.2
Proposal 35 – OAIC to provide guidance to individuals on their rights with respect to supplying credit reports to landlords and real estate agents	5.3.5
Proposal 36 – OAIC to provide guidance to individuals on their correction rights and how to exercise them	5.4.1
Proposal 38 – OAIC to provide guidance to industry on the 'no wrong door' approach to corrections, and will consider the need for future compliance activity	5.4.3
Proposal 42 – OAIC to provide guidance for individuals on the complaints process and who to approach to make a complaint	5.5
Compliance and monitoring	
Proposal 10 – OAIC to update the *Guidelines for Developing Codes* regarding processes for the development of variation applications	3.1.1
Proposal 11 – OAIC to raise visibility of its credit reporting compliance and monitoring activities	3.1.2
Proposal 14 – OAIC to publish a link to CRB audit reports on its website	3.2.1

Issues for review of Part IIIA	
Proposal 3 – Write to the Attorney-General about the suggestion of including overarching principles in Part IIIA	2.1
Proposal 5 – Write to the relevant Ministers to raise the issue of interactions between Part IIIA and the mandatory CCR regime	2.2
Proposal 7 – Write to the Attorney-General about how to best accommodate other entities such as telco and utility providers operating in the credit reporting system	2.3.1
Proposal 8 – Write to the relevant Ministers to raise the issue of emerging finance products, such as BNPL, operating in the credit reporting system	2.3.2
Proposal 9 – Write to the relevant Ministers to raise the issue of whether an ACL should be a requirement to participating in the credit reporting system	2.3.3
Proposal 12 – Write to the Attorney-General to raise the issue of exploring alternative funding avenues to support the OAIC's credit reporting functions	3.1.2
Proposal 16 – Write to the Attorney-General to raise the issue of disclosing 'historic' CCLI	4.1.4
Proposal 18 – Write to the Attorney-General about the suggestion that CPs must notify an individual when they disclose RHI relating to missed payments	4.2.3
Proposal 20 – Write to the Attorney-General about the suggestion that CPs must list default information within a reasonable time and retention period should apply from date of default	4.3.2
Proposal 22 – Write to the Attorney-General about the ongoing application of new arrangement information	4.3.4
Proposal 25 – Write to the Attorney-General about the suggestion that the notice framework within Part IIIA be reviewed	5.1
Proposal 27 – Write to the Attorney-General to raise concerns around the length of the initial credit ban period provided in Part IIIA	5.2.1
Proposal 34 – Write to the Attorney-General to raise the issue of real estate agents, landlords and employers accessing credit reports	5.3.5
Proposal 45 – Write to the Attorney-General to raise the issue of additional uses and disclosures of credit reporting information	6.2

About this Review

This independent review[4] considers the operation of the *Privacy (Credit Reporting) Code 2014* (Version 2.1) (the CR Code). This is the second independent review of the CR Code, following an initial review in 2017.

The registered CR Code is a legislative instrument approved by the Australian Information Commissioner (the Commissioner).[5] The CR Code supplements the provisions contained in Part IIIA of the *Privacy Act 1988* (Privacy Act) and the Privacy Regulation 2013 (Privacy Regulation) with respect to the handling of personal information about individuals' activities in relation to consumer credit. Importantly, a breach of the CR Code is an interference with privacy and a breach of the Privacy Act.

Purpose of the Review

The CR Code requires the Commissioner to initiate an independent review of the CR Code every four years.[6] This is an important governance provision which ensures that the CR Code is subject to regular and independent scrutiny. The review process provides an opportunity for stakeholders to comment on their engagement and practical experience with the CR Code, and explores whether there are opportunities to address any issues.

The review process also provides an opportunity to consider the operation of the CR Code amid social, technological and regulatory developments. Since the last independent review in 2017, there have been a number of developments in Australia's credit reporting landscape, including the introduction of mandatory comprehensive credit reporting, and the development of financial credit products such as Buy Now Pay Later products.

This Review considered whether the CR Code, in its current form, achieves its purpose – that is whether it further particularises how the requirements in Part IIIA should be adhered to by regulated entities. The Review focused on the operation of the CR Code in practice and whether it requires any changes.

Scope of the Review

As noted above, this Review considered Version 2.1 of the CR Code, as this was the version in force at the commencement of the Review in 2021. As such, more recent amendments to the CR Code which addressed changes to the Privacy Act have not been considered as part of this Review. This includes amendments to introduce a new type of information into the credit reporting system, known as 'financial hardship information'.[7]

The Review is not a broader review of Part IIIA of the Privacy Act. Therefore, issues identified with Part IIIA and how it applies to credit reporting bodies (CRBs), credit providers (CPs) and affected

[4] From this point forward, 'review' is capitalised when referring to the review conducted for this report.

[5] Privacy Act, s 26M(2).

[6] Paragraph 24.3 of the CR Code.

[7] See amendments introduced through the *National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Act 2021*.

information recipients (AIRs) are out of scope, except to the extent that there is any inconsistency between the drafting of the CR Code and the requirements of Part IIIA.

The Attorney-General must cause an independent review of Part IIIA to be completed before 1 October 2024.[8] Where stakeholders have raised pertinent issues that would benefit from consideration in the Part IIIA review, this Review has noted them throughout the report. The OAIC will raise these issues with the Attorney-General so they may be considered as part of that review.

Consultation process

In December 2021, the OAIC published a Consultation Paper which canvassed all aspects of the CR Code, such as the governance of the CR Code, the code provisions applying to certain types of information, the protections and rights for individuals, and the permitted activities by regulated entities. The OAIC invited comment from interested individuals, agencies and organisations.

Questions in the Consultation Paper provided a guide and were intended to elicit feedback relevant for the Review. Participants were encouraged to provide data, examples, case studies, or other evidence to support the views presented in their submissions. The closing date for written submissions was 4 February 2022. The list of questions in the Consultation Paper is set out at Appendix A.

In addition to written submissions, IIS Partners also held three roundtable sessions. These roundtables presented an opportunity for stakeholders to discuss their experiences and workshop potential solutions to issues raised.

A list of stakeholders who made submissions is included at Appendix B. Submissions have also been published on the OAIC website. A list of stakeholders who attended and participated in consultation roundtable discussions is set out at Appendix C.

[8] Privacy Act, s 25B.

How to read this report

This report sets out what the Review heard in response to the Consultation Paper and through roundtable discussions. Stakeholder feedback has been important to shaping the analysis in this report and has helped to understand key challenges or issues in relation to the CR Code. In addition, stakeholders' views and comments have assisted in forming the proposals that are presented in this report. Comments received via submissions and roundtable sessions have been summarised and appear in the 'Stakeholder views' sections of the report. The Review received extensive engagement from stakeholders in this Review process. The 'stakeholder views' presented in this report are not exhaustive. Even if a view has not been captured in the report, the Review has considered all stakeholder feedback provided.

The report largely follows a similar structure to the Consultation Paper. Part 1 provides the context for how the CR Code operates in relation to other legislation, industry standards and participants in the credit reporting system. Parts 2 to 6 provide detailed analysis of how the CR Code is operating in practice, and presents proposals on how the issue can be addressed. The issues have been grouped thematically as follows:

Part 2 – Overarching issues

This Part discusses overarching issues with the CR Code. As part of the Review, stakeholders were asked about their opinions on the overall effectiveness of the CR Code. The Consultation Paper also sought stakeholders' views on some broader thematic issues, such as:

- the form and readability of the CR Code (2.1)
- how the CR Code is interacting with the mandatory CCR regime (2.2)
- how the CR Code should apply to other entities (2.3).

Part 3 – Governance of the CR Code

A central concern for the Review, was whether appropriate governance mechanisms were in place to support the effective operation of the CR Code. This part of the report considers:

- the extent to which the CR Code is subject to good governance, awareness, and effective monitoring and compliance (3.1)
- the obligations on CRBs and CPs in relation to internal practices, recordkeeping and accountability measures (3.2).

Part 4 – Types of information

This part of the report considers the different types of information within the credit reporting framework, and considers whether the CR Code is currently operating as intended in relation to the following information types:

- consumer credit liability information (4.1)
- repayment history information (4.2)
- default information and payment information (4.3)

- publicly available information (4.4)
- serious credit infringements (4.5).

Part 5 – Protections and rights for individuals

The Review sought feedback from stakeholders on their experiences in how the CR Code provides protections for individuals' credit information. This part of the report discusses issues relating to the protections and rights provided for individuals in the CR Code, particularly in relation to:

- notice to individuals, particularly issues of confusion around notice and consent (5.1)
- protections for victims of fraud, particularly in relation to the operation of credit ban periods (5.2)
- individuals' experiences in exercising their access rights (5.3)
- individuals' experiences in exercising their correction rights (5.4)
- experiences navigating complaint handling and dispute resolution processes (5.5)
- opportunities to protect individuals affected by domestic abuse through public policy and industry practice (0).

Part 6 – Permitted activities of CRBs and CPs

This part of the report is focussed on the activities of CRBs and CPs that are permitted by the CR Code. This part of the report considers:

- specific issues raised by stakeholders in relation to information requests, including on the topic of 'soft enquiries' (6.1)
- technical issues around the use and disclosure of credit-related personal information by CPs and AIRs (6.2)
- the provisions surrounding direct marketing (6.3)
- transfer of rights provisions (6.4).

For definitions of terms and acronyms, see the Glossary.

Navigation aids

Yellow boxes summarise what the Review sought input on.

OAIC proposals

For ease of reference, the **proposals** in the report are colour coded to indicate their category. See example below.

Proposal 25 – OAIC to raise with the Attorney-General the suggestion that the notice framework within Part IIIA be reviewed

The OAIC will raise the need for a holistic review of the notice framework within Part IIIA with the Attorney-General so it can be considered in preparation for the review of Part IIIA.

The key is set out below.

Proposal categories
CR Code amendments
Education and awareness
Compliance and monitoring
Part IIIA issues

OAIC resolutions of practice issues

OAIC **resolutions** are highlighted in orange boxes. See example below.

OAIC Resolution of Practice Issue 1 – CRBs should have appropriate controls in place to quarantine information from future use or disclosure, where necessary

If CRBs are retaining information beyond the specified retention period, because they are authorised or required to do so, they must have appropriate controls in place to quarantine that information from any future use or disclosure.

Part 1: The CR Code in context

To effectively consider the CR Code, it is important to understand the context in which it operates, and the various participants involved. In Australia, credit reporting is regulated under Part IIIA of the Privacy Act, the Privacy Regulation and the CR Code. In addition to this, there are other instruments and bodies whose activities relate to credit reporting.

This Part of the report describes:

- the CR Code and the Privacy Act (1.1)
- how the CR Code interacts with other instruments (1.2)
- the participants in the credit reporting landscape (1.3).

1.1 The CR Code and the Privacy Act

1.1.1 Overview of the Privacy Act and Part IIIA

One of the objectives of the Privacy Act is to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is protected.[9] To achieve this, Part IIIA regulates the handling of personal information about individuals' activities in relation to consumer credit. Part IIIA of the Privacy Act came into effect in 1991. In 2014, under the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, significant changes were made to Part IIIA to allow for more comprehensive credit reporting.

While not an exhaustive list, Part IIIA outlines, among other things:

- the types of information that CPs can disclose to a CRB, for the purpose of that information being included in the individual's credit report
- what entities can handle that information
- the purposes for which that information may be handled.

Part IIIA specifically governs the collection and handling of credit-related information by CRBs, CPs and AIRs. More information about the types of entities regulated by the Privacy Act is set out at 1.3.1.

1.1.2 Purpose of the CR Code

Section 26N of the Privacy Act defines a CR code as a written code of practice about credit reporting and explains its relationship to Part IIIA. Among other things, a CR code must:

- set out how one or more of the provisions of Part IIIA are to be applied or complied with[10]

[9] Privacy Act, s 2(e).

[10] Privacy Act, s 26N(2)(a).

- make provision for, or in relation to, matters required or permitted by Part IIIA to be provided for by the registered CR code.[11]

A CR code may also impose additional requirements to those imposed by Part IIIA, so long as the additional requirements are not contrary to, or inconsistent with, Part IIIA.[12]

The CR Code provides further detail on how the credit reporting obligations outlined in Part IIIA should be operationalised by CRBs, CPs and AIRs. It outlines what activities are permitted by CPs and CRBs when participating in the credit reporting system. The information handling obligations on CRBs, CPs and AIRs are intended to protect the privacy of individuals, including by providing for access to information and correction rights for individuals, and protections for victims of fraud.

1.1.3 The development of the legal landscape and the CR Code

Since the introduction of the first CR Code, there have been a number of significant developments in the credit reporting landscape as well as in the CR Code itself.

Legal landscape

The predecessor to the CR Code was a code of conduct accompanying Part IIIA of the Privacy Act. In 2006-2008, the Australian Law Reform Commission (ALRC) conducted a significant review and recommended amendments to the Privacy Act, including Part IIIA.[13] These recommendations included that the Privacy Act should provide for and regulate credit reporting and that a credit reporting Code should deal with a range of operational matters relevant to compliance and outline permitted uses and disclosures for credit reporting information.

In early 2014, the Privacy Act was amended to allow CPs and CRBs to use and disclose 'comprehensive credit information' about an individual. This included information about the maximum amount of credit available to a person and how well the person was meeting their repayment obligations. To reflect these amendments, the CR Code was developed in accordance with s 26N of the Privacy Act and the OAIC's *Guidelines for Developing Codes*. The OAIC registered the first CR Code in March 2014.

Occurring alongside this was the Financial System Inquiry[14] and the Productivity Commission Inquiry into Data Availability and Use,[15] which recommended that the Government mandate comprehensive credit reporting in the absence of voluntary participation. The aim of comprehensive credit reporting was to enable CPs to better establish an individual's creditworthiness and lead to a more competitive and efficient credit market.

In the 2017-18 Budget, the Government of the day committed to mandating a comprehensive credit reporting regime if CPs did not meet a threshold of 40% of data reporting by the end of 2017. In

[11] Privacy Act, s 26N(2)(b).

[12] Privacy Act, s 26N(3)(a).

[13] Australian Law Reform Commission, *For your information: Australian privacy law and practice*, ALRC Report No. 108, ALRC, 2008.

[14] Treasury, *Financial system inquiry: final report*, Treasury, Australian Government, 2014.

[15] Productivity Commission, *Data availability and use: inquiry report*, No. 82, Productivity Commission, 2017.

November 2017, it was announced that legislation for a mandatory regime would be introduced as it was clear the 40% target would not be met.[16]

In 2021, mandatory Comprehensive Credit Reporting (CCR) was introduced to all 'eligible licensees'[17] in the *National Consumer Credit Protection Act 2009* (the 'Credit Act') via the *National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Act 2021* (the 'Credit Amendment Act'). This represented a significant shift in the credit reporting system in Australia from a entirely voluntary reporting system to one with mandatory credit reporting for very large banks.

CR Code – recent developments

In April 2017, the OAIC initiated the first independent review of the CR Code. That review resulted in a number of recommendations for changes to the CR Code.

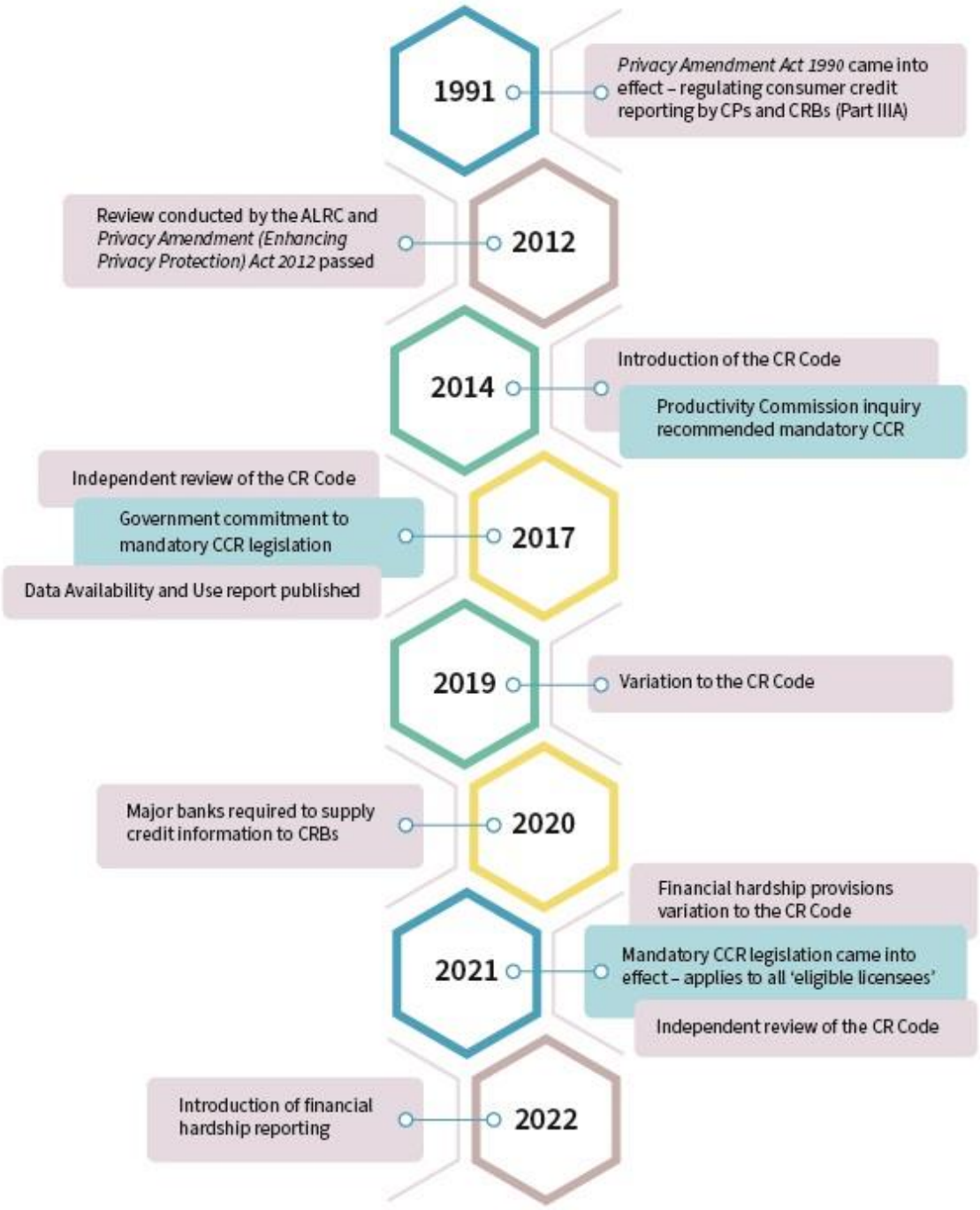
From 2017 until present, there have been four variations to the CR Code. Many of these resulted from the 2017 independent review. The most recent variation was approved in March 2022 and seeks to address the new financial hardship provisions introduced by the Credit Amendment Act. The Credit Amendment Act provided for a new form of information, known as 'financial hardship information', to be included in the credit reporting system from July 2022, and outlined other changes such as the requirement for CRBs to provide an individual with a free copy of their 'credit rating' once every three months, rather than the original 12 months.

In 2021, the OAIC commenced the current independent review of the CR Code which is the subject of this report.

[16] Treasury, *Mandating comprehensive credit reporting* [media release], Treasury, Australian Government, 2 November 2017, accessed 24 May 2022.

[17] Eligible licensees are initially large Authorised Deposit-taking Institutions (ADIs) that hold an Australian Credit Licence. An ADI is considered large when its total resident assets are greater than $100 billion. Other credit providers will be subject to the regime if they are prescribed in regulations.

Figure 1 – History of the CR Code



1.1.4 Future of Part IIIA and relevance for this Review

Section 25B of the Privacy Act sets out the mechanism for a review of Part IIIA. Namely, the Attorney-General must initiate an independent review of the operation of Part IIIA, which must be completed and given to the Attorney-General before 1 October 2024.

The 2024 review of Part IIIA is important because there are issues raised by stakeholders during this Review that would be more appropriately addressed by a change to Part IIIA rather than to the CR

Code. The Review has flagged these issues throughout the report, and the OAIC will write to the Attorney-General to raise these issues ahead of the 2024 review.

1.2 How the CR Code interacts with other instruments

1.2.1 Mandatory Comprehensive Credit Reporting

The move to mandatory CCR has been a gradual process. As noted above, in November 2017, the Commonwealth Treasury announced that the CCR would be mandated for the 'Big Four' banks. In early 2021 under the Credit Amendment Act, the mandatory CCR regime was rolled out to 'eligible licensees' in the Credit Act.[18] Under the Credit Amendment Act, 50% reporting was required for entities that were eligible licensees on 1 July 2021 and 100% reporting from 1 July 2022.

The main effect of these reforms has been to change credit reporting in Australia from a voluntary system to a mandatory one for a few very large credit providers.[19] Mandatory CCR aims to enable CPs to better establish an individual's creditworthiness and to enable a more competitive and efficient credit market.[20] It is expected that this will encourage other CPs to also share comprehensive credit reporting information.[21]

This mandatory CCR regime overlays an obligation to report all available credit information and importantly, is subject to civil penalties for failure to comply. Where previously the big four banks could choose whether to provide credit information about their customers to CRBs, now they must provide the information. This information is then used by a CRB to generate an individual's credit rating or credit score.

The Credit Act requires the Treasurer to initiate an independent review of the mandatory CCR regime to be completed before 1 October 2024.[22] This is different to the review of Part IIIA and will be an opportunity to assess the effectiveness of that regime specifically.

1.2.2 Industry standards

There have been a number of industry standards developed by the Australian Retail Credit Association (ARCA) in order to support CPs and CRBs in complying with Part IIIA and implementing the CR Code. These standards do not have legal effect under the Privacy Act and are subordinate to the CR Code.

---

[18] Eligible Licensees is defined under s 133CN of the Credit Act. Under that section, a licensee is an eligible licensee, on 1 July 2021 or a later day, if on that day the licensee: (a) is a large ADI [i.e. an authorised deposit-taking institution], or is a body corporate of kind prescribed by the regulations; and (b) is a credit provider.

[19] The 2014 Financial System Inquiry and Productivity Commission Inquiry into Data Availability and Use recommended that the Government mandate CCR in the absence of voluntary participation.

[20] Explanatory Memorandum to National Consumer Credit Protection Amendment (Mandatory Credit Reporting and other Measures) Bill 2019, [1.6].

[21] Explanatory Memorandum to the National Consumer Credit Protection Amendment (Mandatory Credit Reporting and other Measures) Bill 2019, [1.15].

[22] Credit Act, s 133CZL.

Australian Credit Reporting Data Standards

One of ARCA's primary objectives is to develop industry codes and standards in relation to the use of information across the retail credit industry. For that reason, ARCA has developed the Australian Credit Reporting Data Standards (Data Standards) and Schema which is available to CPs and CRBs upon request. The Data Standards detail the requirements for reporting credit accounts, and events relating to those accounts, between CPs and CRBs in Australia.

Principles of Reciprocity and Data Exchange

ARCA developed the Principles of Reciprocity and Data Exchange (PRDE) through extensive consultation with ARCA members and other key stakeholders. It is a set of data exchange rules to support Australia's credit reporting system. Participating CRBs and CPs agree to abide by the PRDE in order to have trust and confidence in their credit reporting exchange.

A CRB or CP is bound to comply with the PRDE upon becoming a signatory. Importantly, the PRDE requires that data being supplied meets a particular standard before it is exchanged. This means that data is communicated in a way that can be universally understood by other signatories to the PRDE. The PRDE also outlines dispute resolution and enforcement mechanisms to ensure compliance with the PRDE principles.

In 2015, the Australian Competition and Consumer Commission (ACCC) authorised key provisions of the PRDE relating to the PRDE's reciprocity, consistency and enforceability provisions. In 2020, the ACCC again authorised key paragraphs of the PRDE for a further six years.

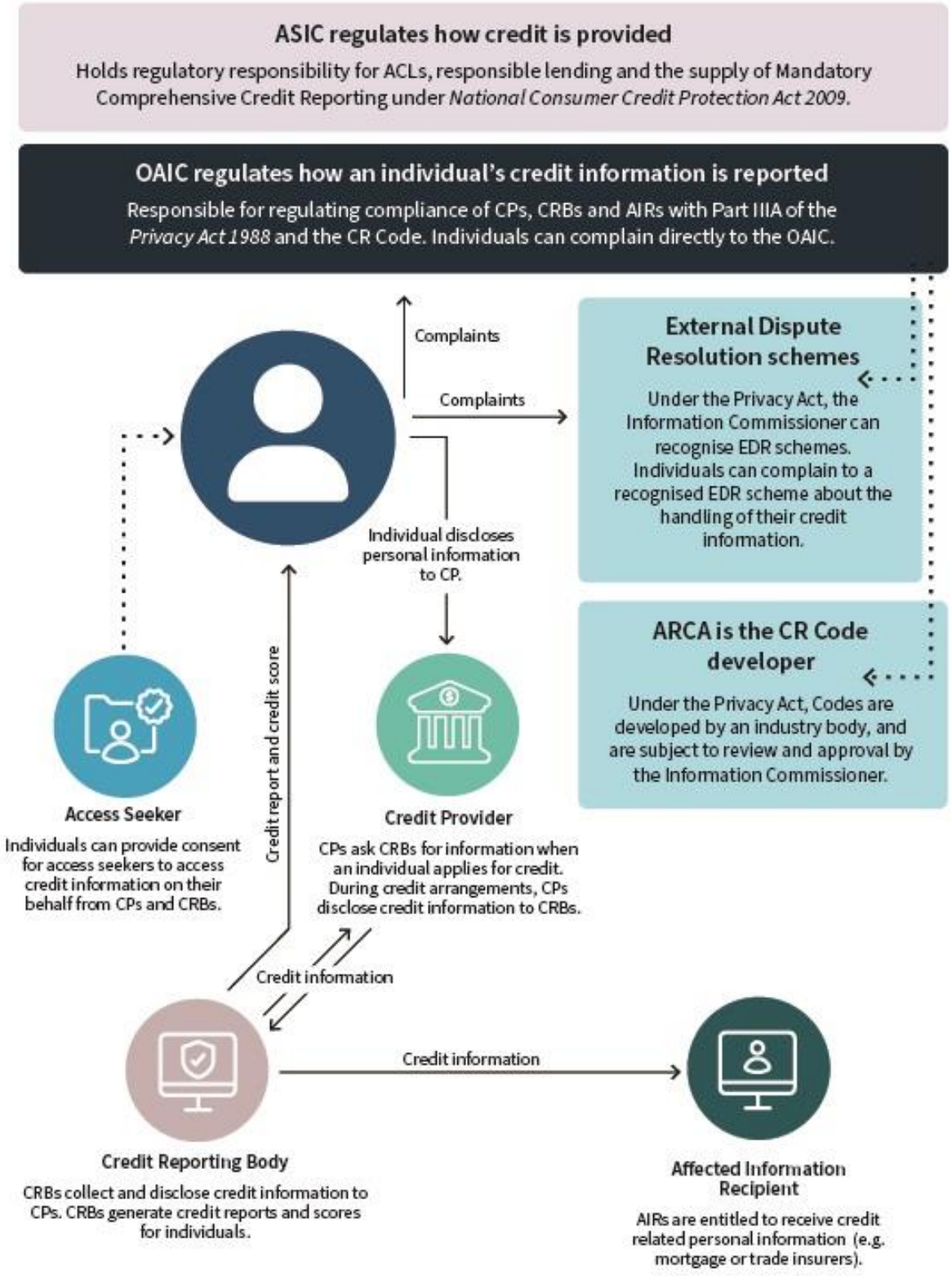
1.3 Who is involved in the credit reporting system?

It is helpful to view the credit reporting system collectively. This section outlines the different entities involved in the credit reporting system, as set out in the following diagram in Figure 2 and the accompanying narrative.

Individuals provide their information to CPs when applying for credit. This information can then be collected, used and disclosed by those participating in the credit reporting system. These bodies have roles and obligations under the Privacy Act and the CR Code when it comes to handling credit reporting information in order to protect an individuals' privacy. The OAIC regulates this activity. EDR schemes also play a role in resolving complaints.

Operating alongside this framework are other regulators and frameworks which regulate the provision of credit more broadly.

Figure 2 – Participants in the credit reporting system



1.3.1 Participants

As outlined above, the participants in the credit reporting system include individuals, access seekers, CPs, CRBs and AIRs.

Individuals – Individuals sit at the centre of the credit reporting system, as they provide their personal information to CPs for the purposes of receiving credit. CPs then use and disclose their personal information and credit information over the life of their loan.

An 'individual' for the purposes of this report is anyone aged 18 and over in Australia who has applied for credit or a loan and has a credit report. Credit reports contain information such as details of an individual's credit card, home loan and mobile phone contract. They also include a credit rating which indicates the band where the individual sits.

Access seekers – An 'access seeker' is a technical term which refers to someone who assists an individual to deal with a CP or CRB with the individual's consent. They act on a written authority from the individual.[23] Access seekers can be community lawyers or financial counsellors that support individuals who are experiencing credit/debt problems, victims of identity theft, and people escaping domestic abuse. They can also be organisations that are providing the individuals with a service, such as debt management companies and mortgage brokers.

Credit Providers (CPs) – CPs are commonly banks and other similar financial institutions that offer credit to individuals in the form of home loans, credit cards and other products. CPs can also include:

- retailers that issue store credit cards for the sale of goods and services
- organisations like telecommunications and utilities providers that supply goods and services where payment is deferred for seven days or more
- organisations that supply credit for the hiring, leasing or renting of goods.

Real estate agents, general insurers and employers are not CPs.

CPs share credit information about their customers with CRBs to enable the CRBs to maintain up-to-date credit reporting information. CPs also collect credit reports from CRBs when assessing applications for credit from individuals.

Credit Reporting Bodies (CRBs) – CRBs give other organisations information about the creditworthiness of an individual. To do this, they collect credit information from CPs and use that information to create credit reports and credit scores about an individual. When a CP is considering whether to offer credit to an individual, it can ask for the credit report of that individual from a CRB. This helps the CP manage risk by making an informed assessment of an individual's creditworthiness. If the individual has poor credit scores, the CP might choose not to approve the individual's application for credit. The CRBs operating in Australia are Equifax, Experian and Illion.

Affected Information Recipients (AIRs) – AIRs are entities that are entitled to receive credit-related personal information under Part IIIA. This includes:

[23] Privacy Act, s 6L.

- mortgage insurers[24] and trade insurers[25]
- a related body corporate of a CP or an entity that assists the CP in processing credit applications[26] or managing credit[27]
- an entity using the information in the course of purchasing a debt owed or purchasing a stake in the CP.[28]

CRBs and CPs may disclose credit-related personal information to AIRs but this is only permitted where the AIR proposes to use the information to fulfil particular functions set out in Part IIIA.[29]

1.3.2 Role of the OAIC

The OAIC is the independent regulator and has a range of regulatory responsibilities and powers in relation to Part IIIA and the CR Code. Under the Privacy Act, it is the role of the Commissioner to appoint the CR code developer, approve the CR Code and, importantly, review and approve any subsequent variations to the CR Code. The Commissioner is required to initiate an independent review of the CR Code every four years. The Commissioner also has the power to recognise external dispute resolution schemes which can play a role in resolving complaints.

A breach of the CR Code is an interference with privacy and a breach of the Privacy Act.[30] The Privacy Act confers on the Commissioner a range of regulatory powers. These includes powers to conduct assessments, undertake voluntary investigations, make enquiries, accept enforceable undertakings, make determinations, seek injunctions and apply to a Court for civil penalties.

These powers also allow the OAIC to undertake a range of regulatory activities in respect of the CR Code. This includes receiving and investigating complaints about CPs and CRBs.

The CR Code also provides for the OAIC's ongoing compliance monitoring of CRBs, CPs and AIRs, which are additional to the OAIC's general oversight of organisations under the Privacy Act. For example, the CR Code requires CRBs to commission an independent review of their processes every three years. CRBs must consult the Commissioner as to the scope and choice of the reviewer and provide a copy of the report to the OAIC.

Additionally, the OAIC has guidance functions that support the overall administration of the CR Code. Sections 28(1)(c)(iv) and 28(1)(d) of the Privacy Act refer to guidance functions of the Commissioner, which include, respectively, (i) promoting understanding and acceptance of the CR Code and (ii) undertaking educational programs for the purposes of promoting the protection of individual privacy.

---

[24] A mortgage insurer protects a lender (e.g. a bank) from situations where a borrower (e.g. a private individual or business) defaults on payments or passes away.

[25] A trade insurer protects businesses from bad debts. They reimburse CPs (e.g. a small business) when their customers are unable to pay – because of default, insolvency (or other agreed reasons).

[26] E.g. a person that processes documents or paperwork associated with making a credit application to the CP.

[27] E.g. a person who manages the credit (such as cash flow to a small business) on behalf of the CP in accordance with a payment schedule.

[28] Which can include a professional legal or financial adviser of the entity.

[29] Privacy Act, s 21N.

[30] Privacy Act, ss 26 and 26M(2).

1.3.3 ARCA as CR code developer

ARCA was established in 2006 to provide an industry forum to advocate for improvements to Australia's credit reporting system. It is an industry association for organisations involved in the provision, exchange and application of retail credit reporting data in Australia. Its members include CPs and CRBs.

In 2012, following the enactment of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which required the development of a CR Code to particularise the provisions of Part IIIA, the Information Commissioner appointed ARCA to develop the CR Code.

The Privacy Act outlines that the CR code developer should be an entity or association representing entities subject to Part IIIA.[31] This is consistent with other codes developed under the Privacy Act.[32]The Privacy Act therefore envisages that the development of Codes will be an industry led process, with the Information Commissioner providing independent review and approval. The Privacy Act also sets out the process for developing a code. The OAIC *Guidelines for Developing Codes* provide guidance to code developers on how codes should be developed, including setting out expectations for consultation and the matters that the Commissioner will consider in reviewing requests to vary a code.[33] These requirements provide important safeguards to ensure that variations to the CR Code have undergone appropriate consultation with relevant stakeholders.

As the code developer, ARCA is also responsible for drafting variation applications to amend the CR Code for the Commissioner's approval.

1.3.4 Role of EDR schemes

Under the Privacy Act, CPs and CRBs must be subject to, or a member of, a recognised external dispute resolution scheme before they can use or disclose certain types of information.[34] For example, the Australian Financial Complaints Authority (AFCA) is one of these external dispute resolution (EDR) schemes recognised by the Information Commissioner under s 35A of the Privacy Act.

AFCA is responsible for handling complaints from individuals about credit, finance and loan products. AFCA assists individuals to reach agreements with respondents on how to resolve their complaints.

Individuals can choose to complain to either AFCA (or another relevant EDR scheme), or alternatively to the OAIC, about the actions of a CP or CRB. Decisions made by AFCA can be binding on a respondent to a complaint.

The OAIC engages regularly with AFCA, including by referring complaints to AFCA under s 50(1)(g) of the Privacy Act in accordance with its information sharing arrangement.[35] The OAIC also provides

---

[31] Privacy Act, s 6.

[32] An APP Code Developer should be an APP entity or association of APP entities subject to the Privacy Act. See Privacy Act, s 6.

[33] OAIC, *Guidelines for Developing Codes*, OAIC, 2013.

[34] Privacy Act, ss 20E(3)(c); 21D(2)(a); 21G(3)(e).

[35] See *Information Sharing Arrangement for the referral of privacy complaints under section 50 of the Privacy Act 1988 (Cth) between The Office of the Australian Information Commissioner and External Dispute Resolution Schemes*, OAIC, 2021.

advice to AFCA on privacy issues relating to Part IIIA and the CR Code to ensure consistency across decisions.

1.3.5 Role of ASIC

The Australian Securities and Investment Commissions (ASIC) is Australia's corporate, markets, financial services and consumer credit regulator. ASIC is responsible for administering and enforcing the Credit Act. The Credit Act governs activity relating to credit contracts, consumer leases, mortgage and guarantees, and credit services. It provides important consumer safeguards. It also sets out obligations for responsible lending and the mandatory supply of comprehensive credit reporting information, as detailed above.

The Credit Act requires entities that engage in 'credit activity' to have a license or authorisation from a licensee. Credit licensees must comply with the responsible lending conduct obligations in Chapter 3 of the Credit Act. The key concept is that credit licensees must not enter into a credit contract with a consumer, suggest a credit contract to a consumer or assist a consumer to apply for a credit contract if the credit contract is unsuitable for the consumer.

The OAIC works closely with ASIC given its role in regulating financial services and the mandatory supply of comprehensive credit reporting.

Part 2: Overarching issues

This Part discusses overarching issues with the CR Code. As part of this Review, stakeholders were asked for their views on the overall effectiveness of the CR Code. The Consultation Paper also sought stakeholders' views on some broader thematic issues, such as:

- the form and readability of the CR Code (2.1)
- how the CR Code is interacting with the mandatory CCR regime (2.2)
- how the CR Code should apply to other entities (2.3).

The primary objective of this Review is to consider the effectiveness of the CR Code. Stakeholders provided invaluable feedback on their experiences and made suggestions for improvements.

Generally, industry stakeholders were of the view that the CR Code was operating effectively in its intended purpose; being a legislative instrument that gives operative effect to Part IIIA. However, consumer advocates raised concerns that the CR Code was not fit for purpose, because it has not kept pace with best practice in complaint handling, and is not an instrument that supports individuals in advocating for their rights. They also raised concerns about the process for developing variations, and the readability of the CR Code for individuals and their advocates.

The proposals set out throughout this report are aimed at addressing this feedback.

2.1 Form and readability of the CR Code

A key issue for the Review related to the format and readability of the CR Code. Some stakeholders raised concerns about the complexity of the CR Code.

Given its purpose, the CR Code format generally reflects Part IIIA. Therefore, the complexity of the CR Code is in some ways, a product of Part IIIA.

> The Review sought stakeholder views regarding whether the CR Code could be amended to address concerns raised about the complexity of the CR Code.

Stakeholder views

This Review received stakeholder feedback that the CR Code is complex and difficult for consumers, and even their legal and financial advisers, to understand.

Consumer advocates noted that readability is a particular issue, with five stakeholders suggesting the CR Code be completely rewritten.[36]

Conversely, other stakeholders noted that the CR Code is not drafted as a document for consumers, but is rather subordinate legislation to which only minor amendments should be made.[37]

[36] See consumer advocates joint submission, p 10; Communications Alliance submission, p 3; CPRC submission, p 5; Legal Aid Queensland submission, p 3; AFIA submission, p 4.

[37] See ARCA submission, p 8; ABA submission, p 3; Experian submission, p 5.

Stakeholders instead suggested targeted guidelines, which could be viewed together with the CR Code and which could be used as a vehicle to address concerns that the contents of the CR Code cannot be understood by consumers.

In addition to guidelines, Legal Aid Queensland revisited some of its suggestions to the 2017 independent review of the CR Code, which included a plain-language rewrite of the contents of the CR Code (thereby reducing the need for further explanation and guidance) and inclusion of a clear Glossary of Terms or definitions section within the CR Code.[38]

Consumer advocates also submitted that a principles-based 'fairness' approach should be incorporated into the CR Code, noting that fairness is a key component of many industry codes of practices in the financial services space, as well as a part of AFCA's rules.[39] They argued that rather than changing the law or detracting from clarity, a principle like fairness would be a lens to apply where there is any discretion or ambiguity.[40]

The Finance Brokers Association of Australia (FBAA) opposed the inclusion of a fairness principle, arguing that the CR Code should remain prescriptive to give the greatest certainty to financial firms and individuals.[41] Experian also opposed this on the basis that it risks creating ambiguity in an already complex domain.[42] During an industry roundtable, ARCA also submitted that making such a change is not possible as Part IIIA itself is not principles-based. Furthermore, it noted that the role of the CR Code (which is intended to be prescriptive for all cases) and AFCA's Rules (which decides on a case-by-case basis) are not comparable.

Review findings

Overall approach to form and readability

There is no doubt that the CR Code is complex, which can make it difficult to interpret, particularly for individuals or those without legal training. However, the primary objective of the CR Code as outlined in Part IIIA of the Privacy Act, is to set out how one or more of the provisions of Part IIIA are to be applied or complied with. In this regard, the CR Code creates legal obligations for regulated entities to comply with and is not intended to be a consumer facing document. The CR Code is a legislative instrument which stipulates how regulated entities should comply with their obligations under Part IIIA. It is not intended to be a plain English guide to Part IIIA.

Notwithstanding this, the Review acknowledges that the CR Code is nonetheless complex. This complexity is, to some extent, a consequence of the detail and complexity of the principal legislation. This makes wholesale changes to language and readability difficult where such changes would introduce inconsistency with Part IIIA. Where possible, the Review has sought to identify areas where provisions may be adjusted to clarify or simplify their meaning. We have also identified areas of complexity that should be addressed in the required independent review of Part IIIA.

[38] See Legal Aid Queensland submission, p 5.

[39] See consumer advocates joint submission, p 9; Legal Aid Queensland submission, p 3.

[40] See consumer advocates joint submission, p 9.

[41] See FBAA submission, p 2.

[42] See Experian submission, p 5.

The Review heard stakeholder feedback that further guidance could be used to provide clarity. Some stakeholders suggested the development of guidelines similar to the APP Guidelines. However, the Review also understands that the primary need for guidance is to ensure that individuals and their advocates have sufficient resources to understand their rights in relation to their credit information. The Review notes that guidelines are generally developed to guide regulated entities about their obligations and support compliance, as opposed to informing individuals about their rights. As such, it is unlikely that guidelines would meet the intended objective of supporting individuals and their advocates. Instead, the Review considers that developing practical, educative resources that are targeted at individuals and their advocates would be more effective in addressing current needs.

Proposal 1 – OAIC to review and update existing credit guidance with a particular focus on guidance for individuals and their advocates

The OAIC will create targeted resources and education materials on particular issues identified by this Review. These resources will be written in plain English and focused primarily on individuals and their advocates.

Proposal 2 – OAIC to consider mechanisms to promote its credit reporting resources

The OAIC will review its website to ensure that credit reporting resources are easy to find and use.

In addition, the OAIC will explore opportunities to partner with ASIC (as owner of the MoneySmart Website), and ARCA (as owner of the CreditSmart Website) to promote OAIC's educational resources and expand its reach.

The OAIC will also consider alternative formats to present information including videos, and interactive material.

Overarching principles

The Review acknowledges why some stakeholders consider that overarching principles, such as fairness, should be incorporated into the CR Code and how such principles could serve the interests of consumers in formalising and clarifying their rights. The Review considers that the introduction of more direct overarching principles would be desirable but would need to be placed in the principal legislation rather than the CR Code. As noted above, the role of the CR Code is to outline how to apply and comply with the provisions of Part IIIA. Placing these principles in the Privacy Act will give them more weight and simplify how they should be interpreted. The Review therefore finds that there may be benefit in this proposal being considered in the required independent review of Part IIIA.

Proposal 3 – OAIC to raise with the Attorney-General the suggestion of including overarching principles in Part IIIA

The OAIC will write to the Attorney-General so that the issue of whether, and how, to introduce overarching principles into the credit reporting framework can be considered in preparation for the review of Part IIIA.

The Review also considers that there may be utility in ensuring the CR Code adequately explains the purpose and effect of each paragraph. The CR Code states that this is performed through the use of a blue row line before each provision which explains what it says. The Review considers that these sections should be reviewed in order to ensure they provide a plain English description of the purpose and intent of the paragraph. Further, the Review considers that many of the references in the source notes column, including references to the 'pre-reform' Code are potentially out of date, and should be reviewed and amended as appropriate. This will assist in mapping intersections between the CR Code and the Privacy Act and Privacy Regulation.

Proposal 4 – Amend CR Code source notes column and blue row lines

The source notes column and the blue rows of the CR Code should be reviewed to ensure that they clearly outline the purpose of the paragraph to which it relates and the applicable provision of the Privacy Act or Privacy Regulation

2.2 Interaction with the mandatory CCR regime

As noted above, the credit reporting system has changed significantly with the introduction of mandatory CCR (see 1.2.1 above for an overview). A central question for this Review was whether the CR Code needs to be updated in light of these changes. While having different objects, the mandatory CCR regime and Part IIIA of the Privacy Act are central to how credit reporting operates in Australia.

One point of possible friction raised by stakeholders was the 'must disclose' posture of CCR and the 'can disclose' posture of the Privacy Act and the CR Code. The mandatory CCR regime requires reporting of all credit reporting information by eligible licensees, while Part IIIA and the CR Code are concerned with what information may be disclosed by a CP to a CRB and vice versa.

The Review sought feedback on whether the CR Code needs to be updated in light of changes brought about by mandatory CCR.

Stakeholder views

The Review received very little stakeholder input on this topic, which may be a reflection of the relatively nascent stage of mandatory CCR in Australia.

ARCA noted that the mandatory supply of credit information required by the Credit Act is in contrast with the operation of Part IIIA and the CR Code, which enables data supply but does not mandate it.[43] This raises some uncertainty as to whether or not particular information can be disclosed. During the roundtables, ARCA made an overall observation that the law needed to be better aligned – including mandatory CCR, the hardship provisions and Part IIIA of the Privacy Act.

Experian submitted that many of the issues noted in the Consultation Paper would not exist if mandatory supply of information applied to all CPs and CRBs.[44]

Consumer advocates stated that they were not in a position to comment on the effect of mandatory CCR on compliance with the CR Code, as they have little or no visibility of industry compliance with the CR Code.[45] They did raise a concern that consumer representatives assisting individuals have experienced greater inflexibility in removing or amending credit reporting information as part of the resolution of a dispute, with mandatory reporting obligations cited as a reason for the inflexibility.[46]

Review findings

As noted above, the Review did not receive substantive feedback on the issue of the CR Code's interaction with the mandatory CCR regime. This appears to be due to the low visibility that some stakeholders (especially consumer advocates) have about how mandatory CCR is operating, as well as the fact that the mandatory CCR regime is still relatively new.

[43] See ARCA submission, p 10.

[44] See Experian submission, p 6.

[45] See consumer advocates joint submission, p 12; Legal Aid Queensland submission, p 5.

[46] Ibid.

The Review acknowledges the issue of uncertainty in reporting practices raised by the mandatory CCR regime versus the voluntary credit reporting regime under the Privacy Act. We consider there is an opportunity for the Attorney-General to engage with the Treasurer on this issue as they conduct parallel reviews of Part IIIA and the mandatory CCR regime.

Proposal 5 – OAIC to raise with the relevant Ministers the issue of interactions between Part IIIA and the mandatory CCR regime

The OAIC will raise with Government the tensions between the credit reporting regimes in the Privacy Act and the Credit Act, including opportunities to create more certainty and consistency.

The OAIC will write to the relevant Ministers about these issues so that they can be considered in preparation of the respective reviews of Part IIIA of the Privacy Act and Part 3-2CA of the Credit Act. Consideration may wish to be given as to whether these reviews can occur in co-ordination with each other given the relevant intersections.

2.3 Other entities

The credit reporting landscape in Australia has changed significantly since the CR Code was last reviewed in 2017. Since that time, there have been a number of new entities that have commenced participating in the credit reporting system.

For example, certain telecommunications (telco) providers such as Optus now participate in the CCR data exchange. As a telco provider, Optus is a non-Australian Credit Licence (ACL) holder and, as such, can only participate in the exchange of consumer credit liability information (CCLI) and cannot disclose or collect repayment history information (RHI).

Another change to the credit industry in Australia has been the rise in Buy Now Pay Later (BNPL) providers and products. Some BNPL providers are ACL holders, or authorised by ACL holders, and some are not.

The Review notes that Part IIIA is not necessarily restricted to banks and was intended to also facilitate participation by other industries. For example, s 6G(2) defines a credit provider to include a small business operator that carries on a business for the sale of goods or the supply of services in relation to credit.

It is important however, that the CR Code is fit for purpose, and is applicable to the entities that use it, and have to comply with it. The Review therefore sought input regarding the participation of new entities and whether amendments to the CR Code would be required to accommodate these entities.

The Review considered issues regarding the participation of new entities, including:

- whether the participation of telco and utilities providers necessitate changes to the CR Code
- whether the participation of BNPL providers and products necessitate changes to the CR Code
- a broader issue regarding extent of participation in the credit reporting system of non-ACL entities and entities that are not bound by responsible lending obligations (noting that such matters may fall outside the scope of the CR Code but may warrant further consideration).

2.3.1 Telecommunications and utilities

As noted above, certain telco providers such as Optus now participate in the CCR data exchange. Many telco providers are non-Australian Credit Licence (ACL) holders and, as such, cannot disclose or collect RHI.

The Review canvassed whether changes could be made to the CR Code to facilitate the participation of telco and utility providers, particularly in relation to their different account arrangements and how this affects the reporting of CCLI. The Review also considered whether the thresholds for default information were appropriate to telco or utility products.

Stakeholder views

A number of stakeholders commented that it is currently unclear how certain elements of CCLI should be reported by telco and utility providers. Stakeholders also raised concerns that the thresholds for reporting default information may not be appropriate to telco or utility products. Generally, stakeholders raised the following issues:

Reporting CCLI 'Account Open and Close' information

Stakeholders noted that it is unclear how the current definitions of account open and close in the CR Code should apply to telco accounts.[47] ARCA noted that in the telco sector, account open and close dates appear to align more to connection and disconnection of service (noting that multiple credit contracts may exist for a phone service, but the overall account may continue to operate until the time of disconnection).[48]

Consumer advocates noted that for telcos, the CR Code needs to be clear that accounts should be terminated where the service has been disconnected or when there is no longer an active account. If an account has been disconnected but the provider is still collecting arrears, the account should still have been terminated for CCLI purposes.[49]

Reporting CCLI 'Credit Limit' information

Another issue raised by ARCA was that currently the credit limit for telco credit is reported as 'not applicable' as it is unclear whether a credit limit can readily be discerned for telco credit.[50] The ABA was supportive of adjusting the credit limit for telco providers to represent monthly repayment for services and handset repayment.[51]

The Communications Alliance was not supportive of telco providers sharing the monthly plan arrangements for each customer, as it did not consider this to be the same as a credit limit.[52] More generally, it welcomed the opportunity to be consulted as part of developing more detailed definitions and related guidance to apply to the telco provider context.

Reporting CCLI 'Credit term' information

Similar to the issue of account open and close above, ARCA noted that the reporting of credit term for telco credit may require further clarity as generally an individual signs up for the provision of a service, which might not be for a specific period of time, or for a service which 'rolls over' and results in multiple contracts.[53]

[47] See ARCA submission, p 14; ABA submission, p 4.

[48] See ARCA submission, p 14.

[49] See consumer advocates joint submission, p 25.

[50] See ARCA submission, p 14.

[51] See ABA submission, p 4.

[52] See Communications Alliance, p 4.

[53] See ARCA submission, p 14.

Reporting 'default information'

The Review also received additional suggestions for clarifying or improving the operation of the default information provisions to reflect the practices and standards of telco and utility providers. For example:

- clarifying the lack of a single 'default date' under Part IIIA[54]
- increasing the minimum default listing threshold in Part IIIA for the energy sector to better reflect current bills, for example from $150 to $300[55]
- introducing a 'sliding scale' where the length of a credit default listing period accords with the relative size of the debt.[56]

Review findings

As an overall observation, the Review notes that the current drafting of the CR Code does not prevent telco and utility providers from reporting CCLI or default information. Rather, the issue is how the different components of CCLI can be interpreted and applied in the context of telco and utility providers.

In terms of the account open and close definition, it is possible for the CR Code to clarify that, in the context of telco or utility providers, this is the connection and disconnection date. As is the case with other types of credit, where an account is no longer active, it should also be considered 'closed' for the purposes of reporting CCLI. This approach will ensure alignment to another proposal from this Review (see Proposal 15 at 4.1.2).

On the issue of applying 'credit limit' and 'credit term' in the context of a telco or utility service, the Review did not receive sufficient information to recommend specific changes to the CR Code to better accommodate these providers. Before amendments are made to the CR Code, there will need to be meaningful and targeted consultation with stakeholders to understand the issues and identify an appropriate way forward.

Proposal 6 – Amend the CR Code to accommodate other entities reporting CCLI

Paragraph 6 of the CR Code should be amended to clarify how 'account open and close' definitions apply to telco and utility providers.

As to 'credit limit' and 'credit term', before amendments are explored, targeted consultation should be undertaken to understand how these definitions can apply to these products, taking into account how industry delivers, and how consumers use, these products.

[54] See ARCA submission, p 25.

[55] See EWON submission, p 3.

[56] See EWON submission, p 3.

The issues raised by stakeholders on the reporting of default information by telco and utility providers relate to provisions in Part IIIA and cannot be changed through the CR Code. For example, the current minimum default listing amount is $150 and is stipulated in s 6Q(1)(d) of the Privacy Act. The OAIC does however, propose to raise these issues with Government for consideration in its review of Part IIIA.

Proposal 7 – OAIC to raise with the Attorney-General the issue of how to best accommodate other entities such as telcos and utilities providers operating in the credit reporting system

The OAIC will raise the issue of how to better accommodate other entities operating in the credit reporting system with the Attorney-General and whether changes are required. For example, clarifying the lack of a single 'default date' and considering updating default listing thresholds and periods to better reflect different sectors' practices and standards.

The OAIC will write to the Attorney-General so that these issues can be considered in preparation for the review of Part IIIA.

2.3.2 New and emerging finance products and BNPL

Another significant change to Australia's credit reporting landscape has been the rise of BNPL providers and products. While some BNPL providers are ACL holders, or authorised by ACL holders, others are not.

The Review called for views on any changes that might need to be made to the CR Code regarding BNPL products and providers, particularly in relation to different account arrangements and the meaning of 'credit limit'.

Stakeholder views

The Review received a number of submissions from stakeholders about the regulation of BNPL products and the shortcomings of the current regime, which went beyond any specific issue with the CR Code.

Consumer advocates were concerned that BNPL entities are not subject to responsible lending and do not require an ACL.[57]

AFIA provided broader comments that the current credit reporting regime is not well-suited to new and emerging finance products that are based on real-time data and insights.[58] For example, the CR Code seems to work well for reporting RHI for 'traditional' lending products that have a regular, monthly repayment schedule (such as home loans or credit cards), but does not work for new and emerging finance products that do not easily fit within the monthly repayment hierarchies

[57] See FRLC submission, p 15.

[58] See AFIA submission, p 2.

established by the CR Code.[59] Specifically, for RHI, AFIA considers that repayment histories should be representative of actual repayment obligations and not restricted to an arbitrary calendar month.[60]

Similarly, Afterpay submitted that the current regime is not designed for BNPL products, with features such as dynamic spending limits and no guaranteed line of credit, among other differences with traditional credit products.[61] Afterpay noted that it does not participate in the credit reporting regime under the Privacy Act.[62]

EWON raised an issue with new energy retailer business models that integrate energy accounts and loans (including BNPL) for products such as solar panels.[63] Financial Counselling Australia raised the necessity of thinking through consumer safeguards in concert with facilitating the inclusion of BNPL into the credit reporting system.

Experian noted that the industry would benefit from clarity over the application of Part IIIA to BNPL entities.[64]

Among stakeholder submissions, ARCA noted that the Data Standards have been amended to allow for the reporting of two types of BNPL accounts, (i) BNPL Facility account and (ii) BNPL Transaction account.[65] ARCA submitted that BNPL Facility accounts tend to operate in a manner similar to traditional revolving credit facilities with a single credit limit, while BNPL Transaction accounts are more challenging as there would appear to be many transactions. ARCA considered that this issue could be addressed by industry, or alternatively by a change to Part IIIA or the CR Code to better facilitate the reporting of BNPL transaction accounts (such as the reporting of 'grouped' credit).[66]

In relation to the definition of credit limit, ARCA also submitted that there is merit in reviewing the existing credit limit categories in paragraph 6 of the CR Code to ensure they adequately reflect the operation of BNPL credit, including features such as:[67]

- no interest charges, but rather other kinds of fees
- a series of weekly or fortnightly payments over a short term, between 4 to 10 weeks in length
- that CPs may update the existing credit limit categories in accordance with the payment schedule multiple times within a short timeframe.

Review findings

The Review notes that there have been significant changes in the ways that individuals access credit. New and emerging credit products, including BNPL products, are now diverse and mature in their operation. Amendments to regulation are required to ensure consumers are protected, and that the

[59] See AFIA submission, p 2.

[60] See AFIA submission, p 6.

[61] See Afterpay submission, p 4.

[62] See Afterpay submission, p 3.

[63] See EWON submission, p 2.

[64] See Experian submission, p 6.

[65] See ARCA submission, p 14.

[66] See ARCA submission, p 15.

[67] Ibid.

legislation continues to achieve its objective. For example, BNPL products have the potential to disrupt the credit reporting industry and may result in inconsistency of reporting of individuals that are in similar financial situations based on the type of product they are accessing.[68]

From stakeholder submissions, it appears that many of these new finance providers are operating as 'non-participating credit providers' such that they are not using or disclosing credit information. This means that they are exempt from the requirements under Part IIIA.

The Review considers that it is crucial that any amendments to the Privacy Act and the CR Code which provide for the reporting of credit information in relation to these products, are part of a broader conversation about the appropriate regulation of the provision of these newer finance models.

The Review concludes that the general concerns with regulation of BNPL raised by stakeholders during this process, are beyond the remit of the CR Code and should be considered holistically given the interaction with mandatory CCR and responsible lending obligations.

Furthermore, any specific changes to the CR Code (such as the reporting of RHI for these products) should only occur after a more fundamental consideration of the credit reporting system and its applicability to emerging products. This is a broader question for Government which the Review considers could take place as part of the review of Part IIIA (see Proposal 7 at 2.3.1 above) and the review of the mandatory CCR regime under the Credit Act.

We note that the Assistant Treasurer announced on 12 July 2022 that the Government will be consulting on options to improve the regulation of credit in Australia (including Buy Now Pay Later).[69] This might be an appropriate forum to consider this issue.

Proposal 8 – OAIC to raise with the relevant Ministers the issue of emerging finance products such as Buy Now Pay Later operating in the credit reporting system

The OAIC will raise the issue of emerging finance products such as Buy Now Pay Later entities operating in the credit reporting system with the relevant Ministers in preparation for the review of Part IIIA of the Privacy Act and Part 3-2CA of the Credit Act, and in the consultation currently being undertaken regarding the regulation of BNPL products.

This includes whether the 'non-participating credit provider' definition should capture these products, and whether changes are required more broadly to appropriately regulate the reporting of information for these products (for example, whether more flexibility is needed around the definition of RHI).

[68] Recent amendments were made to the Privacy Act to ensure that individuals in like financial situations are treated similarly: see Explanatory Memorandum to National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Bill 2019 at 2.10.

[69] See: Address to the Responsible Lending and Borrowing Summit, Sydney | Treasury Ministers.

2.3.3 Participation by non-ACL entities

In the course of preparing for the Review, stakeholders presented a range of views on licensing requirements to access credit reporting information. Some stakeholders were of the view that CPs should have an ACL and comply with responsible lending obligations before they are allowed to access credit reporting information, whilst other stakeholders considered that access to RHI should be expanded to include non-ACL licensed CPs. The Consultation Paper therefore sought stakeholders' views on this, while noting that such matters may be outside the scope of the CR Code.

Stakeholder views

Stakeholder views significantly diverged between industry and consumer groups on this issue.

ARCA stated that its policy position is that access and disclosure of RHI ought to be available to all credit providers, including telco and utilities providers, as well as BNPL providers who may not hold an ACL.[70] It noted that there are clear benefits to both industry and consumers for broadening the operation of CCR, including the ability for 'new to credit' individuals to demonstrate their creditworthiness to potential lenders. This would also resolve an inconsistency where RHI are reported by BNPL providers holding an ACL but not for BNPL accounts held with CPs not holding an ACL.

The ABA considered that the Privacy Act should be amended to allow non-ACL holders to participate in reporting RHI.[71] Like ARCA, it argued that allowing data from entities such as telco, utilities and BNPL providers would better enable individuals with little to no credit history to access credit.

Consumer advocates expressed serious concerns relating to the use of credit reporting information, including RHI, by CPs or for credit products which are not subject to responsible lending obligations under the Credit Act.[72] They covered the legislative history and emphasised that the intention of Parliament was that only regulated products would have RHI reported against them, and only CPs considering applications for regulated credit products could access RHI. They also reflected individuals' concerns that 'negative' RHI might be listed on their credit reports, and that if the original credit was not subject to a proper affordability check as required by responsible lending obligations, this will distort the credit reporting system and disadvantage individuals.[73]

Review findings

The Review sought to capture stakeholder views on an important policy question that is related to, but distinct from, the CR Code itself.

Consumer advocates presented a strong case based on legislative history and intent that CPs must have an ACL and comply with responsible lending obligations before they are allowed to access credit reporting information.

---

[70] See ARCA submission, p 16.

[71] See ABA submission, p 4.

[72] See consumer advocates joint submission, p 15; Legal Aid Queensland submission, p 7.

[73] See consumer advocates joint submission, p 15.

Industry submissions argued that this position should be changed in the opposite manner – that access to RHI should not be restricted to CPs that hold an ACL. They raised consumer benefit – particularly establishing creditworthiness for 'new to credit' individuals – as a reason in favour of this position, although the Review notes that this would ideally be supported by real world evidence that this would in fact be the result.

The Review concludes that this is a broader policy issue for Government, which would have significant implications for the broader financial regulatory sphere. As such, this issue would benefit from consideration as part of the review of Part IIIA.

Proposal 9 – OAIC will raise the issue of whether an ACL should be a requirement to participating in the credit reporting system with the relevant Ministers

The OAIC recognises that this issue has significant implications for the broader financial regulatory sphere. As such, the OAIC will raise the issue with the relevant Ministers so that it can be holistically considered.

The OAIC will write to relevant Ministers so that this issue can be considered in preparation for the review of Part IIIA.

Part 3: Governance of the CR Code

The effective governance of the CR Code is central to instilling confidence that Part IIIA of the Privacy Act and the CR Code are being adhered to by regulated entities. Appropriate governance needs to ensure that protections are afforded to individuals and their right to privacy is respected, while facilitating an efficient credit reporting system and ensuring that the objective of the CR Code is being met.

The Review invited stakeholders' views and experiences in how the CR Code is developed and varied, and how compliance is monitored and enforced.

This part of the report is divided into two sections. The first is focused on governance of the Code itself including how it is developed, updated and overseen (3.1). The second focuses on governance requirements that apply to CRBs and CPs (3.2).

The report presents a number of proposals to strengthen governance across each of these areas.

3.1 Code governance, oversight and awareness

The OAIC is committed to ensuring the good governance of the CR Code and that regulated entities are complying with their obligations. The OAIC also considers that general awareness of the credit reporting framework, and the rights and obligations instilled within, is important.

The Review was interested in hearing from stakeholders about their experiences and sought feedback on opportunities for improvement.

Stakeholder submissions have continued to highlight the importance of good governance across areas of code development (i.e. development of the CR Code and any subsequent variations), monitoring of compliance with the CR Code and enforcement of its provisions.

The Review sought feedback regarding the current processes for code governance, and how the CR Code is monitored and enforced.

This section of the report presents findings in relation to:

- how the CR Code is developed and amended (3.1.1)
- processes for monitoring and enforcing compliance (3.1.2)
- opportunities to enhance industry and individual's education and awareness of their obligations and rights (3.1.3).

3.1.1 Code development

The Privacy Act provides for the development of Codes to further particularise the Privacy Act to certain industries or acts and practices. It also envisages that there will be a credit reporting code that will further particularise the provisions of Part IIIA. The Privacy Act envisages that the development of Codes will be an industry led process, with the Information Commissioner providing independent review and approval. After careful consideration by the OAIC, ARCA was requested to be the code developer for the CR Code.

The first CR Code was drafted by ARCA in 2013.[74] As code developer, ARCA also develops variations to the CR Code. Variations can be developed at any time to ensure the Code remains current and fit for purpose. Variation applications are submitted to the Information Commissioner for independent review, and may require amendment before being approved. To date, ARCA has developed and submitted four variation applications to the OAIC which have been approved following engagement with OAIC staff.

The Review sought feedback regarding the current process for developing variations to the registered CR Code.

Stakeholder views

Code governance, and particularly the role of ARCA as code developer, was the subject of significant feedback in both roundtable consultations and written submissions. The feedback differed considerably, with consumer and industry groups holding strongly opposed views.

Some consumer advocates raised strong objection to ARCA holding the role of code developer, with concern primarily centred on a perception that any privacy code (and subsequent amendments) developed by an industry body could not adequately consider consumers and would tend to favour an industry perspective.[75] Industry representatives, on the other hand, pointed to the deep expertise within ARCA about the credit reporting landscape, and felt the consultation and other efforts taken by ARCA evidenced the seriousness with which it takes its role.[76]

During roundtable consultations, some stakeholders observed that ARCA takes a 'policy shop' (rather than holistic) approach to the development of variations to the CR Code – that is, ARCA appears to internally determine the need for a variation, conducts research, drafts the relevant variation and then circulates the contents of the draft variation to stakeholders along with explanation for their review and feedback. This was considered by some stakeholders to be less than ideal, with roundtable consultations suggesting that an earlier entry into the process would enable stakeholders to better influence the nature or scope of proposed variations.

Review findings

The Review notes that under the Privacy Act, the CR code developer is an entity, or association of entities, subject to Part IIIA.[77] Part IIIB also specifies the required activities of a code developer and the permitted contents of a written code of practice.

The OAIC code development regime is consistent across Privacy Codes under the Privacy Act and is not particular to credit reporting. Codes registered under the Privacy Act are not intended to be consumer-facing, but rather are legislative instruments directed at regulated entities which have legal effect. This differs from other codes, such as the Banking Code of Conduct, which is voluntary and approved by ASIC, but is not a legislative instrument.

[74] The CR Code was approved by the Information Commissioner and registered in 2014.

[75] See Legal Aid Queensland submission, p 8; consumer advocates joint submission, p 16.

[76] See ARCA submission, p 16; Communications Alliance submission, p 4; Experian submission, p 7.

[77] Privacy Act, s 6.

The OAIC's *Guidelines for Developing Codes* state the factors that the Commissioner will take into account in identifying an appropriate code developer including whether they:[78]

- have the capacity to develop a code (both in terms of resources and expertise), and
- are generally representative of the entities in the sector or industry to which the code will apply.

ARCA has sufficient expertise in the credit reporting space and is appropriately resourced to undertake the code developer role. Further, no stakeholder was able to point to a more appropriate body to undertake the role of code developer during the Review process.

Given ARCA's expertise and the OAIC's role in independently approving any variations to the CR Code, the Review considers that this appointment remains appropriate. We acknowledge that ARCA commits significant time and resources to developing variation applications, and regularly meets consultation requirements. The consultation requirements in the *Guidelines for Developing Codes* provide important safeguards to ensure that variations to the CR Code have undergone appropriate consultation with relevant stakeholders.

Notwithstanding this, the Review has heard stakeholders concerns about their ability to provide early input on proposals before formal drafting is prepared. The Review considers that the CR Code would benefit from all stakeholders being invited to provide early input on proposals for variation applications.

A good example of this process in practice is the current work being undertaken by ARCA to understand the relationship between domestic abuse and credit reporting outcomes.

To address stakeholder concerns regarding consultation on proposed variations, the Review proposes that the OAIC review and update its *Guidelines for Developing Codes* to further articulate expectations as to how the consultation and approval process should operate.[79]

Proposal 10 – OAIC to update the *Guidelines for Developing Codes* regarding processes for the development of variation applications

The OAIC will update the *Guidelines for Developing Codes* to outline expectations on how variation applications will be developed. It is proposed that the Guidelines will require stakeholder input at an earlier stage (i.e. at an issues identification stage before decisions are taken to draft specific provisions).

[78] OAIC, *Guidelines for Developing Codes*, OAIC, 2013, [2.49].

[79] Section 26V of the Privacy Act provides that the Commissioner may make written guidelines to, among other things, outline the matters that the Commissioner may consider in approving a variation to the CR Code.

3.1.2 Compliance and monitoring

The CR Code provides for the OAIC's ongoing compliance monitoring of CRBs, CPs and AIRs, which are additional to the OAIC's general oversight of organisations regulated under the Privacy Act. Most notably the CR Code:

- requires the Commissioner to undertake an independent review of the operation of the CR Code every four years
- requires CRBs to commission an independent review of their processes every three years – CRBs must consult with the Commissioner as to the scope and choice of the reviewer and provide the OAIC with a copy of the report, while also making it publicly available.

The CR Code also requires CRBs to ensure that regular audits of CPs are undertaken to show their compliance with Part IIIA and the CR Code in accordance with their written agreement.

This Review considered the 2017 independent review recommendation that the OAIC internally review its regulatory activities in respect of the CR Code and, having regard to its available resources or ability to seek further funding if required, consider options for increasing its proactive monitoring and enforcement activities.

Another consideration of this Review was whether, in accordance with Part 3 of the OAIC's *Guidelines for Developing Codes*, a body (i.e. a code administrator or code administration committee) could be established to assist with compliance objectives.[80]

The Review sought feedback regarding whether additional compliance monitoring and governance arrangements should be stipulated in the CR Code.

Stakeholder views

Proactive monitoring and enforcement of the CR Code was a matter on which many stakeholders provided comment. In early consultations, and at the roundtable sessions, consumer advocates were concerned that not enough is presently being done to prioritise consumer outcomes through compliance monitoring.

While ARCA submitted that it is unaware of any significant compliance issues with the CR Code,[81] other stakeholders nevertheless noted the need for enforcement of (and reporting on) repeated or ongoing breaches of CR Code provisions. AFIA noted that a code compliance committee (or similar) would improve governance and build awareness of, and trust in, the CR Code by all stakeholders, including financiers and consumers.[82]

The CPRC stated that the rights and protections afforded to consumers should be at the heart of the credit reporting regime, and that a more dedicated focus on enforcement by the OAIC would support

[80] This is a consideration first raised in 2013; where, in its code development process, ARCA asked industry and consumer representatives whether there is a sufficiently compelling case for an additional layer of governance – that is, a code administrator that oversees CPs and CRBs and reports to the Commissioner on matters of compliance.

[81] See ARCA submission, p 17.

[82] See AFIA submission, p 5.

this.[83] Where CPRC, EWON and consumer advocates more broadly were in favour of the creation of independent governance arrangements, such as a separate code administrator or committee, ARCA considered that creation of such arrangements would effectively duplicate the role of the OAIC.[84]

ARCA also referred to its submission to the review of the Privacy Act more broadly, that it would be supportive of an industry levy to fund the OAIC.[85]

Review findings

The Review considers that non-compliance with the CR Code – whether minor or systemic – is more likely to be identified and addressed through a proactive monitoring and enforcement regime. The Review acknowledges that there is a broad agreement among stakeholders that achieving such a regime should be a priority, but that there were divergent views as to the best solution.

The Review notes that the OAIC undertakes regulatory and policy work in relation to credit reporting. For example, the 2020-21 Annual Report published details about the number and type of credit complaints received by the OAIC. However, stakeholder feedback generally reflects that this work is not well known by the broader community.

Furthermore, in addition to this, the OAIC undertakes regulatory and policy work, such as responding to enquiries from regulated entities and individuals, engaging with stakeholders such as EDR schemes on issues relating to compliance with Part IIIA and the CR Code and advising on proposed Bills that impact on privacy and credit reporting. The Review considers that more could be done to raise the visibility of the OAIC's current regulatory and policy work, including where it engages with EDR schemes on issues relating to compliance with Part IIIA and the CR Code.

Proposal 11 – OAIC to raise visibility of its credit reporting compliance and monitoring activities

The OAIC will consider how information relating to its credit reporting compliance and monitoring activities can be shared with the community more broadly to increase the visibility of this work.

The Review considers that the OAIC is best placed to undertake compliance and enforcement work given its expertise and its position as an independent regulator. We note that the OAIC's ability to discharge its monitoring and enforcement functions are subject to it being appropriately resourced. The Review also acknowledges that the OAIC must make decisions about where to focus its resources.

The Review does not consider that the introduction of new or additional oversight arrangements is necessary; rather, the objective should be to ensure that the OAIC is appropriately resourced to properly enforce existing arrangements. As such, the Review supports the exploration of increased resourcing for the OAIC via a suitable avenue so that it may effectively discharge its credit reporting oversight functions.

[83] See CPRC submission, p 2.

[84] See CPRC submission, p 2; ARCA submission, p 17.

[85] See ARCA submission, p 17.

Proposal 12 – OAIC will raise with the Attorney-General the issue of exploring alternative funding avenues to support the OAIC's credit reporting functions

The OAIC will raise with the Attorney-General the need for ongoing funding for the OAIC in respect of its credit reporting oversight functions, in preparation for the review of Part IIIA.

Any funding model would need to preserve the OAIC's regulatory independence and enable the OAIC to direct its resources to priority areas as needed.

The OAIC will write to Government so that this issue can be considered in preparation for the review of Part IIIA.

3.1.3 Education and awareness

The foundation for compliance with any legislative scheme is strong general awareness of key concepts and requirements. Education and other knowledge-building initiatives can assist with this.

The OAIC has published detailed information about the CR Code on its website. However, it does not currently conduct training for industry or individuals. ARCA, as code developer and the industry body with extensive practical expertise, has published information about its role as code developer and has been developing guidance for individuals in consultation with civil society groups which is available online.[86]

The Review sought feedback regarding the extent to which industry and individuals have access to the information they need to understand and/or apply the CR Code in practice.

Stakeholder views

There was general agreement among stakeholder submissions that better, though not necessarily more, information is needed for industry and individuals to understand and apply the CR Code.

AFIA stated that a lack of education and awareness in the sector has resulted in some undesirable outcomes. For example, it stated that the growth of the 'credit repair' industry, and the lack of consumer understanding about credit reporting, has led to exploitative companies stepping in and generating profits from individuals even though free, financial support is available from financial institutions, financial counsellors and others.[87]

Several stakeholders questioned whether more information would be helpful, given factors such as lack of user engagement and sophistication, as well as the risk of information overload.[88]

On the other hand, both ARCA and consumer advocates noted that effective information delivery needs to be accessible, multi-channel (including via advisers and intermediaries), and context and

[86] See CreditSmart website.

[87] See AFIA submission, p 6.

[88] See, e.g. consumer advocates joint submission, p 21; FBAA submission, p 4; CPRC submission, p 3; Legal Aid Queensland submission, p 10.

time specific.[89] In particular, consumer advocates considered that investment in educational resources should be directed at advocates such as community lawyers, domestic violence advocates or financial counsellors rather than more direct-to-consumer resources.[90]

Some stakeholders also suggested that the OAIC could play a more active role in education and awareness, such as through the provision of plain-English guidance that outlines the key rights and obligations of individuals.[91]

Review findings

This Review finds that ARCA's work – which has been done in consultation with other relevant stakeholders – to explain its role as code developer and provide guidance to consumers via the Credit Smart website should continue. [92] We accept the stakeholder feedback that any further OAIC guidance should be tailored, timely and relevant, so that:

- individuals with a specific issue or need can easily access information to practically guide them in that situation
- consumer advocates and representatives working on behalf of individuals are able to understand and apply provisions in the CR Code and Part IIIA effectively.

Complementary to this, the Review notes the OAIC's role to promote understanding and acceptance of the CR Code.[93] We consider that Proposal 1 at 2.1 of this report (OAIC to consider mechanisms to promote its credit reporting resources) will have the dual benefit of educating consumers and their advocates about (a) how the CR Code should be interpreted and applied, and (b) individual rights of consumers under the CR Code.

The Review heard a number of areas in which stakeholders have raised the need for additional guidance. A snapshot is presented below. These issues are discussed throughout this report in relation to specific CR Code provisions or individual rights and protections. Each of these have a corresponding proposal to develop specific guidance on these issues.

- **CCLI** – Ensure account is reported as closed when consumer credit is terminated or otherwise ceases to be in force (refer to 4.1.2 and Proposal 15)
- **Publicly available information** – Develop guidance on the concept of creditworthiness to help participants determine what 'court proceedings information' and 'publicly available information' may be collected and disclosed (refer to 4.4 and Proposal 23).
- **Notice** – Develop guidance to clarify notice versus consent when it comes to CPs' disclosures of personal information and information requests to CRBs (refer to 5.1 and Proposal 26).

[89] See ARCA submission, p 19; consumer advocates joint submission, p 21; Legal Aid Queensland submission, p 10.

[90] See consumer advocates joint submission, p 22.

[91] See Experian submission, p 7; Communications Alliance submission, p 4; ABA submission, p 5; CPRC submission, p 4.

[92] Credit Smart website.

[93] Privacy Act, s 28(1)(c)(iv).

- **Protections for victims of fraud** – Develop guidance for individuals and CRBs aimed at clarifying and simplifying the credit ban application and extension process (refer to 5.2.2 and Proposal 30).
- **Access** – Develop guidance to explain that individuals do not need to supply their credit reports to landlords and real estate agents to support their rental applications (refer to 5.3.5 and Proposal 35).
- **Correction** – Develop guidance aimed at explaining the correction process, including individuals' rights and obligations under the CR Code and Part IIIA (refer to 5.4.1 and Proposal 36).

OAIC to publish guidance on the above issues

The OAIC will develop and publish guidance on the above issues. Refer to Proposals 15, 23, 26, 30, 35 and 36 throughout the report for further details.

3.2 Governance obligations applying to CRBs and CPs

The Privacy Act establishes a closed system, in which only certain entities can have access to credit information. It is important that CRBs and CPs are only collecting, using or disclosing credit reporting information for the purposes outlined in the Privacy Act. These provisions ensure that an individual's privacy is respected, while also ensuring an efficient credit reporting system.

The Privacy Act and the CR Code outline a range of policies and processes that CRBs and CPs must follow to ensure compliance with their obligations. These provisions are intended to enhance transparency around regulated entities' activities, and increase confidence in their information handling practices.

The Privacy Act and the CR Code also set out the role of the Information Commissioner in monitoring compliance and undertaking enforcement action where necessary.

The Review sought feedback regarding the current governance obligations and processes were sufficient or required amendment.

This section of the report presents findings in relation to:

- the provisions on credit reporting agreements, audits, training and policies (3.2.1)
- the provisions regulating internal practices and recordkeeping (3.2.2).

3.2.1 Audits, training and policies

The Privacy Act and the CR Code establish a range of governance processes which provide for the monitoring of compliance. These requirements are set out below. These processes are in addition to the oversight powers and functions of the OAIC.

CRB agreements and audits of CPs

Part IIIA establishes requirements that CRBs and CPs must have written agreements in place to ensure the accuracy and security of credit information being supplied from CPs to CRBs.[94] These written agreements are a mechanism to ensure the credit information that the CP gives to the CRB is accurate and to safeguard any credit reporting information it receives from the CRB.

Part IIIA also requires that CRBs ensure CPs are undertaking regular independent audits to check compliance with those written agreements.

The CR Code imposes some additional requirements in paragraphs 2, 3 and 23, including for example that credit reporting agreements between a CRB and a CP must oblige both parties to comply with Part IIIA, the Regulations and the CR Code[95] and CRBs must publish its credit reporting policy on its website.[96]

Independent audit of CRBs

Separately, the CR Code also requires CRBs to commission an independent body to undertake regular audits of their operations and processes to assess compliance with their obligations under Part IIIA, the Regulations and the CR code. CRBs must consult with the Commissioner on the appointment of the independent auditor, and the scope of the audit. A copy of the independent audit report must also be provided to the OAIC.

The Review sought feedback regarding the provisions on credit reporting agreements, audits, training and policies.

Stakeholder views

Stakeholders were divided on the appropriateness of the existing provisions.

ARCA submitted that the provisions are appropriate and no specific amendments are required.[97] Experian also considered the provisions to be appropriate. They asserted that most audits of CPs result in findings or observations about compliance, implying that they do add value.[98]

Consumer advocates submitted that the current system of relying almost entirely on CRBs to monitor CPs' compliance with their Part IIIA obligations represented a conflict of interest.[99] They argued that as CPs are paying clients, CRBs would be less incentivised to report incidents of non-compliance under the CR Code, at least compared to an independent governance body.

Consumer advocates further considered that the results of the CRB audits prescribed by ss 20N and 20Q should be made public, even if it is on a de-identified basis and in periodic tranches.[100] This would

[94] Privacy Act, ss 20N and 20Q.

[95] See paragraph 2 of the CR Code.

[96] See paragraph 3.1 of the CR Code.

[97] See ARCA submission, p 20.

[98] See Experian submission, p 8.

[99] See consumer advocates joint submission, p 22.

[100] See consumer advocates joint submission, p 22; Legal Aid Queensland submission, p 11.

bring a level of transparency and accountability to CP compliance with credit reporting obligations that does not currently exist.[101]

Review findings

The Review did not find evidence of serious, systemic breaches by CPs involving the quality or security of credit report information. However, it is difficult to conclude that there are no issues with CPs complying with their obligations given the limited visibility over the current processes.

The Review considers that in principle, there is limited risks with CRBs auditing CPs' practices, especially where the audits are required to be conducted by an independent person. CRBs have strong incentives to care about receiving high quality credit reporting information and to ensure that the credit reporting information they disclose is securely handled. However, the Review accepts that the current process may result in a perceived conflict of interest and that without transparency, the effectiveness of audits and their outcomes is necessarily limited in achieving its purpose.

The Review notes that currently paragraph 23.11(o) of the CR Code requires CRBs to report information about its monitoring and auditing activity for each financial year. Having reviewed the latest annual report (2020-21) for each CRB[102] – in particular their sections on 'monitoring and auditing activities' – the Review considers that the publicly available information is insufficient to provide confidence about the effectiveness of these monitoring and auditing activities. This is both a function of the current drafting of paragraph 23.11(o) as well as the CRBs' approach in describing their activities at a high level.

The Review supports the idea raised by some stakeholders that CRBs' audits of CPs be published to help give confidence that compliance monitoring is both rigorous and effective. These can be redacted as needed to ensure they do not include personal information, or commercially sensitive information. Such audits could be made available alongside the CRBs' credit reporting policies and annual reports. Publication of audit reports would support the OAIC's oversight, offering an indication of possible systemic issues that may warrant further regulatory activity via a targeted assessment or investigation.

Proposal 13 – Amend the CR Code to require CRBs to publish their CP audits and submit these to the OAIC

Amend paragraph 23 to require CRBs to publish their CP audits and submit these to the OAIC. These reports can be redacted as needed for publication to ensure they do not include personal or commercially sensitive information.

---

[101] Consumer advocates also noted that there are no public transparency or accountability mechanisms incorporated into paragraphs 5.3 and 5.4 (Practices, procedures and systems), 15 (Security of credit reporting information) or 22 (Record keeping) of the CR Code.

[102] See Equifax Australia Information Services & Solutions Pty Limited, *2020/2021 Credit Reporting Annual Report* (August 2021); Experian Australia Credit Services Pty Ltd, *Annual Credit Report 2020 - 2021* (August 2021); Illion Data Registries Pty Ltd, *Annual Report* (August 2021).

Further, the Review finds that there would also be benefit in ensuring that the independent audit reports of CRBs are easily accessible by individuals. While CRBs are currently required under the CR Code to make their reports publicly available,[103] this is usually done by providing a link on their website.

However, the Review heard that individuals are not always aware of these reports, or do not have access to them. Further, it is inconsistent across CRBs how visible these reports are, and how long they are publicly available for. As such, the Review finds that there would be benefit in the OAIC also publishing links to these CRB audit reports available on its website, to ensure the reports are accessible, and to increase transparency and visibility over these audit processes.

Proposal 14 – OAIC to publish a link to CRB audit reports on its website

The OAIC will publish links to the CRBs' audit reports (provided under paragraph 24 of the CR Code) on its website to promote transparency of CRB practices. These reports can be redacted as necessary to ensure they do not include personal or commercially sensitive information.

[103] Paragraph 24.2 of the CR Code.

3.2.2 Internal practices and record-keeping

Part IIIA of the Privacy Act contains provisions that require CRBs and CPs to implement internal procedures and systems to ensure compliance with Part IIIA and the CR Code.[104] Part IIIA and paragraphs 5.3, 5.4, 15 and 22 of the CR Code also impose recordkeeping obligations. In particular, the CR Code:

- details what a CRB or CPs internal practices, procedures and systems must cover
- requires CRBs and CPs to maintain reasonable practices, procedures and systems to ensure information security
- prohibits CRBs and CPs from standardising CP numbering conventions for consumer credit
- gives further information about how CRBs and CPs must meet their recordkeeping obligations, including what to record when relevant credit information is collected, disclosed, or destroyed
- specifies that records should be retained for a minimum of five years unless, the CRB is required by Part IIIA, the Regulations or the CR code to destroy the information at the end of the applicable retention period.

The Review sought feedback regarding the provisions regulating internal practices and recordkeeping.

Stakeholder views

The Review did not receive significant feedback from stakeholders on the provisions of internal practices and recordkeeping. However, ARCA and Experian raised a discrete issue about the application of the data retention and destruction provisions to data input files.[105]

Data input files are the vehicle in which CPs disclose credit information to CRBs. Data input files can contain multiple records for each account (i.e. a mixture of different types of credit information, subject to different retention periods). Upon receipt, the CRB extracts information contained in the data input file and enters it into the CRB database, which is the 'source of truth' for credit information; the information is then managed and destroyed according to the relevant retention period. However, the data input file is retained in a separate database and serves as a record for the CRB; it provides evidence of the actual disclosure of credit information, which could become relevant if a complaint or dispute later arises with respect to the information.

ARCA and Experian noted that because the data input file represents a 'mix' of different types of credit information, there is no practical way to destroy certain elements of the data upon reaching the retention period without also destroying the entire file. ARCA suggested that the CR Code could be amended to provide a limited exemption for data input files from retention period and destruction

[104] Privacy Act, ss 20B and 21B.

[105] See ARCA submission, p 20; Experian submission, p 8.

requirements.[106] Experian called for clear guidance as to the period of time that such data input files can be retained.[107]

ARCA observed that this issue of data input files was not well understood at the time of drafting of the data retention and destruction provisions in the Privacy Act and the CR Code.

Review findings

The Review finds that data input files are subject to the retention periods and exceptions set out in Part IIIA of the Privacy Act (to the extent the data input file holds a type of credit information). ARCA and Experian have raised practical issues where there are different types of credit information with different retention periods contained in the one data input file.

Section 20W of the Privacy Act does not prescribe a retention period in circumstances where a record may retain credit information which is subject to multiple retention periods. Section 20ZA of the Privacy Act outlines that where a CRB is not required to destroy information because they are authorised or required by law to retain it, it must not use or disclose that information. That is, the CRB is entitled to retain but cannot use the information. In these circumstances, the OAIC would expect that the CRB has appropriate processes and controls in place to quarantine that information to ensure it is not used or disclosed.

OAIC Resolution of Practice Issue 1 – CRBs should have appropriate controls in place to quarantine information from future use or disclosure, where necessary

If CRBs are retaining information beyond the specified retention period, because they are authorised or required to do so, they must have appropriate controls in place to quarantine that information from any future use or disclosure.

[106] See ARCA submission, p 21.

[107] See Experian submission, p 8.

Part 4: Types of information

Under the Privacy Act there are a range of different types of credit information. Each information type provides different insights into an individual's overall creditworthiness. Under the Privacy Act, each information type is subject to unique requirements, reflective of what the information represents about an individual.

The Review was interested in hearing stakeholders' views and experiences on whether the safeguards around each information type were operating as intended. In particular, the Consultation Paper sought stakeholders' views, experiences and suggestions regarding the following types of information:

- consumer credit liability information (4.1)
- repayment history information (4.2)
- default information and payment information (4.3)
- publicly available information (4.4)
- serious credit infringements (4.5).

4.1 Consumer credit liability information

Consumer credit liability information (CCLI) relates to information about an account that an individual has (for example, an individual's loan or their credit card account). For this reason, CCLI is sometimes referred to as account information.

CCLI captures a range of different information points, including:[108]

- the name of the CP
- whether the CP is a licensee
- the type of consumer credit (for example, a loan or a credit card account)
- the day on which the consumer credit is entered into
- the terms or conditions of the consumer credit that relate to repayment of the amount of the credit (such as whether the repayments are principal and interest, or interest only)
- the maximum amount of credit available under the consumer credit
- the day on which the consumer credit is terminated or otherwise ceases to be in force.

This information can be used by CPs when the individual applies for a new loan to assist CPs in assessing whether the individual can afford the new debt. This information stays on an individual's credit report while the loan is open and for two years after it is closed.

[108] Privacy Act, s 6(1).

The CR Code contains specific provisions applying to CCLI. In particular, paragraph 6 defines the meaning of key CCLI information points, requires common descriptors be used by CPs when disclosing CCLI to CRBs, and requires CPs to tell the CRB when credit is terminated or ceases to be in force.

The Review sought feedback regarding the provisions regulating the collection, use and disclosure of CCLI. This section of the report presents findings in relation to:

- technical reporting of 'account open date' (4.1.1)
- listing of CCLI for inactive accounts (4.1.2)
- what CCLI can be reported on a guarantor's credit report (4.1.3)
- whether historic (previously disclosed) CCLI can be disclosed (4.1.4).

4.1.1 Account open date

One of the key information points about CCLI is when the account was opened. Paragraph 6.2 of the CR Code explains that 'the day on which the consumer credit is entered into' aligns with the unconditional approval of credit and the generation of the credit account in the CP's system. However, at times there is a gap between approval and account generation, which could lead to uncertainty about which date the CP should give to the CRB when providing CCLI.

Stakeholder views

ARCA flagged this issue in the Review. It explained that this tended to occur with home loan and construction loan accounts, where the gap could be weeks or even months.[109] This is because individuals get approved for a loan, but then might take time to be a successful purchaser of a property. ARCA has canvassed this issue with its members and reported during the roundtable that they are clear as to when the account should be considered opened, namely when both conditions – approval and account generation – are met.

ARCA further considered whether it is possible to use unconditional approval as the sole factor and concluded that this could lead to potential individual confusion and could generate unnecessary disputes.[110] Ultimately its view is that there is nothing that can be practically done and there would be little benefit to changing the definition in the CR Code.

The Review did not receive other stakeholder submissions on this issue.

Review findings

The Review recognises that in limited circumstances there could be an issue with the account open date as explained by ARCA. After receiving formal submissions, the Review followed up with consumer advocates about this issue and they reported that they do not see this as a big issue that required amendment to the CR Code, or other action being taken.

[109] See ARCA submission, p 21.

[110] See ARCA submission, p 22.

In light of the above, the Review concludes that nothing further needs to be done at this point in relation to this issue, except for ongoing monitoring.

4.1.2 Listing CCLI for inactive accounts

Another information point for CCLI is when the account is closed. Paragraph 6.2 of the CR Code sets out the situations in which consumer credit is terminated or otherwise ceases to be in force (i.e. when the account is 'closed'). In some cases, it appears that where debt buyers purchase debts from the original CP, the debt buyer continues to provide CCLI to the CRB where that account has been 'charged off' by the original CP but has not been reported as closed. The practical effect of this practice is that debts can potentially live on in the credit reporting system indefinitely as CCLI. This is at odds with the data retention provisions in Part IIIA which require disposal of default information after five years.

Stakeholder views

Stakeholder submissions agreed that this is an issue that should be addressed.

Consumer advocates were very concerned about the practice of listing CCLI for credit accounts that are no longer active with the original CP. They reported coming across multiple examples where the debt buyer discloses CCLI to CRBs in such situations and noted that this contravenes the Privacy Act and is confusing to individuals.[111] They also considered that individuals should be able to request the removal of CCLI if the debt is statute barred and the original CP has not disclosed to the CRB when the debt was charged off.[112]

Legal Aid Queensland raised a similar issue with debt buyers listing CCLI where a court judgment has been obtained to terminate the credit contract, but the judgment has fallen off the credit report (the retention period being 5 years for court proceedings information).[113] Legal Aid Queensland suggested that the CR Code could clarify that once a judgment is obtained, the contract which formed the basis of the litigation is terminated.

ARCA shared consumer advocates' concerns with this practice. ARCA noted that the intention of the account close definition is that where the credit has been charged off by a CP, but a debt remains outstanding, the credit will be reported as closed.[114] ARCA supported amending the CR Code to limit the ability to 'pick and choose' how the account close date is reported, to prevent a debt buyer submitting CCLI for an account which has been charged off.

Review findings

The Review finds that the current practice of listing CCLI for accounts that are supposed to be closed circumvents the intentions of Part IIIA and the CR Code. It also causes confusion to individuals.

The Review considers that paragraph 6.2 of the CR Code should clarify that consumer credit is reported as closed on the *earlier* of any of the following events occurring – consumer credit is

[111] See consumer advocates joint submission, p 25.

[112] See consumer advocates joint submission, p 27.

[113] See Legal Aid Queensland submission, p 11.

[114] See ARCA submission, p 22.

terminated, consumer credit is charged off, or consumer credit is repaid. This will prevent the current practice of CPs choosing which event amounts to an 'account close' date

Proposal 15 – Amend the CR Code to clarify the definition of 'account close' in respect of CCLI

Amend paragraph 6 of the CR Code so that consumer credit is reported as closed on the earlier of these events occurring – consumer credit is terminated, consumer credit is charged off, or consumer credit is repaid.

4.1.3 Information disclosed on a guarantor's credit report

A guarantor for a borrower is responsible for paying back the loan if the borrower cannot. Currently, the Privacy Act allows default information regarding the guarantor's failure to pay an overdue payment under the guarantee to be disclosed on that guarantor's credit report. However, there is uncertainty as to what other information (if any) can be disclosed on the guarantor's credit report in respect of the credit which that individual has guaranteed.

CCLI is defined in s 6(1)(e) of the Privacy Act to include terms or conditions of an individual's consumer credit that relate to the repayment of the amount of credit, and that are prescribed by the regulations.

The Privacy Regulation 2013 ss 6(d) and 6(f) state that these terms and conditions include whether the individual is a guarantor to another individual's credit, and any variation to the terms or conditions of that credit arrangement.

Stakeholder views

ARCA considered that there was uncertainty around interpretation of s 6 of the Privacy Regulation, and whether information should be reported on the guarantor's credit report.[115]

ARCA argued that CCLI about credit guaranteed by an individual, but for which the individual is not the borrower, should not be disclosed on the guarantor's credit report.[116] Among other reasons, it noted that information about guaranteed credit does little to aid the assessment of the guarantor's creditworthiness.

ARCA considered that to resolve the current uncertainty, the Privacy Regulation should be amended to remove s 6(d) (which refers to an individual's guarantor status).[117] Once that has occurred, the CR Code could be amended to specify that the only information permitted to be disclosed in respect of credit guaranteed by an individual is guarantor default information or an information request.

The Review did not receive other stakeholder views on this issue.

[115] Privacy Regulation, s 6(d).

[116] See ARCA submission, p 11.

[117] See ARCA submission, p 12.

Review findings

The Review considers that the Privacy Regulation is clear on what CCLI should be disclosed on a guarantor's credit report. The regulations do not extend to the terms and conditions of the guarantor arrangement. That is, only information that the individual is a guarantor, and information about any changes made to the terms and conditions of the guaranteed consumer credit arrangement, should be disclosed in relation to the guarantee.

On the suggestion that the CR Code be amended to clarify that the only information permitted to be disclosed in respect of credit guaranteed by an individual is guarantor default information or an information request, the Review considers this is not necessary. This is already provided for by ss 6Q(2) and 6R(1)(c) of the Privacy Act.

In light of the above, the Review does not consider that any changes are required to be made to the Privacy Regulation or the CR Code to address this issue.

4.1.4 Historic CCLI

The Consultation Paper sought stakeholder views on uncertainty about whether CRBs could use 'historic' CCLI (that is, CCLI that had previously been disclosed to the CRB) associated with a consumer credit account.

The Review canvassed whether a CRB may hold and disclose multiple entries about the credit limit associated with an account (referred to as 'the maximum amount of credit available under the consumer credit'), or whether only the existing (or current) limit may be held and disclosed.

This issue also arises in relation to other CCLI information points – for example, whether a CRB can, or should, record both current and previous CPs for an individual.

Stakeholder views

Stakeholder submissions were mixed as to whether it is feasible and/or desirable for CRBs to hold current and historic CCLI associated with a consumer credit account.

ARCA thought there is merit in including both historic and current CCLI for categories such as credit limit, the name of the CP and possibly changes to certain terms and conditions (e.g. that the credit has changed from 'principal and interest' to 'interest only' and vice versa).[118] However, it noted that the reporting of a historical dataset would also need to consider a range of technical difficulties such as how many previous datasets could be reported.[119] It submitted that understanding how a credit limit or term and condition has changed would enable CPs to better assess an individual's creditworthiness. Furthermore, there would be a consumer benefit for individuals to have a record of CPs, such as in debt purchase scenarios. ARCA considered that the CR Code could be amended to provide this clarity.[120] Experian was also supportive of amending the CR Code to facilitate this.[121]

---

[118] See ARCA submission, p 22.

[119] See ARCA submission, p 23.

[120] Ibid, p 23.

[121] See Experian submission, p 9.

Equifax noted as a matter of fact that CRBs collect both current and historic CCLI, and that it saw nothing in the Privacy Act to prevent a CRB from using and disclosing either information as CCLI.[122] It noted that CRBs have a responsibility to ensure that the CCLI it uses and discloses is accurate and up to date. It argued that the current credit limit remains accurate, by reference to the point in time to which it relates. Equifax submitted that there are a number of examples of point in time, historical credit information (including CCLI) that may continue to be held by CRBs even when updated information is available, pursuant to s 20W of the Privacy Act.[123]

Consumer advocates considered that the CCLI definition in the Privacy Act and the CR Code refer to a 'maximum amount of credit available under the consumer credit' – that is, a single amount that is current at the point where it is updated.[124] Similarly, the Privacy Act and the CR Code definitions refer to 'credit provider' and 'provider', both of which are singular. While consumer advocates saw value in the credit report listing past CPs under the same contract so that individuals can recognise the debt, they submitted that any change regarding historic CCLI would require an amendment to the Privacy Act.[125]

Review findings

The Review considers that as a starting point the retention provisions outlined in s 20W of the Privacy Act state that CCLI can only be held for 2 years from the day that the consumer credit is terminated or otherwise ceases to be in force. After this date, the CCLI needs to be destroyed.

As to the disclosure of 'historic' CCLI during this time, the Privacy Act's definition of CCLI is silent as to whether it includes current and/or historic information about the account, and the explanatory materials for this do not clarify how it should be interpreted. The Review notes that this aspect of the legislation is ambiguous, and it is open on a statutory interpretation approach to take either position.

Therefore, at this stage, the OAIC has taken the position that only current CCLI should be disclosed to ensure consistency across CRBs. In our view, this position is more consistent with the overall intention of the credit reporting framework in Australia to protect consumers, and the wording used in the definition of CCLI in s 6 of the Privacy Act. This interpretation also supports the principle that a CRB should only hold the minimum amount of information necessary to ensure the protection of personal information is balanced with the need to undertake credit reporting activities. This clarification by the OAIC will allow industry to take a consistent approach when reporting this information, resulting in more predictable outcomes for individuals.

However, the Review also considers that given the lack of clarity outlined above, it would be appropriate to raise the issue of the meaning of 'historic' CCLI for the purposes of the Privacy Act for further consideration in the review of Part IIIA by the Attorney-General.

---

[122] See Equifax submission, p 2.

[123] Privacy Act s 20W which prescribes retention periods for credit information.

[124] See consumer advocates joint submission, p 27.

[125] See consumer advocates joint submission, p 28.

OAIC Resolution of Practice Issue 2 – CRBs should only disclose current information when disclosing CCLI

To ensure consistency, the OAIC considers that industry should only disclose current CCLI to a CP regarding a consumer. This is more consistent with the overall intention of Part IIIA of the Privacy Act.

Proposal 16 – OAIC to raise with the Attorney-General the issue of disclosing 'historic' CCLI

The OAIC will write to the Attorney-General to raise the issue of clarifying the definition and disclosure practices relating to current and 'historic' CCLI, so it can be considered in preparation for the review of Part IIIA.

4.2 Repayment History Information

The Privacy Act allows CPs to disclose whether individuals are meeting their obligations under their credit arrangement. This is reported as Repayment History Information (RHI) and shows on a month-by-month basis if an individual has made their loan payments on time. It indicates to other CPs how the individual manages their debt.

RHI is defined in s 6V of the Privacy Act to include:[126]

- whether or not the individual has met an obligation to make a monthly payment that is due and payable in relation to the consumer credit
- the day on which the monthly payment is due and payable
- if the individual makes the monthly payment after the day on which the payment is due and payable (i.e. where the payment is overdue) – the day on which the individual makes that overdue payment.

Paragraph 8 of the CR Code contains specific provisions applying to RHI which:

- clarify aspects of the definition of RHI, including what it means for payments to be overdue
- specify the reasonable steps a CP must take when disclosing RHI to a CRB, for example that a CP cannot disclose RHI about that credit more frequently than once each month.

The CR Code also introduces a 14 day grace period for individuals before RHI is reported. Therefore, a CP can only report a missed payment if the individual hasn't paid within the grace period of 14 days. When an individual applies for a new loan, the lender can see that individual's RHI for the previous 2-year period. RHI is reflected by a number on the credit report - '0' meaning that the payment has been made on time, '1' meaning that the individual is 15-29 days overdue, etc.

[126] Privacy Act, s 6V.

Under the Privacy Act, not all CPs can report or access RHI. CPs need have an ACL or be prescribed by the regulations. Generally, this means that only banks, credit unions and other types of finance companies can report or access RHI. Other companies like telcos, gas and electricity providers cannot access or report RHI.

The Review sought feedback regarding the provisions regulating the collection, use and disclosure of Repayment History Information.

This section of the report presents findings in relation to:

- addressing uncertainty about monthly reporting of RHI (4.2.1)
- inability to correct RHI due to circumstances beyond the individual's control (4.2.2)
- whether individuals should be notified about certain disclosures of RHI to CRBs (4.3).

4.2.1 RHI and monthly reporting

As outlined above, RHI is shown on a credit report on a month-by-month basis, that is it shows how many days an individual is overdue for that month. The CR Code specifies how CPs should determine overdue days in an RHI reporting month. The CR Code restricts CPs from disclosing RHI more frequently than once a month.[127] The CR Code also defines 'month' as a period starting at any day of a calendar month and ending:

- immediately before the start of the corresponding day of the next calendar month
- where the day in (1) is a non-business day, the end of the next business day following that day, or
- if there is no such day, at the end of the next calendar month.[128]

The Consultation Paper sought stakeholder's experience with whether this reporting was operating well in practice, particularly whether shorter months might be skewing the reporting of subsequent months.

Stakeholder views

There were limited submissions on the issue of monthly reporting.

ARCA identified a discreet technical issue from its members with determining the RHI 'month' outlined in the CR Code against varying calendar dates.[129]

ARCA submitted that on the current definition, the RHI 'month' would only align to the definition for months ending in the 31st and it is not clear how a RHI month should be treated when the calendar month ended on the 28th, 29th or 30th. It noted that this issue is relatively limited and would depend on the type of CP product and the RHI reporting approach adopted by the CP. ARCA suggested minor amendments be made to the CR Code to allow CPs to apply a level of flexibility when setting, or resetting, the RHI month.

[127] Paragraph 8.2(a) of the CR Code.
[128] Paragraph 1.2(i) of the CR Code.
[129] See ARCA submission, p 23.

Review findings

The Review considers that the current difficulties identified with determining the RHI 'month' may be clarified by amending the definition outlined in the CR Code. The current definition may need to be amended to provide flexibility for CPs in reporting RHI and resolve situations where a strict interpretation of the meaning of a 'month' would result in a poor consumer outcome. Any amendments to the CR Code should be guided by the principles that reporting should reflect an individual's expectations around their repayment obligations and reflect their repayment behaviour.

Addressing this issue would also ensure that industry is reporting RHI consistently and that it is provided with the clarity it needs to apply, and comply with, its obligations.

Proposal 17 – Amend CR Code to clarify definition of 'month' to more flexibly accommodate CP reporting practices

Further consideration should be given to amending paragraph 1.2(i) of the CR Code to clarify the definition of 'month'. Any amendments to the CR Code should be guided by the principles that reporting should reflect an individual's expectations around their repayment obligations and reflect their repayment behaviour.

4.2.2 Flexibility not to list or to remove RHI

Currently paragraph 20.5 of the CR Code allows an individual to request correction of default information if it relates to an overdue payment which occurred because of 'unavoidable consequences of circumstances beyond the individual's control.'[130] This correction right does not extend to RHI. Nor is there any other flexibility in the CR Code in terms of not listing RHI related to missed payments in the event of unavoidable circumstances.

The Review sought stakeholder's views on whether this remained appropriate.

Stakeholder views

There was generally consensus among stakeholders that the CR Code should enable individuals to request correction of RHI in certain unavoidable circumstances, including where an individual is a victim of domestic abuse.

Consumer advocates argued that the CR Code can and should protect individuals from having information disclosed on their credit files that does not reflect their creditworthiness. They submitted that paragraph 20.5 should also apply to the correction of RHI if it relates to missed payments (i.e. 'negative RHI') that occurred in unavoidable circumstances.[131] Legal Aid Queensland also noted the absence of such a correction right in the CR Code and recommended its inclusion.[132]

[130] The report uses the phrase 'unavoidable circumstances' as shorthand to refer to 'unavoidable consequences of circumstances beyond the individual's control'.

[131] See consumer advocates joint submission, p 29.

[132] See Legal Aid Queensland submission, p 12.

ARCA was also supportive of this proposal, while noting a possible implementation issue regarding correction versus suppression of RHI depending on if an individual can establish that the payment obligation was met.[133]

Review findings

Enabling correction of RHI relating to a missed payment in unavoidable circumstances benefits both individuals and industry by providing a more accurate picture of a person's creditworthiness. It also serves to reassure individuals who may be going through a difficult period that they will not be disadvantaged by RHI which shows a missed payment obligation on their credit report where this was beyond their control. Amending the CR Code would appear to address this issue.

The Review notes that this proposal can be folded into a broader proposal to enable correction of other kinds of credit-related personal information in unavoidable circumstances, including not just default information but also RHI and CCLI. We discuss this further in section 5.4.4 and Proposal 41 of the report below. We have also restated this proposal below, for ease of reading.

Proposal – Amend CR Code to expand the categories of information that can be corrected

Amend paragraph 20.5 to expand the categories of information that can be corrected beyond just that of default information.

4.2.3 Notification of RHI disclosures

Part IIIA of the Privacy Act requires a CP to notify individuals of certain matters if the CP is likely to disclose the information to a CRB.[134] For example, CPs must notify individuals in relation to the disclosure of default information,[135] and the CP's opinion that an individual has committed a serious credit infringement.[136] However, there are no specific notification obligations when the CP is disclosing RHI which relates to missed payment obligations of an individual.

Suggestions had been raised that it would be beneficial to require CPs to notify an individual when they disclose RHI that shows a payment is overdue. The Review sought stakeholders' views on this suggestion.

Stakeholder views

Consumer advocates were in favour of requiring CPs who are reporting missed payments to notify their customers on regular account statements or by SMS, about the information reported to the CRB and its meaning.[137] They argued that doing so would have benefits across the board. They stated that for CPs, this would increase consumer confidence, encourage timely payments and reduce complaints. For individuals, it would enable them to change their behaviour, dispute adverse listings

[133] See ARCA submission, p 24.

[134] Privacy Act s 21C(1).

[135] Privacy Act, s 21D(3)(d).

[136] Paragraph 12.1(f) of the CR Code.

[137] See consumer advocates joint submission, p 29.

in a timely fashion and they would be more aware of the impacts on their credit reports. Lastly, for CRBs it would enable them to hold more accurate information if consumers are informed and given an opportunity to correct errors at the time of listing.

The FBAA opposed the requirement for CPs to separately notify individuals when reporting RHI which relates to missed payment obligations. It argued that this requirement would lead to a significant reporting burden that is likely to be unmanageable for CPs and lead to individuals being overwhelmed with notifications.[138]

ARCA also opposed this requirement. It noted that default information and serious credit infringements were 'one off' events which are clearly understood to have a negative impact on an assessment of an individual's creditworthiness, thus warranting a notification.[139] By contrast, RHI is an ongoing monthly dataset that reflects an individual's account behaviour, where compliance or non-compliance with payment obligations is already reflected in account statements and payment reminders. Finally, ARCA noted that this issue was raised as part of the 2017 CR Code review and that review concluded that the issue needed to be addressed by legislative reform to Part IIIA.

Review findings

The Review appreciates the strong views on both sides in relation to notification of RHI that shows a missed payment obligation.

We consider that consumer advocates raise good points about the potential benefits for all stakeholders if individuals were to receive timely and effective notice of the fact that their missed payments will be being reported to a CRB, and the effect of this.

The Review also acknowledges the points raised by industry stakeholders in relation to practicality, notification fatigue and the fact that RHI is qualitatively different to information about events that clearly have a negative impact on an individual's creditworthiness (such as defaults and serious credit infringements).

Furthermore, the Review is mindful of the risk imbalances in the credit reporting system, where a minor action or inaction on the part of the CP or the individual can have a significant detrimental impact. For example, consumer advocates included two case studies where individuals ended up in an adverse financial situation because they were not notified earlier about their RHI reporting a missed payment obligation.[140]

On balance the Review supports the idea of CPs notifying individuals when they are reporting RHI relating to missed payments only (i.e. notification will not be required when regular RHI is reported). However, we consider that for such notifications to be effective, their implementation must be approached thoughtfully. For example, the implementation should:

- not be onerous for CPs to carry out
- mitigate against the risk of notification fatigue

[138] See FBAA submission, p 4.

[139] See ARCA submission, p 25.

[140] See consumer advocates joint submission, pp 30-32.

- be distinct from existing regular communications about account statements and payment reminders.

However, given this will be a significant change to the credit reporting system, the Review considers that such an obligation would better sit in the principal legislation. As such, the OAIC will write to the Attorney-General on this issue. This issue of how notification operates more generally in the CR Code is further considered in section 5.1.1 of this report.

Proposal 18 – OAIC to raise with the Attorney-General the suggestion that CPs must notify an individual when they disclose RHI relating to missed payments

The OAIC will raise with the Attorney-General the suggestion of introducing a requirement that CPs notify individuals about disclosure of RHI relating to missed payments. The OAIC will write to the Attorney-General so that this issue can be considered in preparation for the review of Part IIIA.

4.3 Default information and payment information

The Privacy Act permits CRBs to collect default information (information that relates to overdue payments) and payment information (information relating to payment of an overdue payment previously disclosed to a CRB as default information).[141]

As default information is likely to have an impact on an individual's credit report, the Privacy Act has strict requirements which must be met before this this information can be collected, used or disclosed. For example, the payment must be at least 60 days overdue, and the amount overdue must be $150 or more and not statute barred.

Further, the Privacy Act also requires CPs to update CRBs when an overdue amount has been paid, if they had previously disclosed this as default information.[142]

Paragraph 9 of the CR Code applies to default information and:

- explains the process for when an individual has submitted a hardship request – i.e. a CP must not disclose default information to a CRB if it is in the process of deciding an individual's hardship request
- specifies the timing and order of notices provided by CPs to individuals about repaying the overdue payment (s 6Q) and the fact that default information will be disclosed to the CRB (s 21D(3)(d))
- explains how overdue amounts must be reported including in cases where additional amounts have accrued since the s 21D(3)(d) notice.

Paragraph 10 of the CR Code applies to payment information and:

- defines what it means for an overdue payment to be considered paid

[141] Privacy Act, ss 6Q and 6T.

[142] Privacy Act, s 21E.

- requires the CP to disclose payment information to the CRB within 3 days if the individual requests this.

The Review sought feedback regarding the provisions regulating the collection, use and disclosure of default information and payment information.

This section of the report presents findings in relation to:

- establishing a positive obligation on CPs to request the removal of default information that has become statute barred (4.3.1)
- requiring CPs to list any defaults with CRBs within a reasonable period of time (4.3.2)
- requiring a standalone s 21D(3)(d) notice (4.3.3)
- resolving uncertainty about how to report 'new arrangement information' (4.3.4).

4.3.1 Removal of statute barred debts

Default information cannot be reported where the CP is prevented by a statute of limitations from recovering the overdue payment.[143] In practice however, such defaults that are listed on a credit report may not be removed until (or if) an individual realises they are stature barred and seeks their removal.

Paragraph 20.6 of the CR Code states that on request by an individual, a CRB must correct credit reporting information it holds by destroying default information where the statute of limitations to collect the debt has expired. In other words, where it is stature barred from collecting the debt.

The Review canvassed whether CPs should have a positive obligation to ask or notify a CRB to destroy default information when the statute of limitations has expired for recovery of the overdue amount.

Stakeholder views

ARCA noted that paragraph 20.6 of the Code already imposes a correction obligation on a CRB to destroy default information for a statute barred debt.[144] It was not supportive of introducing a positive obligation unless there was evidence of non-compliance with the existing provision.

Consumer advocates strongly supported establishing a positive obligation on CPs to remove statute barred debts. They provided case studies where defaults are listed just prior to the statute of limitations taking effect and are not removed once that date is reached, thus continuing to negatively impact an individual's credit score.[145] They observed that many individuals would have no idea that the debt is statute barred even if they get a copy of their credit report and see the default.

Consumer advocates further argued that the principles underpinning paragraph 20.6 to enable the removal of default information due to a statute of limitation should also apply to other types of

[143] Privacy Act, s 6Q(1)(c).

[144] See ARCA submission, p 26.

[145] See consumer advocates joint submission, p 33.

information, including CCLI and RHI.[146] They considered that paragraph 20.6 should be amended accordingly.

EWON and TIO also supported establishing a positive obligation on CPs.[147] EWON agreed with consumer advocates that the negative impact on individuals' credit reports could continue well beyond the statute barred date if the default information was still listed. EWON further suggested that CPs should be required to include the date that the debt fell overdue when reporting to the CRB, to help identify debts that exceed the statute barred period.[148]

The Communications Alliance agreed that there should be a positive obligation to remove statute barred debts, but that this should lie with CRBs rather than CPs, given that the retention period is based on the date that CRBs collected the default information.[149] It suggested a similar idea to EWON that CPs could provide a 'limitations' date to the CRBs at the time of listing a default to indicate when a debt will become statute barred.

Review findings

The Review acknowledges that paragraph 20.6 of the CR Code already requires CRBs to destroy default information that relates to an overdue payment that is statute barred. However, the onus is on individuals to *request* this removal. Submissions received from consumer advocates and industry ombudsmen during this Review indicate that this very rarely happens in practice, as individuals are often not aware of the applicable statute of limitation period.

The Review finds that currently there is a significant imbalance in that:

- individuals have the burden of initiating the correction of statute barred debts
- many individuals do not have a sophisticated understanding of credit reporting and may not be aware that there is a problem in the first place[150]
- failure to correct statute barred debts can have significant and tangible negative impacts on their ability to access credit.

The Review considers that the CR Code should be amended to address this imbalance. Based on the submissions and further deliberation, we consider that it is preferable for the positive obligation to be placed on CRBs to take reasonable steps to remove default information. This is because:

- CRBs have a more comprehensive view into individuals' default information
- CRBs operate nationally and would need to be aware of the statute of limitations in various jurisdictions

[146] See consumer advocates joint submission, p 14.

[147] See EWON submission, p 3; and TIO submission, p 6.

[148] See EWON submission, p 3.

[149] See Communications Alliance submission, pp 4-5.

[150] For example, TIO noted that individuals often do not learn about default listings until they apply for credit, which can be many years after the default has been listed – see TIO submission, p 6.

- it would be simpler for the CRBs to do the correction rather than adding an extra compliance layer for CPs.

However, to assist CRBs with this obligation, the CR Code should also be amended to impose a corresponding obligation on CPs to take reasonable steps to inform CRBs when a debt has or will become statute barred. CPs should also list the date that the debt became overdue.

The Review notes that making these proposed changes to the CR Code will complement existing requirements in Part IIIA for CPs and CRBs to maintain the quality of credit information. Under s 21U of the Privacy Act, CPs have an obligation to maintain the quality of its credit information (including default information),[151] and where they make a correction, they are required to notify each recipient of the information of this correction, including CRBs).[152] Likewise, CRBs have a general obligation to take reasonable steps to maintain the quality of its credit information.[153]

The Review further considers that it may be beneficial for industry to develop a consistent approach for CPs to report default information in a way that helps CRBs to identify when debts will exceed the statute barred period.

Proposal 19 – Amend CR Code to introduce positive obligations on CRBs to remove statute barred debts and on CPs to inform CRBs when a debt has or will become statute barred

Paragraph 20.6 of the CR Code should be amended to require:

- CRBs to remove statute barred debts from individuals' credit reports where it is reasonable for them to have been aware of the statute of limitations
- CPs to take reasonable steps to inform CRBs when a debt has or will become statute barred
- when disclosing default information, CPs to provide CRBs with the date that the debt became overdue.

The above amendments should not alter the ability of an individual to request removal.

The Review has considered the proposal to amend paragraph 20.6 to be inclusive of amending all credit information. We conclude that it does not need to be changed.

The provision turns on the operation of statutes of limitation that legally bar CPs from enforcing debt obligations against individuals after a certain period. The intention of paragraph 20.6 is to remove information that would enable a CP to represent that it can take enforcement action against an individual. Other credit information, such as CCLI and RHI, indicate the facts about the contract rather than going to its enforcement. In any case, as consumer advocates noted in their submission most of this information should be excluded already under the relevant retention periods.

[151] That is, 'having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading' – Privacy Act, s 21U(1).

[152] Privacy Act, s 21U(2).

[153] Privacy Act, s 20N.

4.3.2 Listing default within reasonable period and extending such listings

Under the Privacy Act the retention period for default information commences from the date the CRB receives that information (i.e. the date that the CP discloses the default information to the CRB).[154]

Paragraph 9.3(f) of the CR Code requires that a CP disclose default information to the CRB within 14 days of, and no later than 3 months after, the date on which the CP gives a s 21D(3)(d) notice to the individual.

The Review was interested to understand practices around when defaults are listed by CPs, and whether any delays to listing default information resulted in artificially extending the period that default information would appear on an individual's credit report.

Stakeholder views

Legal Aid Queensland noted the example of defaults being listed many years after the credit contract became due and payable, and recommended that if CPs wish to list a default they must do so within a reasonable period or otherwise lose the right to list (as opposed to a mandatory obligation to list).[155]

TIO noted that it receives complaints about aged default listings and submitted that these complaints could be reduced if CPs and CRBs were required to take earlier action in listing or removing defaults.[156] EWON likewise supported a requirement for CPs to list defaults within a reasonable timeframe. It proposed a period of 12 months, which may need to be adjusted to different industries and entities.[157]

On the other hand, the Communications Alliance submitted that the proposal to list defaults within a reasonable timeframe is problematic because there would need to be multiple exemptions given the complex nature of debt collections. They submitted that this could lead to an increase in compliance burdens.[158] It suggested that a better way to address the problem would be to amend the Privacy Act so that CRBs must retain default information for up to 5 years from when the debt was overdue, rather than from when they collected the default information.

ARCA raised the different legal and industry instruments that govern the reporting of default information, including the mandatory supply requirements under the Credit Act and the data standards of the PRDE.[159] It considered that a requirement to list defaults within a reasonable period is a matter for those instruments rather than for the CR Code.

Review findings

The Review is concerned by the examples provided and the possible practice that CPs are choosing to list defaults years after the initial debt was incurred by the individual. It appears to show that default listings are being artificially extended by a CP or 'reset' by a subsequent debt buyer who decides to

---

[154] Privacy Act, s 20W.

[155] Ibid.

[156] See TIO submission, p 6.

[157] See EWON submission, p 4.

[158] See Communications Alliance submission, p 5.

[159] See ARCA submission, p 26.

list the default again. This practice is not in keeping with the intention of Part IIIA. The Review considers that a default should be listed within a reasonable time from when the debt was originally incurred. This will need to be addressed through amendments to Part IIIA.

Further, the Review acknowledges that this may also show an issue with the wording of Part IIIA, where the retention of default information in s 20W is determined by the day on which the CRB *collects* the information. If a CP takes years to list a default, when the CRB eventually receives the information, it is obliged to retain it for a further 5 years from that date. This effectively may result in default information being kept for a much longer period than what was envisioned under Part IIIA, and arguably circumventing the purpose of s 20W.

The Review concludes that these issues should be considered in the required independent review of Part IIIA.

Proposal 20 – OAIC to raise with the Attorney-General the suggestion that CPs must list default information within a reasonable time and retention period should apply from date of default

The OAIC will raise with the Government the need for:

- CPs to be required to list default information within a reasonable time of the debt being incurred, and
- the CRB retention period in 20W to apply from the date of the default, not the date the CRB collects the information.

The OAIC will write to the Attorney-General so that these suggestions can be considered in preparation for the review of Part IIIA.

4.3.3 Standalone s 21D(3)(d) notices

Section 21D(3)(d) of the Privacy Act states that a CP can disclose default information about an individual to a CRB if it has given the individual a notice in writing stating its intention to disclose and 14 days have passed since that notice was issued. Paragraph 9.3(a) of the CR Code specifies that the s 21D(3)(d) notice must be given separately to the s 6Q notice (which is an earlier notice informing the borrower of their default and requesting that they pay the overdue payment).

It appears that in some cases, the s 21D(3)(d) notice is included in other correspondence to the individual. As such, there is a question about whether this reduces individual awareness about the fact that a default is about to be listed and whether CPs should be required to issue a separate notice instead. The Consultation Paper sought views on this issue.

Stakeholder views

Stakeholder submissions were mainly in favour of requiring a standalone s 21D(3)(d) notice to be issued.

Consumer advocates stressed that default notices need to be clear and distinct from any other type of written correspondence, or the risk is very high that individuals will not read them in time to resolve

or dispute the overdue payment.[160] EWON supported the standalone notice as it would aid customer understanding of the status of their debt and the potential consequences of non-payment.[161] TIO was also supportive, noting that it is standard practice for telco providers to send standalone notices to individuals where the provider intends to disclose default information.[162]

ARCA stated that it was unclear as to when s 21D(3)(d) notices may be combined with other notices.[163] It noted that since the s 21D(3)(d) notice is the subsequent notice given where the failure to pay has not been rectified, and as a matter of practice it is likely to be a standalone notice.

Review findings

In principle, requiring a standalone s 21D(3)(d) notice has several benefits, including that:

- it aids in individual understanding and action to address an overdue payment
- it enables CPs to communicate clearly to individuals about what will happen and potentially receive payment
- it would be consistent with industry good practice.

The Review did not receive any contrary arguments. Given the impact for individuals, we consider there is merit in clarifying that a s 21D(3)(d) notice must be a standalone notice in the CR Code.

Proposal 21 – Amend CR Code to specify that s 21D(3)(d) notice must be a standalone notice

Amend paragraph 9.3 to specify that the s 21D(3)(d) notice communicating intention by a CP to disclose default information to a CRB must be provided as a standalone notice and not bundled with any other correspondence.

4.3.4 New arrangement information

Under the Privacy Act, new arrangement information about an individual is a statement that the terms and conditions of the original consumer credit have been varied, or that the individual has been provided with other consumer credit that relates to that amount of credit (either wholly or in part).[164]

The Privacy Act provides that new arrangement information is a type of credit information. The CR Code briefly addresses new arrangement information in provisions relating to serious credit infringement disclosure (paragraph 12.2) and correction of default information (paragraph 20.5(a)(ii)) but does not otherwise regulate new arrangement information.

[160] See consumer advocates joint submission, p 33.

[161] See EWON submission, p 4.

[162] See TIO submission, p 6.

[163] See ARCA submission, p 26.

[164] Privacy Act, s 6S.

Stakeholder views

Consumer advocates raised an issue with uncertainty in the CR Code about how to report payment information where a default is resolved through the establishment of a new arrangement with the individual, and the new arrangement does not involve full payment of the original overdue amount.[165] They recommended that paragraph 10 of the CR Code be amended to resolve this uncertainty.

On the other hand, ARCA reported that it has received feedback from members indicating that new arrangement information has become a largely redundant dataset.[166] This is because it is technically complex to report and there is limited practical utility in doing so. ARCA is in the process of amending the PRDE to remove new arrangement information as a contribution requirement. It submitted that there is little value in amending the CR Code provisions dealing with new arrangement information, given the shift away from the use or disclosure of this dataset.[167]

Experian confirmed that very few CPs are currently reporting new arrangement information.[168]

Review findings

Notwithstanding the issue identified by consumer advocates, the feedback received by the Review is that new arrangement information may not be reported and used by industry.

While the introduction of financial hardship information into the credit reporting system is outside the scope of this Review of the CR Code, moving forward, the Review acknowledges that financial hardship arrangements may have an impact on the utility of new arrangement information and its purpose. However, as new arrangement information is a type of information listed in the Privacy Act, we consider that this is a matter better addressed by the review of Part IIIA.

Proposal 22 – OAIC to raise with the Attorney-General the ongoing application of new arrangement information

The OAIC will raise the issue of the ongoing application of new arrangement information with the Attorney-General in preparation for the review of Part IIIA.

4.4 Publicly available information

The Review has heard that there was confusion about what information can be recorded as publicly available information, particularly when it comes to court judgments.

Section 6N of the Privacy Act defines credit information to include 'publicly available information' and 'court proceedings information'.

Publicly available information is information about an individual's credit activities or creditworthiness in Australia, that is not 'court proceedings information' or information on the

[165] See consumer advocates joint submission, p 33.

[166] See ARCA submission, p 27.

[167] Ibid.

[168] See Experian submission, p 9.

National Personal Insolvency Index.[169] CRBs are permitted to collect, use and disclose 'publicly available information' if it relates to the individual's creditworthiness and meets those additional requirements.

'Court proceedings information' is defined in the Privacy Act to mean a judgment that is made about the individual in relation to credit that was applied for, or provided to, the individual.[170]

Paragraph 11 of the CR Code was introduced to clarify the definition of 'publicly available information' including what information a CRB can collect. This was because there were some circumstances where court judgments may not meet the definition of 'court proceedings information' under the Privacy Act but may nonetheless be captured by the definition of 'publicly available information'. Paragraph 11.2 of the CR Code was introduced in 2020 to provide clarity regarding this situation. This paragraph excludes the following from being 'publicly available information':

- originating processes from a Court or Tribunal
- any judgments or proceedings where the individual's rights have been subrogated to an insurer, and
- any judgments unrelated to credit.

This is because the above does not relate to an individual's creditworthiness. It means that a CRB is prohibited from collecting this information.

The Review sought stakeholder views on how the provisions regulating publicly available information were operating in practice.

This section of the report presents findings in relation to what court judgments (if any) can be reported.

Stakeholder views

As noted above, paragraph 11.2(c) of the CR Code excludes 'any judgment or proceedings that is otherwise unrelated to credit' from the definition of publicly available information because this information does not relate to the individual's creditworthiness.

Many stakeholders raised concerns about when and what type of court judgments fall within the definition of publicly available information, given the exclusions in paragraph 11.2 of the CR Code and where the information is not court proceedings information. For example, stakeholders provided examples including debts relating to council rates.

ARCA considered that there is ambiguity in the CR Code. It noted that AFCA had previously questioned judgments that do not clearly fit the definitions, such as judgments for payments of council rates.[171] ARCA suggested further clarification may be needed in the CR Code regarding such judgments,

[169] Privacy Act, s 6N(k).

[170] Privacy Act, s 6(1).

[171] See ARCA submission, p 28.

including whether the judgment must have bearing on an individual's creditworthiness to be able to be collected or disclosed.

Consumer advocates submitted that the current wording of paragraph 11.2(c) is confusing and recommended that the provision be amended to provide more clarity around the types of judgments which do not go to creditworthiness.[172]

Consumer advocates stated that creditworthiness is the key to determining what other judgments could fall within the definition of publicly available information.[173] They cautioned that any clarification of judgments that go to an individual's creditworthiness should consider that individuals may be deterred from defending a matter in court if a judgment against them will be recorded on their credit report and will impact their ability to obtain credit in the future.[174]

Experian submitted that currently there is serious inconsistency and confusion among CRBs, individuals and AFCA regarding the recording of court proceedings and publicly available information.[175] Both consumer advocates and Experian noted a lack of parity between CRBs in the kinds of court proceedings and publicly available information that they report, which results in confusion for individuals.[176]

Experian raised the following issues that would benefit from greater guidance:[177]

- whether a judgment relates to credit that has been provided to, or applied by, the individual (especially given that various court registries around Australia have differing levels of detail regarding judgments)
- what kinds of court judgments relate to credit that has been provided to, or applied by, the individual. Currently, there are differences of opinion within industry on this
- what types of judgment relate to creditworthiness and can therefore be recorded as publicly available information
- whether the full judgment amount should be recorded on a credit file.

Review findings

The Review acknowledges the uncertainty in this area and stakeholders have raised a number of situations where it is unclear whether the information falls within the definition of credit information – whether as publicly available information or as court proceedings information.

The Review notes that the purpose of allowing the collection of publicly available information is to inform a CP about an individuals' creditworthiness. Therefore, information that does not relate to

[172] See consumer advocates joint submission, p 35.

[173] See consumer advocates joint submission, p 35. See also Legal Aid Queensland submission, p 12.

[174] See consumer advocates joint submission, p 35.

[175] See Experian submission, p 10.

[176] See consumer advocates joint submission, p 35; Experian submission p 10.

[177] See Experian submission, p 10.

credit should not be collected as it does not serve this purpose, and could unfairly prejudice an individual with factors that are not relevant to their ability to repay a loan.

Likewise, court proceedings information is restricted to information that relates to credit provided to, or applied for, by an individual. Therefore, judgments which do not relate to an underlying claim for debt cannot be captured as court proceedings information.

Furthermore, originating processes cannot be considered court proceedings information as it is not a judgment. The CR Code also excludes originating processes from the definition of publicly available information.

Given the uncertainty in this area, the Review considers that the development of guidance to outline the above principles may be helpful. For clarity, the guidance could also provide examples of cases that do not relate to an individual's creditworthiness and cannot be collected. Stakeholders provided the following indicative examples to the Review that they considered may not go to an individual's creditworthiness:

- judgments relating to driving or professional competency
- judgments in family law proceedings, such as relating to disputed (non-)payments and overpaid child support
- a person who disputes the quality or extent of building work and ends up with a judgment for an amount owing.

Proposal 23 – OAIC to develop guidance about 'court proceedings information', and 'publicly available information'

The OAIC will provide guidance on the principles to be considered when assessing whether information meets the requirements of 'court proceedings information' and 'publicly available information'. The OAIC will consider addressing specific examples raised by stakeholders.

4.5 Serious credit infringements

The Privacy Act allows a CRB to collect information about serious credit infringements (SCIs). A SCI is more serious than a default as it represents cases where an individual has fraudulently obtained credit, sought to fraudulently evade credit obligations, or no longer intends to comply with their credit obligations.

The CR Code contains specific provisions applying to SCIs in paragraph 12 and:

- requires a CP to reasonably establish that the individual made false statements when disclosing a SCI to a CRB
- sets out the reasonable steps a CP must take to contact an individual before the CP may disclose a SCI to a CRB after six months of no contact with the individual
- requires a CRB to destroy SCI information where the overdue amount has since been paid or the CP enters a new arrangement with the individual.

The Review sought feedback regarding the provisions regulating the collection, use and disclosure of Serious Credit Infringements.

Stakeholder views

ARCA noted that SCIs are no longer being disclosed by CPs, with each CRB indicating that no SCIs had been disclosed for the previous 12 months.[178] Experian added that the SCI provisions are rarely used in practice due to the onerous requirements currently in place.[179] It considered that the intended objectives of these provisions are not being met.

Consumer advocates stated that they have no concerns with paragraph 12 of the CR Code.[180]

Review findings

The feedback received by the Review is that the SCI provisions are not used often. The Review considers that this would reflect the seriousness of activities that would amount to an SCI. The Review did not receive any feedback about issues with these provisions as drafted. Therefore, the Review makes no findings in relation to this paragraph of the CR Code.

[178] See ARCA submission, p 28.

[179] See Experian submission, p 10.

[180] See consumer advocates joint submission, p 36.

Part 5: Protections and rights for individuals

The Privacy Act and the CR Code allow regulated entities to collect, use and disclose an individual's personal information for the purposes of credit reporting. This information assists credit providers in their business of providing credit to individuals. However, the Privacy Act balances the use of this information by ensuring that an individual's privacy is respected.

The CR Code contains a range of provisions that are intended to protect the rights and privacy of individuals. There are protections for victims of fraud, for individuals to complain and correct information about them and for individuals to access their information.

These protections and rights are supplemented by requirements on regulated entities. Such as the requirement to provide notice about how they will handle personal information in their business practices.

This Part discusses issues relating to the protections and rights provided for individuals in the CR Code.

The Review was interested in hearing stakeholders' views and experiences on whether the protections and rights for individuals were operating as intended. In particular, the Consultation Paper sought stakeholders' views, experiences and suggestions regarding the following:

- whether the notification requirements were fit for purpose (5.1)
- whether the protections for victims of fraud were effective (5.2)
- whether any amendments were required to the provisions providing for access rights (5.3)
- whether any amendments were required to the provisions providing for correction rights (5.4)
- the effectiveness of the complaint handling and dispute resolution processes for an individual (5.5)
- whether any amendments could assist in protecting individuals affected by domestic abuse (0).

5.1 Notice to individuals

One of the key pillars of effective information handling is being transparent with individuals about how an entity will handle an individual's personal information. These transparency obligations are critical in enabling individuals to exercise privacy self-management. They are also an important accountability mechanism for organisations.

The Privacy Act requires a CP to notify an individual that they are likely to disclose information to a CRB.[181] It also requires the CP to notify or ensure that the individual is aware of the CRB with which the CP shares information with and any other matters specified in the CR Code. This notification must occur at or before the time of collection of the personal information. In practice, most CPs provide this notice to individuals at the time they apply for a loan, or other credit product.

Paragraph 4 of the CR Code contains additional notice requirements, including outlining what a notice must include (referred to as 'notifiable matters'). It also outlines what steps a CP may take in

[181] Privacy Act, s 21C.

complying with its notification obligations – such as publishing a statement of the notifiable matters on its website and making the individual aware that its website contains information about credit reporting.[182]

Importantly, the Privacy Act and the CR Code do not require CPs to get an individual's consent before disclosing credit information to a CRB.[183] Rather, CPs have an obligation to notify the individual that this will occur. In preparing the Consultation Paper, the Review heard from stakeholders that there has been an increase in the number of credit reporting complaints based on individuals not having consented to the disclosure of their credit information.

The Review sought stakeholder views on how the notification provisions were operating in practice, particularly regarding whether there was confusion around requirements for notice and consent.

This section of the report presents findings in relation to how notification processes could be improved.

Stakeholder views

Stakeholders generally agreed that consumers are confused about whether their consent is required to disclose their information to a CRB, and when notification is sufficient.

Consumer advocates observed that most individuals do not understand that the reporting of information to CRBs only requires notice to the individual and not their consent.

Two industry ombudsmen submitted that they receive complaints that demonstrate consumer confusion about the difference between notice and consent for credit enquiries.[184]

ARCA considered that while the notification provisions are appropriate, it saw an issue with correction requests being made on the basis that the individual did not consent to the credit enquiry.[185] Given the level of misunderstanding of this issue, ARCA proposed changing the CR Code to make it explicit that information requests (also referred to as credit enquiries) only require notification to an individual, and do not require consent.

Review findings

Part IIIA is clear that notification, and not an individual's consent, is required for a CP to disclose personal information to a CRB.[186] However, the Review considers that there is a general level of misunderstanding in the community about what the law requires.

A potential cause of this is that individuals are not appropriately informed about when information is going to be disclosed. As such, the Review suggests that there may be merit in holistically reviewing the notification regime within the Credit Reporting framework. This should involve clarifying the

[182] Paragraph 4.2 of the CR Code.

[183] Privacy Act, s 6R(1).

[184] See EWON submission, p 5; TIO submission, p 3.

[185] See ARCA submission, p 28.

[186] Privacy Act, s 21C.

notification obligations in Part IIIA and reviewing the notification requirements that exist for CPs under paragraph 4 of the CR Code to ensure they are achieving their objectives in appropriately informing individuals about the circumstances in which their information will be used and disclosed. For example, paragraph 4 could outline the circumstances and principles around when notification will be required and how it should be provided. Consideration should be given to mechanisms that will ensure that notifications are meaningful. This would assist in ensuring individuals are adequately informed about when and how their information will be used, and should reduce the confusion and number of complaints from individuals.

In addition to amending the CR Code, the Review considers that there may be benefit in raising this issue with the Attorney-General for consideration in the 2024 review of Part IIIA.

In parallel, the Review considers it would be beneficial to have further guidance developed for individuals, which explain when notice is required and how this differs from instances where consent will be required.

Proposal 24 – Amend the CR Code regarding notification obligations

Paragraph 4 of the CR Code should be reviewed and amended to provide further clarity around notification obligations. These amendments should seek to ensure that the notification obligations in the CR Code remain fit for purpose taking account of s 21C of the Privacy Act

The amendments should provide further particularity around the circumstances and principles around when notification should occur, and what information should be provided.

The timing of these amendments should be considered, noting Proposal 25 which suggests a holistic review of the notice framework.

Proposal 25 – OAIC to raise with the Attorney-General the suggestion that the notice framework within Part IIIA be reviewed

The OAIC will raise the need for a holistic review of the notice framework within Part IIIA with the Attorney-General so it can be considered in preparation for the review of Part IIIA.

Proposal 26 – OAIC to provide guidance to individuals on which circumstances require notice and which require consent

The OAIC will develop guidance for individuals which clarify the circumstances in which a CP is required to provide notice and when an individuals' consent is required.

5.2 Protections for victims of fraud

The Privacy Act recognises that individuals who have been a victim of fraud are particularly vulnerable, and their credit information could be used in ways that could cause them harm. The

Privacy Act provides specific protections which allow a victim of fraud to act quickly to try to mitigate the risk of suffering losses.[187]

One of the key protections available to victims of fraud is the ability to ask that a CRB not use or disclose credit reporting information about them.[188] When this occurs, a CRB must not use or disclose this information during what is known as the 'ban period'. The Privacy Act provides that the ban period lasts for 21 days but may be extended if the individual requests an extension and the CRB believes on reasonable grounds that the individual has been a victim of fraud.

The CR Code contains additional requirements for ban periods in paragraph 17, which:

- set out actions that a CRB must take immediately if an individual asks the CRB to implement a ban period, or to extend a ban period
- allows the individual to ask the CRB to ask other CRBs to also implement, or extend, a ban period
- requires a CRB to tell CPs that request credit reporting information that a ban is in place and the effect of the ban
- requires a CRB to notify the individual at least five days before the ban period is due to end, that it is going to finish, and to explain the individual's rights to extend the ban period. The CRB must also explain what, if any, information it requires to support the individual's allegation of fraud.

The Review sought stakeholder views on how the provisions providing protections for victims of fraud were operating in practice.

This section of the report presents findings in relation to:

- the impact of the current 21 day credit ban period (5.2.1)
- the process for implementing and extending a ban (5.2.2)
- whether alerts should be provided to individuals during a ban period (5.2.3).

5.2.1 Credit ban period

The Review sought stakeholder feedback on how the credit ban period was operating in today's world and whether the 21 day period remained appropriate. The Review also noted that there were different approaches globally, including some jurisdictions where the ban applied indefinitely until an individual asks for the ban to be removed.

In seeking stakeholders' views, the Review acknowledged that this issue might be better considered by the 2024 review of Part IIIA. Nevertheless, feedback was sought in case opportunities existed to improve processes in the interim through amendments to the CR Code, or the development of guidance.

[187] Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 142.

[188] Privacy Act, s 20K.

Stakeholder views

There was broad agreement across stakeholder groups that the 21 day initial ban period is inadequate,[189] along with proposals to increase this to 30 days or even indefinitely.[190] Stakeholders also recognised that the 21 day period is provided for in the Privacy Act and so there is limited option for the CR Code to address this.

ARCA suggested that one approach to addressing the issue would be to maintain the 21-day initial ban period and specify in the CR Code a consistent period to be applied across CRBs for a ban period extension.[191] However, ARCA also cautioned that introducing changes to ban periods should seek to avoid situations where individuals use this to opt out of the credit reporting system (e.g. someone who was at significant risk of default placing a ban on their credit report to prevent a CP receiving an alert).[192]

Consumer advocates also suggested a possible approach for extending the credit ban period while complying with Part IIIA - amending the CR Code to require CRBs to give an individual the option to automatically extend the ban period when they first approach the CR Code to implement the ban.[193]

In addition to discussion on the ban period, Experian sought clarity on the word 'immediately' used in paragraph 17.1 of the CR Code (where an individual believes they have been a victim of fraud and requests that a CRB not use or disclose their credit reporting information, the CRB must 'immediately' put in place a credit ban). It noted that implementing the ban immediately is not possible, as it needs to verify identity first and take other steps prior to implementing the ban. It proposed use of the wording, 'as soon as possible after receiving a request' instead. [194]

Review findings

Section 20K of the Privacy Act stipulates that an initial ban will last 21 days. While the Review considers that there may be benefit in extending this initial ban period, and this has the support of the majority of stakeholders, this cannot be achieved through amending the CR Code. Therefore, the OAIC proposes to raise this issue with the Attorney-General to be considered in the review of Part IIIA.

Proposal 27 – OAIC to raise with the Attorney-General concerns around the length of initial credit ban period provided in Part IIIA

The OAIC will raise the issue of extending the initial ban period in s 20K from 21 days with the Attorney-General so it can be considered in preparation for the review of Part IIIA.

---

[189] See ARCA submission, p 29; consumer advocates joint submission, p 37; Legal Aid Queensland submission, p 13; Experian submission, p 11; Communications Alliance submission, p 6.

[190] See IDCARE submission, p 4; Experian submission, p 11.

[191] See ARCA submission, p 29.

[192] See ARCA submission, p 30.

[193] See consumer advocates joint submission, p 37.

[194] See Experian submission, p 11.

As to the extension of the ban period, the Privacy Act does not prescribe the length of ban extensions. Furthermore, the Explanatory Memorandum anticipates that the CR Code can provide further detail as to the operation of the extension process.[195] Therefore, the Review considers that it is open to the CR Code to particularise how extensions should apply. From stakeholder submissions, it does not appear that individuals are exercising their option to extend the ban period, even where it may benefit them.[196]

The Review has heard that the initial ban period is generally inadequate and that where an individual is a victim of fraud or a data breach it is likely that they will need to extend the ban period to protect against harm and misuse. The evidence provided by stakeholders suggest that individuals are able to request an initial ban, but for some reason this is often not extended (either because they are not aware of the process, or it becomes onerous to keep seeking multiple extensions).

The Review considers that there may be a benefit for CRBs to provide an option to individuals, at the time of requesting an initial ban, that they may 'automatically' extend the ban period, where the circumstances warrant this. The Review considers that this will protect individuals' credit reporting information during a particularly vulnerable time. The Review considers that the option to offer an 'automatic' extension to the ban period should be open to a CRB where the circumstances require this. The Review notes that this proposal is complemented by Proposal 29 which will provide further clarity for CRBs on the expected level of evidence that they need to implement an extension, including that CRBs should not require unduly onerous evidence from an individual. In our view, this would be a good interim solution until the initial ban period of 21 days can be reviewed as part of the independent review of Part IIIA.

Proposal 28 – Amend the CR Code to allow CRBs to offer individuals an automatic extension to the ban period when they make their initial request, where appropriate

Paragraph 17 of the CR Code should be reviewed and amended to allow CRBs to offer individuals with an automatic extension to the ban period at the time they initially request a ban, where appropriate.

These amendments should take into account the requirements of s 20K(4), and provide that CRBs should assess the appropriateness of this option in each case.

As to the issue raised by Experian, the Review acknowledges that CRBs will need to take steps to verify the identity of the person seeking the ban, prior to implementing it, and that this process is in keeping with the intention of the CR Code and Part IIIA. The Review considers that the use of the word 'immediately' in paragraph 17.1 however, is intended to capture the seriousness of situations that require credit bans, and that they should be acted on with haste to prevent any further detriment to the individual. The Review considers that changing this wording has the potential to reduce an individual's protections and is not necessary in order to clarify a CRBs obligations. For this reason, the Review does not propose to make this change.

---

[195] Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 143.

[196] ARCA noted in its submission that Equifax have internal analysis which shows that more than 70 percent of people do not seek a further extension beyond 21 days. See ARCA submission, p 29.

5.2.2 Burden of proof for demonstrating risk of fraud

As noted above, in order for a CRB to agree to extend a ban period, it must believe on reasonable grounds that the individual has been, or is likely to be, a victim of fraud.[197] Under the CR Code, CRBs can ask the individual for information to support the individual's allegation of fraud. The effect of Part IIIA and the CR Code is to put the onus on the individual. This may not be optimal in cases where the individual's identity credentials have been stolen, or it is otherwise difficult for them to meet the request (e.g. due to emotional distress). However, it is important to note that the Explanatory Memorandum[198] outlines that it is not expected that an individual would ordinarily need to present documentary evidence to support their application.

For this reason, the Review sought stakeholder views and experiences on how this was operating in practice.

Stakeholder views

Both consumer and industry stakeholders raised concerns with the current requirement under the Privacy Act for individuals to support an allegation of fraud, noting that it may be too high.

IDCARE noted that in its experience this has a negative effect on individuals attempting to extend credit bans if their identity credentials are lost.[199] Namely, they may not be able to extend a ban until they gain a police report number, which they can only do if they prove misuse has occurred. IDCARE observed this process is reactive and means that individuals must wait for misuse to occur, rather than proactively preventing that misuse.

Other stakeholders that advocated for a change in the current burden of proof include the Communications Alliance and TIO.[200]

Experian submitted that the current requirement for CRBs to believe on reasonable grounds that the individual has been a victim of fraud is unduly onerous and can result in inconsistent approaches between CRBs.[201] They considered that CRBs are placed in a difficult position of making a subjective determination as to whether or not there are 'reasonable grounds', and conversely that individuals are unnecessarily burdened with the task of collating proof of fraud. Experian welcomed more guidance on the level of proof or evidence required to extend the ban period. Although noted that its overarching position is that the ban period should be set by the individual themselves and should continue for as long as the individual requires.[202]

ARCA noted that the challenge for CRBs and CPs in cases of identity theft is often establishing that the individual claiming identity theft is the victim and not the fraudster seeking to change account

[197] Privacy Act, s 20K(4).

[198] Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 142.

[199] See IDCARE submission, p 5.

[200] See Communications Alliance submission, p 6; TIO submission, p 9.

[201] See Experian submission, p 11.

[202] See Experian submission, p 12.

credentials.[203] As such, it is important that some measure exists to ensure the person alleging fraud is legitimate.

Separately, Experian also expressed concern that they were unsure whether the collection of personal information was permissible. Under the current CR Code provisions, a CRB is required to communicate with an individual who requests a ban including to provide various information to the individual. To do so, the CRB needs to collect contact information from the individual. However, Experian considered that a strict reading of paragraph 5 of the CR Code leaves a question mark as to whether this kind of collection is permissible.[204]

Review findings

The Review has concerns with many of the case studies raised which suggest that the current process is not operating as intended. While the Privacy Act does not specify how a CRB should form a reasonable belief that an individual is or likely to be a victim of fraud, the Explanatory Memorandum does provide helpful guidance as to the intended operation of these provisions:

> '*Identity fraud can happen quickly and consequences for a victim of identity fraud can be significant. In this context, the purpose of this provision is to allow an individual who has been, or is likely to be, the victim of fraud to act quickly to try to ameliorate the risk of suffering losses. It is not expected that an individual would ordinarily need to, for example, present documentary evidence to support their belief.* '[205]

The Explanatory Memorandum further provides that when it comes to extending the ban period:

> '*A credit reporting body could ask the individual to demonstrate the basis for their belief that they are, or may be, the victim of fraud. This would depend on the circumstances of each case, but would not necessarily require any court based evidence (such as the arrest of a person who is alleged to have committed the fraud). In some cases, the risk of fraud may continue for a significant period and the credit reporting body should make a judgement in the circumstances of the appropriate period of time for the extension. It is not intended that an individual would be placed under additional stress by the imposition of short extension periods that have to be regularly renewed if the circumstances do not warrant this approach.*'[206]

The Explanatory Memorandum is clear that the process for an individual seeking to implement an initial ban period, or to extend that ban period, should not be unduly onerous or cause additional stress.

The Explanatory Memorandum acknowledges that where a ban period is being extended, the CRB needs to believe on reasonable grounds that the individual has been, or is likely to be, a victim of fraud. However, it also states that this could simply involve asking the individual to explain their basis for their belief, and should be determined on a case-by-case basis.

---

[203] See ARCA submission, p 30.

[204] See Experian submission, p 12.

[205] Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 142.

[206] Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 143.

The current situation appears to be suboptimal for individuals and CRBs alike. It also appears to be contrary to the intention of the legislation. The experience of organisations helping individuals is that the current burden of proof being expected can be unworkable and fails to proactively prevent fraud or misuse.

The Explanatory Memorandum specifically anticipated that the CR Code may provide further detail as to how the extension process should apply. As such, the Review proposes that amendments to the CR Code be made which clarifies that CRBs do not require detailed, documentary evidence to support their belief that they have been a victim of fraud.

To support these amendments, the OAIC will also develop guidance to individuals which provides a plain English explanation of the credit ban application and extension process.

Proposal 29 – Amend the CR Code to provide further clarity on the expected level of evidence that a CRB needs to implement a ban period and/or extension

Amend paragraph 17 of the CR Code to provide more detail about the expected level of evidence a CRB can require from an individual in implementing a ban period, and extending the ban. These amendments should clarify that CRBs should make an assessment on the circumstances of each case, but should not require unduly onerous evidence from an individual.

Proposal 30 – OAIC to develop guidance for individuals to explain the credit ban application and extension process

The OAIC will develop guidance for individuals explaining the credit ban application and extension process, and their rights during this period.

The OAIC will prioritise the development of such guidance to assist individuals until the 21 day period can be reviewed as part of the independent review of Part IIIA (refer Proposal 27 above).

We acknowledge the concern ARCA raised about CRBs and CPs ensuring that they are dealing with a legitimate individual in cases of identity theft. However, in the specific case of a credit ban this seems less of a concern since the point of applying for a ban is to prevent any further reporting of, or access to, credit, which is not something a bad actor would conceivably want to do.

On the issue raised by Experian of collecting personal information to process a credit ban request, the OAIC has taken the position that CRBs are permitted to collect and use personal information when communicating with individuals regarding credit bans.

OAIC Resolution of Practice Issue 3 – CRBs can collect and use personal information for the purposes of communicating with individuals to whom the information relates, regarding credit bans

CRBs are able to collect and use information from an individual for the purposes of implementing a ban or to otherwise communicate with them about a credit ban.

5.2.3 Alerts during credit ban

The Review canvassed a possible option to support victims of fraud by allowing free alerts to the individual where there has been an attempt to access their credit reporting information during a ban period. This would assist individuals to know that someone is still trying to access their report, and may support any fraud proceedings, or support an application for an extension to the ban period.

Stakeholder views

Stakeholders representing consumers were in favour of this proposal.[207] IDCARE reasoned that this would further inform individuals as to the risks relating to the actions of others attempting to gain credit in their name through unauthorised attempts at credit checking.[208]

The Communications Alliance submitted that rather than alerting individuals, which is likely to cause unnecessary stress and offers no resolution, alerts should instead be sent to CRBs and CPs so they know they are dealing with a victim of fraud or a banned identity/credential.[209]

ARCA and Experian questioned the premise of this proposal. Experian noted that credit enquiries are not recorded during a ban period and CPs are unlikely to provide consumer credit if there is a ban on the individual's credit file.[210] ARCA further observed that it is unclear whether alerts would play any role to assist the individual to monitor efforts by the fraudster to access their credit report, since credit enquiries are not recorded during a ban period.[211]

Review findings

The Review considers that while alerts may be useful in some circumstances, CRBs have outlined that currently there would be nothing to alert since they do not record credit enquiries during a ban period in the first place.

However, the Review had further engagement with ARCA on this issue, and understands that in principle CRBs may be able to record such access attempts in their systems. The Review considers that this outcome could be positive for individuals, on the basis that it could support an application for an extension of a ban period, or otherwise, assist the individual in proving fraud or theft against them. The Review therefore, considers that it is worth exploring the possibility of this further in consultation with CRBs.

Proposal 31 – Amend CR Code to require a CRB to record and alert an individual of access requests during a ban period

The CR Code should be amended to require CRBs to make a record of access requests during a ban period and alert individuals of any attempts to access this information during that period.

---

[207] See consumer advocates joint submission, p 40; Legal Aid Queensland submission, p 14; IDCARE submission, p 7.

[208] See IDCARE submission, p 6.

[209] See Communications Alliance submission, p 7.

[210] See Experian submission, p 12.

[211] See ARCA submission, p 30.

5.3 Access rights

A key right for individuals is the ability to request access to their credit reporting information. Credit reporting information is used for matters relating to an individual's credit related activities and errors or omissions may have significant consequences for the individual. As such, the Privacy Act recognises that it is essential that the individual be able to obtain free access on a reasonably regular basis.

Under the Privacy Act CRBs and CPs must provide that access to the credit reporting information that they hold about an individual.[212] The CRB or CP must provide this information within a reasonable period. A CRB is not permitted to charge for access, provided the individual (whether directly or through an agent) has not made a request for access within the preceding three months. If a request has been made within the preceding three months, the CRB may impose a charge, but this must not be excessive.

The CR Code contains additional requirements for access in paragraph 19, which:

- require CRBs and CPs to verify the individual's identity before granting access
- formally removes any access fee where the individual has been refused credit in the previous 90 days (even if they have received access to their credit information for free in the preceding 3 months)
- require CRBs to make clear an individual's rights to receive their credit report free of charge in certain circumstances
- outline the scope and manner of access required of CRBs and CPs, including that the information be presented clearly and accessibly with supporting explanation
- clarify that CRBs and CPs are not required to disclose proprietary data analysis methods or computer programs when responding to access requests.

The Review sought stakeholder views on how the access rights provisions were operating in practice.

This section of the report presents findings in relation to:

- how an individual could access all of their credit reports (5.3.1)
- the form in which an individual can access their credit report (5.3.2)
- how advocates can access credit reports on behalf of an individual (5.3.3)
- the processes for recognising authorities how are acting on an individual's behalf (5.3.4)
- concerns that third parties are inappropriately accessing credit information (5.3.5).

[212] Privacy Act, ss 20R and 21T.

5.3.1 One access request to multiple reports

Under the Privacy Act, CPs may disclose credit information to any or all of the CRBs, depending on what they have notified the individual about.[213] This means that where an individual wants to access their credit report, they must reach out to each relevant CRB that the CP has disclosed information to. In practice, this could result in an individual having up to three credit reports.

The Review sought stakeholders view on whether individuals should be able to receive their credit reports by making just one access request to any of the CRBs.

Stakeholder views

Stakeholder submissions were divided on this proposal.

Consumer advocates favoured the inclusion of such a provision.[214] They recounted their experience of helping individuals go through three separate processes to access all of their credit reports, characterising it as both time consuming and sometimes administratively difficult.[215] They reported that the difficulty of the process could also be detrimental to their clients' personal wellbeing.

IDCARE was also supportive of the proposal to streamline access. Both IDCARE and consumer advocates noted that having one access request actioned by all three CRBs would align the access provisions to the existing credit ban provisions in paragraph 17 of the CR Code (where a ban request to one CRB is notified to, and applied by, the other CRBs).[216] IDCARE also observed that many CPs only tell individuals about the CRB that they have a relationship with and not the others; this complicates the journey for individuals seeking access to all of their credit information.[217]

Experian opposed the proposal, submitting that it would be impractical to achieve if CRBs are to meet their own identity verification processes.[218] ARCA agreed that such an initiative would be difficult to coordinate across the CRBs given their identity verification requirements. It argued that any coordination has the potential to hamper overall data security.[219]

ARCA offered an alternative solution– when an individual obtains a credit report with a particular CRB, that CRB could also include links to the relevant 'free credit report' websites with their CRB counterparts.[220] This would ensure that individuals are actively informed of their ability to obtain their credit information from all three CRBs, while allowing each CRB to undertake its own identity verification processes. IDCARE raised a similar suggestion when discussing the limited knowledge that individuals have of all three CRBs.[221]

---

[213] Privacy Act, s 21C.

[214] See consumer advocates joint submission, p 41; and Legal Aid Queensland, p 14.

[215] See consumer advocates joint submission, p 41.

[216] See IDCARE submission, p 4; and consumer advocates joint submission, p 42.

[217] See IDCARE submission, p 3.

[218] See Experian submission, p 13.

[219] See ARCA submission, p 32.

[220] Ibid.

[221] See IDCARE submission, p 3.

Review findings

The Review acknowledges the practical difficulties raised by consumer advocates in terms of accessing credit information from all three CRBs. However, the requirement to conduct identity verification is explicitly provided for in the CR Code, and it benefits both individuals and CRBs in terms of preventing fraud and mitigating privacy and security risks. These requirements make it impractical for an individual to make one request to all three CRBs while also ensuring that each CRB has met those requirements.

At the same time however, the Review considers that there is scope for improving individuals' awareness of other CRBs and simplifying how individuals can access credit reports from each of them. We consider there is merit to the alternative solution of requiring CRBs to provide information to individuals on how they can access their credit reports held by other CRBs.

Proposal 32 – Amend CR Code to require CRBs to provide information to individuals on how they can access their credit reports held by other CRBs

Amend paragraph 19 to specify that when an individual seeks access to their credit report from a CRB, the CRB must also provide the individual with information on how they can access their credit reports held by other CRBs.

5.3.2 Access to hard copy credit reports

As noted above, the Privacy Act requires CRBs and CPs to provide access to credit reporting information that they hold about an individual.

The Review was interested in stakeholders' experiences about how these credit reports were provided, and whether they were accessible for all members of the community.

Stakeholder views

Consumer advocates noted that accessing reports can be difficult for vulnerable individuals who do not have an email account or access to the Internet, and recommended that consumers be able to request access to alternative forms of their credit report, such as a physical copy.[222]

Review findings

The Review recognises the issue raised by consumer advocates that some individuals may have trouble accessing credit reports digitally.

The OAIC considers it to be good practice for entities to provide alternative methods of access to meet the needs of the individual, including through alternative formats.[223] Credit reports hold vital information about an individual and their ability to obtain credit in future. It is important that this information is accessible by all individuals.

[222] See consumer advocates joint submission, p 41; and Legal Aid Queensland, p 14.

[223] OAIC, 'Chapter 12: APP 12 – Access to personal information', [12.71].

While the Review heard that some CRBs already provide physical copies on request, we consider that it would be preferable for the CR Code to make this obligation clear to all CRBs.

Proposal 33 – Amend CR Code to specify that CRBs must provide physical copies of credit reports upon request

Amend paragraph 19 to specify that CRBs must provide individuals with physical copies of their credit reports on request.

5.3.3 Access charges

The Privacy Act allows an individual to access a copy of their credit report every 3 months, free of charge.[224] If an individual wishes to receive their credit report more regularly, the CRB must not charge an excessive fee. The Review sought feedback on concerns from stakeholders about this provision, including where they are acting as an access seeker on behalf of an individual.

Stakeholder views

IDCARE expressed concerns regarding the cost that it incurs to apply for a credit report on behalf of a victim of crime.[225] It submitted that the CR Code should exempt costs to charities acting on behalf of victims of crime or others requiring benevolent relief.

Experian also raised uncertainty around charging fees for access seeker requests where an entity is acting on behalf of individuals.[226]

Review findings

The Review identified two perspectives to access charges during the review. On the one hand, IDCARE noted that it was cost prohibitive to act on behalf of fraud and identity crime victims if it had to pay for the individuals' credit reports. On the other hand, Experian told us that it has an arrangement with IDCARE to provide access to credit information and in order to build and maintain this service, Experian charges a reasonable commercial fee for this access.

The Review notes that under s 20R of the Privacy Act and paragraph 19.4 of the CR Code access seekers acting on behalf an individual is entitled to receive the credit report for free every three months.

Therefore, the OAIC has taken the position that CRBs should not be charging access seekers in these circumstances. For access that is required on a more frequent or timely basis, the Review considers that IDCARE should raise its concerns about access charges directly with the CRBs, to determine if they can come to a mutually acceptable arrangement. The Review notes that the any charges that are made must not be excessive.[227]

---

[224] Privacy Act, s 20R(5).

[225] See IDCARE submission, p 8.

[226] See Experian submission, p 12.

[227] Privacy Act, s 20R(6).

OAIC Resolution of Practice Issue 4 – CRBs must provide access seekers with a copy of credit reports free of charge, once every 3 months

In accordance with the Privacy Act and the CR Code, CRBs must not charge an access seeker to access a credit report on behalf of an individual if that individual has not received a copy of their credit report in the last three months. For more frequent access, the CRB must not impose an excessive charge for the access seeker.

5.3.4 Recognition of standard authorities from individual's representatives

An important provision exists in the Privacy Act which allows an 'access seeker' to obtain credit reporting information on an individual's behalf, with their consent. This can be helpful when an individual does not know how to access their credit report, or where they require assistance from an advocate.

An access seeker in relation to credit reporting information or credit eligibility information is defined in s 6L of the Privacy Act as (a) the individual to whom the information relates, or (b) a person assisting the individual to deal with an CRB or CP who is authorised in writing to make an access request.

The Review sought stakeholder views on how this was operating in practice, particularly any processes around the recognition of standard authorities when acting as an access seeker, and issues with accessing credit reporting information on an individual's behalf during a credit ban.

Stakeholder views

Consumer advocates reported that financial counsellors and community lawyers have encountered difficulties with CRBs not recognising their authorities to act on behalf of clients, as well as difficulties accessing credit reports even when they have an authority in place.[228]

On the other hand, Experian raised a number of questions, including whether a CRB or the agent should have responsibility of verifying an agent's authorisation and the individual's consent.

Separately, IDCARE submitted that where a credit ban is in place, IDCARE has had difficulty in accessing the individual's information from a CRB via an access seeker arrangement.[229] This has meant that individuals have had to apply directly to CRBs. This makes it difficult for IDCARE to act on behalf of people affected by fraud or identity theft who do not have the capacity to perform their own access request.

Experian raised a question as to whether a CRB can continue to provide credit reporting information to such access seekers once a ban is in place.[230] Experian was supportive of entities that assist

[228] See consumer advocates joint submission, p 42.

[229] See IDCARE submission, p 3.

[230] See Experian submission, p 12.

individuals when fraud occurs but would like more guidance on the checks and balances for granting access requests made on the individuals' behalf.[231]

Review findings

The Review considers that the access seeker arrangements in the Privacy Act are critical to ensuring individuals are able to seek out support when they need it.

The Review notes that section 20K(2) of the Privacy Act provides an exception to the prohibition on use or disclosure of credit reporting information during a ban period, namely, where the individual expressly consents in writing to such a use or disclosure.

The Review acknowledges that CRBs have obligations regarding identity verification, including verifying the consent provided by individuals. However, the Review considers that it is important that individuals are still able to be supported by their advocates and that CRBs' processes facilitate this.

Therefore, in relation to recognising advocates, the OAIC has taken the position that:

- CRBs should have processes in place to recognise standard authorities from advocates to act on an individuals' behalf
- CRBs need to ensure that they appropriately recognise the written consent of individuals who have requested the support of an advocate during a ban period.

In both cases, advocates will need to ensure that they are appropriately obtaining that written consent from the individual and providing that to CRBs in the required form.

OAIC Resolution of Practice Issue 5 – CRBs should recognise standard authorities from advocates

CRBs and consumer advocates (such as financial counsellors, IDCARE etc) should put in place mutually acceptable arrangements that recognise consumer advocates' authority to act on behalf of individuals.

OAIC Resolution of Practice Issue 6 – CRBs must provide access to advocates during a ban period where consent provided

Section 20K allows CRBs to use and disclose credit information to an advocate acting on an individual's behalf during a ban period, where the individual has expressly consented to this in writing.

[231] See Experian submission, p 12.

5.3.5 Inappropriate access by third parties

The Privacy Act implements strict restrictions on who can access credit reporting information about an individual. This is in recognition that credit reporting information is a particularly significant kind of personal information.

The Review heard from stakeholders' that certain third parties had been asking individuals to provide access to their credit reporting information. This practice appears to circumvent the strict controls in place to prevent certain entities accessing credit reporting information.

The Review sought feedback on this issue.

Stakeholder views

Both consumer advocates and industry raised concerns about third parties accessing an individual's credit report in a way that undermines privacy and the intent of the credit reporting system.

Consumer advocates observed that there is currently a common problem where real estate agents or landlords request individuals to supply a copy of their credit report as part of their rental application.[232] They submitted that this is a common workaround of the rules which otherwise prevent them from accessing information within the credit reporting system.

Experian also reported that it is becoming increasingly aware of instances where individuals are 'consenting' to the disclosure of their credit information to entities who would not otherwise be entitled to access such information (including recruiters, employers and real estate agents assessing lease applications).[233] Experian questioned the validity of the consent provided in these instances and noted that this kind of access could have very serious implications for individuals with a poor credit history. It considered that more clarification or restriction is warranted, so that CRBs are not left to make a subjective determination on whether such uses are appropriate.

ARCA noted that it is difficult to see how such practices can be controlled, given that the individual has unrestricted access to their own credit information and can subsequently provide their credit report to anyone.

Consumer advocates recommended that the CR Code should impose stronger rules preventing real estate agents and landlords from asking individuals to supply a credit report to apply for rental accommodation.[234]

As an alternative, consumer advocates suggested that industry could work with consumer representatives towards a solution where individuals applying for a rental application could provide a 'simple' copy of their credit report which does not include RHI or financial hardship information.[235]

---

[232] See consumer advocates joint submission, p 42.

[233] See Experian submission, p 4.

[234] See consumer advocates joint submission, p 43.

[235] Ibid.

Review findings

While the previous issue in section 5.3.4 concerned consumer advocates having trouble helping individuals due to practical difficulties with accessing their credit information, here the issue is entities accessing credit information via the access seeker provisions when they are not permitted to.

As outlined above, the Privacy Act implements strict controls on what types of entities can gain access to credit reporting information. Sections 24 and 24A of the Privacy Act impose both a civil penalty offence and criminal offence on entities who obtain information from CRBs and CPs where they are not allowed to.

Relevantly, ss 24 and 24A do not impose those offences where the entity obtaining the information is an access seeker.

The definition of an access seeker in s 6L(1)(b) is very broad and encompasses any person (i) who is assisting the individual to deal with a CRB or CP; and (ii) who is authorised, in writing, by the individual to make a request in relation to the information under the relevant access seeker provisions. The Review understands that in practice there are many people who act as access seekers, to support an individual in dealing with a CRB or CP. However, it is important to understand who is explicitly excluded from being authorised as an access seeker under Part IIIA.

Under s 6L(b)(ii) an individual must not authorise a person to be their access seeker if they are prevented from accessing information under s 6G(5) or (6) of the Privacy Act. Relevantly, s 6G(5) specifically excludes real estate agents from the definition of a credit provider who can access credit information. An individual's employer and a general insurer are also excluded from this definition. This means that a real estate agent cannot be authorised to act as an individual's access seeker or receive credit information about them – even if they have consented to this.

However, the Review appreciates that there is nothing stopping individuals from providing their credit report to anyone once they have obtained it themselves. This highlights the power imbalance that exists between a real estate agent and an individual who is looking for a place to live, including that individuals may wish to demonstrate their positive credit history to real estate agents and landlords to enhance their rental application. The Review has significant concerns with this practice, and considers that it is contrary to the intentions of Part IIIA of the Privacy Act.[236] The Review also notes that in some circumstances real estate agents and employers may not be covered by the Privacy Act, which limits the ability for the OAIC to regulate this activity.

Given the implications of this practice, we consider that this issue is worthy of further consideration in the required independent review of Part IIIA. In the meantime, the Review considers that the OAIC should develop consumer guidance to explain the rights of individuals with respect to their credit reports. Further, if individuals, CRBs or CPs consider that entities are obtaining credit information contrary to ss 24 and 24A of the Privacy Act, complaints should be made to the OAIC.

[236] Australia's first credit reporting laws were enacted in 1990 and restricted certain existing practices, such as the provision of credit reports to real estate agents to check prospective tenants on the basis that it was an unacceptable invasion of privacy. See Australian Law Reform Commission, *For your information: Australian privacy law and practice*, ALRC Report No. 108, ALRC, 2008.

On the suggestion of developing a 'simple' credit report to be used in these circumstances, the Review does not consider it acceptable, or allowable under Part IIIA, for real estate agents and landlords to access a credit report, even under these circumstances.

Proposal 34 – OAIC to raise with the Attorney-General the issue of real estate agents, landlords and employers accessing credit reports

The OAIC will raise with the Attorney-General the current practice of real estate agents, landlords and employers accessing credit reports and whether amendments are required to further protect against this practice. The OAIC will write to the Attorney-General so that this issue can be considered in preparation for the review of Part IIIA.

Proposal 35 – OAIC to provide guidance to individuals on their rights with respect to supplying credit reports to landlords and real estate agents

The OAIC will develop guidance that explains to individuals that they do not need to supply their credit reports to landlords and real estate agents to support their rental applications, and that real estate agents are specifically excluded from the credit reporting framework in the Privacy Act.

OAIC Resolution of Practice Issue 7 – Real estate agencies and employers must not seek access to an individual's credit reporting information

The OAIC considers that Real estate agencies seeking access to individuals' credit reports is not intended under the Privacy Act. Real estate agencies should not ask individuals for a copy of their credit report or access their credit reporting information.

Further, CRBs must not provide this information to real estate agencies or employers through the access seeker provisions.

5.4 Correction rights

It is important that credit reporting information about an individual is accurate. Credit reporting is a significant kind of information which can have real consequences for individuals. As such, the Privacy Act provides that CRBs and CPs must take reasonable steps to correct information where it is inaccurate, out of date, incomplete, irrelevant or misleading.[237] The Privacy Act also provides a right to individuals to request that their personal information be corrected.[238] The Privacy Act sets out that correction requests must be actioned within 30 days.

Paragraph 20 of the CR Code addresses different operative requirements for CRBs and CPs in giving effect to correction requests.[239] The CR Code provides for a 'first responder' process, which sets out that where a CP is approached by an individual to correct their personal information, that CP becomes the 'first responder' and must take reasonable steps to provide consultation requests to other relevant CRBs and CPs.

The Review sought stakeholder views on how the correction rights provisions were operating in practice.

This section of the report presents findings in relation to:

- the level of complexity in the correction provisions (5.4.1)
- the processes for correcting multiple instances of incorrect information (5.4.2)
- a 'no wrong door' approach to correction requests (5.4.3)
- the adequacy of provisions that allow for corrections in circumstances that are beyond an individual's control (5.4.4)
- the timeframes for addressing correction requests (5.4.5).

5.4.1 Complexity of correction provisions

The CR Code contains a number of important obligations and requirements in relation to a CP or CRB actioning correction requests from an individual.[240]

The ability to request correction of credit reporting information where it is inaccurate, irrelevant, out of date or misleading is fundamental to a fair and fully functioning credit reporting system that adequately reflects a consumer's credit position.

The Review canvassed whether there were amendments that could be made to this paragraph of the CR Code to clarify these obligations and to ensure individuals are aware of how to use their correction rights.

[237] Privacy Act, ss 20S and 21U.

[238] Privacy Act, ss 20T and 21V.

[239] See ARCA submission, p 33.

[240] Paragraph 20 of the CR Code.

Stakeholder views

As an overarching comment, consumer advocates submitted that correction of information is one of the most important issues for individuals.[241] They considered that the current provisions in paragraph 20 are complex and confusing, which undermines the ability of individuals to advocate for themselves and pursue correction of credit-related personal information. They proposed that the provisions should be redrafted to be principles-based and in plain English.[242]

On the other hand, ARCA's view was that the correction provisions are appropriate.[243] They reasoned that the provisions are not intended to exhaustively map the correction process, but rather to ensure the operational efficacy of that process for regulated entities. ARCA considered that if the provisions are considered too complex, appropriate guidance material could be developed external to the CR Code.[244]

Experian thought that the correction provisions should be clarified to expressly enable the efficient exchange of information between CRBs and CPs for this purpose.[245] As an example, it noted that contact information such as phone and email are necessary to support a correction request but are not expressly permitted in the CR Code to be collected by a CRB.

Review findings

The disagreement between consumer advocates and ARCA about paragraph 20 specifically – in terms of its complexity and appropriateness – also captures the difference of opinion about the CR Code more broadly, as discussed above in **Error! Reference source not found.** and 2.1.

We reiterate that a central object of the CR Code is to set out how regulated entities are to apply or comply with specific provisions of Part IIIA. This necessarily has an operational focus regarding industry compliance.

The Review considers that the current specificity of paragraph 20 is required to ensure consistent application across regulated entities. However, the Review acknowledges concerns raised by consumer advocates. The Review considers it appropriate that the OAIC develop additional guidance to support individuals in understanding their rights and how the corrections process works from the perspective of individuals.

Proposal 36 – OAIC to provide guidance to individuals on their correction rights and how to exercise them

The OAIC will develop targeted guidance pieces for individuals to explain the correction process and how individuals and their advocates can exercise their correction rights.

[241] See consumer advocates joint submission, p 43.

[242] Ibid.

[243] See ARCA submission, p 32.

[244] See ARCA submission, p 33.

[245] See Experian submission, p 14.

On the issue of whether CRBs and CPs can share an individual's contact information for the purpose of allowing a CRB or CP to action a correction request, the OAIC considers that CRBs and CPs are permitted to disclose personal information for this purpose.

OAIC Resolution of Practice Issue 8 – CRBs and CPs can share contact information for the purposes of actioning a correction request

When taking steps to action and resolve a correction request, CRBs and CPs are allowed to share contact information that relates to the individual including for example, phone number and email address

5.4.2 Multiple instances of incorrect information

The Review called for views on whether the approach to corrections could be simplified in cases where there are multiple instances of incorrect information, such as those that arise in cases of economic abuse or fraud. The current arrangements mean that an individual has to go through a separate correction process for each incorrect item listed on their credit report during the relevant period.

Stakeholder views

Stakeholder submissions were unanimously in favour of simplifying the approach to corrections where there are multiple instances of incorrect information.

Consumer advocates raised this proposal in several contexts, including protections for victims of fraud,[246] feedback on correction provisions in general,[247] and supporting people affected by domestic abuse.[248] They noted that it can be extremely difficult and even re-traumatising for a victim of economic abuse or fraud to try to remove many credit enquiries relating to different CPs from their report.[249] They considered that there should be a clear process whereby the relevant facts can be established once and the onus is then on a CRB to liaise with CPs and remove inaccurate or incorrect listings from the credit report.[250]

IDCARE provided insights on its practical experience in helping victims of crime deal with incorrect information as a result of unauthorised credit enquiries.[251] They observed that in some cases this has totalled more than 20 CPs. IDCARE argued that victims of crime are not equipped to handle these situations, often because they are not aware which CPs might have been approached. Instead, CRBs are better placed to address multiple corrections because of their knowledge and relationship with CPs.[252]

---

[246] See consumer advocates joint submission, p 38.

[247] See consumer advocates joint submission, p 44.

[248] See consumer advocates joint submission, p 48.

[249] See consumer advocates joint submission, p 38.

[250] See consumer advocates joint submission, p 50.

[251] See IDCARE submission, p 9.

[252] Ibid.

Legal Aid Queensland, Communications Alliance and the TIO were all generally supportive of simplifying the process of correcting multiple instances of incorrect information.[253]

ARCA submitted that its members appreciate the issue of multiple instances of incorrect information identified in the Consultation Paper.[254] ARCA members were supportive of simplifying the correction process, provided that there are practical ways to ensure that fraudulent entries are differentiated from legitimate entries in a credit report when removing incorrect information.

Review findings

Correction rights are fundamental to ensuring an accurate credit reporting system in Australia. Enabling multiple correction of instances of incorrect information through a single correction process addresses a current gap in the credit reporting system. Further, this change has support across both consumer and industry representatives and is in line with the overall intention of the correction provisions in Part IIIA. Amending the CR Code would go some way to clarifying this and improving the correction process for individuals, particularly where they are vulnerable or do not know who to engage to seek correction of their personal information.

The Review considers that CRBs are best placed to coordinate the correction of multiple instances of incorrect information. Both consumer advocates and CRBs however, should be consulted when determining amendments to the CR Code.

Proposal 37 – Amend CR Code to introduce a mechanism to correct multiple instances of incorrect information stemming from one event

Amend paragraph 20 to enable correction of multiple instances of incorrect information.

The code developer should consult with CPs/CRBs and consumer advocates to determine the best approach.

5.4.3 'No wrong door' correction

A related issue is whether individuals can have their correction request readily dealt with regardless of whether they approach the CP or CRB – that is that they will not be unnecessarily bounced between entities. This is essentially a 'no wrong door' approach whereby it does not matter who the individual approaches in the first instance.

Section 23C of the Privacy Act outlines that where there is a complaint about correction of personal information, the CP or CRB that the individual first approached (the respondent) to the complaint must notify other CRBs or CPs relevant to the complaint, or that also holds the information. These are sometimes referred to as the 'first responder' provisions.

Stakeholder views

Consumer advocates strongly supported a 'no wrong door' approach to corrections. They noted that since both CRBs and CPs have correction obligations under Part IIIA, this often results in a CRB or CP

[253] See Legal Aid Queensland submission, p 14; Communications Alliance submission, p 7; TIO submission, p 5.

[254] See ARCA submission, p 33.

referring an individual to another CRB or CP rather than completing the correction request itself.[255] They also identified situations where an individual may have no knowledge of which CPs were involved, such as instances of fraud or financial abuse, and when the account has been sold to a debt collector.

EWON made similar points in support of a 'no wrong door' approach. It reported that in its experience individuals can feel bounced around between CPs and CRBs, and it highlighted two case studies where there has been a transfer of rights and it is unclear whether the individual needs to deal with the original or acquiring CP.[256]

ARCA submitted that the first responder provisions which underpin the correction obligations in the Privacy Act are already intended to ensure there is a 'no wrong door' approach to corrections. Therefore, they submitted that a CRBs or CPs unwillingness to process a correction request may be a compliance issue rather than an issue with the CR Code.

Review findings

The Review acknowledges consumer advocates' and EWON's submissions that individuals are encountering difficulties with having their correction request dealt with. Given the 'first responder' provisions are intended to act as a 'no wrong door' approach, we consider that this is a practice issue among CRBs and CPs, rather than a CR Code drafting issue.

To redress this current practice, the Review considers that education and awareness materials should be developed for industry regarding how the 'no wrong door' approach is supposed to work and for individuals on how they can exercise their correction rights. The guidance for individuals will be related to that developed under Proposal 36 and 5.4.1 above.

Furthermore, the Review suggests that this area should be a future focus of upcoming CRB audit reports required under paragraph 24.3 of the CR Code. The outcome of these reports will give more transparency around current industry practices, and might inform future OAIC regulatory activity.

Proposal 38 – OAIC to provide guidance to industry on the 'no wrong door' approach to corrections and will consider the need for future compliance activity

The OAIC will develop guidance for industry explaining expectations of the operation of the 'no wrong door' approach to correction requests. Following the development of this guidance, the OAIC will consider whether further compliance activity into how CRBs and CPs are responding to correction requests in accordance with its Privacy Regulatory Action Policy.[257]

The OAIC will also expect CRBs to include this issue in the scope of their future audit reports required under paragraph 24.3 of the CR Code.

[255] See consumer advocates joint submission, p 44.

[256] See EWON submission, p 6.

[257] See Privacy regulatory action policy, OAIC, 2018, accessed 24 May 2022.

5.4.4 Circumstances beyond individual's control

The CR Code requires the destruction of default information in cases where an overdue payment occurred because of circumstances beyond the individual's control.[258] However, this can only occur where the individual has entered into a new arrangement and the overdue payment relates to that arrangement, or if a CP has disclosed payment information about that individual. Currently the CR Code gives three examples of circumstances beyond an individual's control, including: natural disasters, bank errors in processing a direct debit, or fraud.[259]

The Review sought feedback on whether this list should be expanded to specifically reference domestic abuse.

Stakeholder views

All stakeholders were unanimously in favour of expanding the list of unavoidable circumstances in paragraph 20.5 to include domestic abuse.[260] See section 5.6 below for further consideration of issues proposed by stakeholders as a way of protecting individuals affected by domestic abuse.

Some stakeholders proposed further enhancements to paragraph 20.5 for domestic abuse specifically, and unavoidable circumstances more generally.

Correction to be made by either CRB or CP

ARCA submitted that there is merit in reviewing the requirement in paragraph 20.5 that the correction request is made only to the CRB, in consultation with the CP.[261] ARCA considered that it may be appropriate for either the CP or CRB to make the correction where they receive a request, depending on who holds the information. EWON also suggested that CPs should be obligated to action correction requests.[262]

Flexibility to not list or remove certain types of information

Consumer advocates and the TIO submitted that the most important issue when supporting victims of abuse is the need for CPs to have greater flexibility to not list, or to remove, missed payment information from credit reports.[263] They proposed that the CR Code should clarify that CPs can suppress or correct any past credit reporting information. ARCA also supported enabling the removal of information beyond just default information, to include RHI and CCLI in domestic abuse situations.[264]

---

[258] Paragraph 20.5 of the CR Code.

[259] Paragraph 20.5(a)(iii) of the CR Code.

[260] See ARCA submission, p 34; consumer advocates joint submission, p 44; TIO submission, p 8; EWON submission, p 5.

[261] See ARCA submission, p 34.

[262] See EWON submission, p 6.

[263] See consumer advocates joint submission, p 49.

[264] See ARCA submission, p 35.

ARCA observed that whether or not a CP is compelled to report particular information, however, is outside the scope of Part IIIA and the CR Code.[265] These reporting requirements are addressed by the PRDE and for eligible licensees, the mandatory CCR framework.

Review findings

Paragraph 20.5 provides a non-exhaustive list of examples of unavoidable circumstances. Listing domestic abuse as a specific example and expanding correction rights for individuals would unambiguously affirm the importance of addressing this issue and ensure that the credit reporting system keeps pace with broader industry developments in protecting vulnerable people. The Review therefore considers that amending the CR Code is warranted. The Review notes the importance of maintaining the non-exhaustive nature of the list of examples in paragraph 20.5. This will go some way to providing flexibility for CPs to consider the circumstances of each individual request.

Furthermore, expanding paragraph 20.5 beyond correcting default information would be in line with ss 20S and 21U of the Privacy Act, which contemplate the correction of credit reporting information and credit eligibility information in cases where the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

As to the issue of making a correction request to a CP, the Review considers that there is benefit in amending the CR Code to allow for this. This is to acknowledge that either a CP or a CRB can hold the relevant information about the individual that requires correction.

Proposal 39 – Amend CR Code to include domestic abuse as an example of circumstances beyond the individual's control

Amend paragraph 20.5 to add domestic abuse as a specific example of circumstances beyond the individual's control.

The amended paragraph should maintain the non-exhaustive nature of the list of circumstances beyond an individual's control.

Proposal 40 – Amend CR Code to extend correction requests to include CPs

Amend paragraph 20.5 to so that the correction request can be made to either the CP or CRB.

Proposal 41 – Amend CR Code to expand the categories of information that can be corrected

Amend paragraph 20.5 to expand the categories of information that can be corrected beyond just that of default information.

[265] See ARCA submission, p 36.

5.4.5 Correction timeframes

Under Part IIIA, a CRB or CP must process a correction request within 30 days of the request, unless the individual agrees to a longer period in writing.[266]

The Review sought feedback from stakeholders on how these correction timeframes were operating in practice.

Stakeholder views

Consumer advocates submitted that the correction timeframes are weak and that in many cases the 30 day period is not reasonable and results in a detriment to the individual (such as where the individual is seeking approval for a new line of credit in order to purchase a house or vehicle and the deadline passes).[267] They recommended that the CR Code set much tighter timeframes for 'simple' correction requests and to make clear that the 30-day timeframe in the Privacy Act is a maximum time period that accommodates more complex correction requests.

The Review followed up with consumer advocates and they gave the following examples of 'simple' correction requests:

- when the prima facie evidence provided to the CRB shows the default belongs to a different person and was listed in error
- when the lender and consumer have already come to an agreement in writing that the credit reporting information needs to be changed/updated/erased
- when a client has evidence of a prior listing for the same debt
- when the listing has been made by a company with no power to list
- when the debt has become statute barred
- where the person produces a 'commonwealth victims' certificate' as evidence that the listing is fraudulent.

ARCA noted that the CR Code currently provides for corrections to be made in a shorter timeframe.[268] Paragraph 20.4 provides that when a CRB or CP receives a correction request, they must determine whether the information needs to be corrected 'as soon as practicable'. Once this has been determined, they must correct the information within five business days.

Review findings

The Review acknowledges that the Privacy Act provides a period of 30 days for addressing correction requests. It is important to recognise that this period is intended to cover all types of correction requests, including those that are more complicated or require consultation. With this in mind, where

[266] Privacy Act, ss 20T and 21V.

[267] See consumer advocates joint submission, p 44.

[268] See ARCA submission, p 34.

correction requests are relatively straightforward it is expected that the correction request would ordinarily be considered and resolved well within the 30 days.[269]

Furthermore, the CR Code requires CPs and CRBs to determine whether information needs to be corrected as soon as practicable.[270] It is important for CPs and CRBs to individually assess correction requests, and ensure they are processed according to their level of complexity.

Therefore, on this issue, the OAIC has taken the position that CRBs and CPs should take whatever reasonable steps are required to resolve correction requests in a timely manner. In doing so, CRBs and CPs should be mindful that the 30 day period within the Privacy Act sets out a maximum period for correction, and is not intended to be a minimum period. The Review notes that this accords with the intention of these provisions set out in the Explanatory Memorandum.

OAIC Resolution of Practice Issue 9 – CRBs and CPs should actively resolve correction requests as soon as practicable

The 30 day correction timeframe in the Privacy Act is a maximum period, and should not be interpreted by CRBs and CPs as the standard timeframe for processing correction requests.

The intention of the correction timeframes is to ensure timely correction. The OAIC expects CRBs and CPs to demonstrate they have taken the necessary steps to efficiently address each correction request based on the issues at hand.

5.5 Complaint handling and dispute resolution

Individuals have a right to complain about acts or practices that may be a breach of Part IIIA or the CR Code. Individuals can complain directly to a CRB or CP, to a recognised EDR Scheme, or to the Commissioner.

The Privacy Act contains prescriptive requirements for the complaint handling processes of CRBs and CPs. Consistent with other entities bound by the Privacy Act, CRBs and CPs are required to implement practices, procedures or systems to enable them to deal with privacy-related enquiries or complaints.[271] Under Part IIIA, a complaint must be acknowledged within 7 days and a decision made about the complaint within 30 days.[272]

The usual complaint handling scheme for credit-related privacy complaints is modified by Part IIIA for CRBs and CPs where the complaint relates to an individual's request for access to, or correction of, their credit-related information. If an individual makes an access or correction request and the request is refused, the Privacy Act does not require the individual to then make a privacy complaint to the CRB or CP. Rather, they may (a) complain directly to the recognised EDR scheme of which the CRB or CP is a member, or (b) complain directly to the Commissioner.[273]

---

[269] Explanatory Memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 150.

[270] Paragraph 20.4 of the CR Code.

[271] Privacy Act, ss 20B(2) and 21B(2).

[272] Privacy Act, s 23B.

[273] Privacy Act, s 40(1B).

The CR Code contains additional requirements for complaints in paragraph 21, which:

- bind CRBs and CPs, which are not already bound by other industry complaint handling requirements, to comply with ISO 10002:2018(E), an international standard containing guidelines for complaints handling
- require a CRB to be a member of a recognised external dispute resolution (EDR) scheme[274]
- require a CRB or CP that is consulted by another CRB or CP about a complaint to respond as soon as practicable
- explain the steps a CRB or CP should take if it believes it will not be able to resolve the complaint within the 30-day period
- outline notice requirements for a CRB or CP to notify other relevant entities of a complaint.

The Review sought stakeholder feedback regarding the provisions regulating complaint handling and dispute resolution.

This section of the report presents findings in relation to the current operation of the complaint provisions.

Stakeholder views

Early views shared by consumer advocates indicated that, while ostensibly designed to make privacy complaints in relation to credit-related information easier for individuals, the combined requirements of Part IIIA and general obligations under the Privacy Act (which are then encapsulated in the CR Code) may be an obstacle to individuals engaging with the complaint process.

In their written submission, consumer advocates observed that in their experience, CRB complaint handling teams are understaffed and lack appropriate training and expertise, and there is little incentive for CRBs to invest in complaint handling.[275] A similar point was made by IDCARE during roundtable discussions. Also in roundtable discussions, Legal Aid Queensland suggested that the CR Code be amended to set out what consumers can expect when entering the complaints process, noting the current drafting appears to primarily address how CPs and CRBs deal with each other, rather than with the individual.

Several industry stakeholders raised issues with the operation of complaints and EDR processes. FBAA drew attention to the challenges facing CPs when dealing with complaints relating to credit enquiries. Even where the CP's actions are correct and justified, the complainant may nevertheless take the matter to EDR and cause great expense for the CP.[276] AFIA noted that CPs have borne escalating costs due to credit repair firms, and to a lesser extent AFCA decisions, that challenge

[274] CPs must also be part of a recognised EDR scheme, such as the Australian Financial Complaints Authority (AFCA), to enable disclosure of credit-related personal information to CRBs – see Privacy Act, s 21D.

[275] See consumer advocates joint submission, p 45.

[276] See FBAA submission, p 5.

default listings even though they are made accurately and in accordance with the credit reporting framework.[277]

Experian raised concerns about the cost incurred by CPs and CRBs in respect of AFCA claims, even when they are resolved in favour of the CP or CRB.[278] It suggested a process for consumer advocates initiating bulk claims to obtain a preliminary AFCA view of the underlying issue, to reduce these types of claims and the cost and time involved in their resolution.

Review findings

Stakeholder submissions to the Review identified various problems encountered by both consumer and industry representatives when it came to dealing with complaints and the EDR process.

In relation to Legal Aid Queensland's observation about the complaint handling provisions being more tailored to CPs and CRBs rather than individuals, this is a point that was also raised about the correction provisions specifically (see 5.4.1) and the CR Code more generally (see **Error! Reference source not found.**). As noted above, the Review considers this necessary to achieve the CR Code's purpose of providing entities with further particularity about how to comply with their obligations. However, the Review considers that tailored guidance for individuals on how they can exercise their rights may be an appropriate mechanism to address this issue.

The Review does not consider that amendments to the CR Code could resolve the issues identified in stakeholder submissions. These include the resourcing of complaint handling teams within CPs and CRBs, the actions of the credit repair firms, and the way AFCA makes decisions and allocates costs. However, the Review considers that each of the issues raised could potentially be addressed by changes to industry practices. For example, if CRBs and CPs invested more resources in their complaint handling teams, this might go some way to reducing the number of complaints that are taken to AFCA or other external EDR schemes, thus minimising the costs incurred by CPs or CRBs in relation to actions taken by credit repair firms.

However, it was repeatedly raised by stakeholders that individuals are not aware of their complaint rights and how to exercise them. For this reason, the Review proposes that the OAIC produce guidance aimed at individuals with this purpose in mind.

Proposal 42 – OAIC to provide guidance for individuals on the complaints process and who to approach to make a complaint

The OAIC will develop targeted guidance for individuals which outlines the complaints process relevant to credit reporting, including CP and CRB obligations in acknowledging and responding to complaints.

[277] See AFIA submission, p 6.

[278] See Experian submission, p 14.

5.6 Protecting individuals affected by domestic abuse

The UN describes domestic abuse, also called 'domestic violence', as a pattern of behaviour in any relationship that is used to gain or maintain power and control over an intimate partner. It is behaviour that intimidates, manipulates, or humiliates a person, or is otherwise used to gain or maintain power or control over another person. It may be characterised by coercive control and financial (economic) abuse, among other types of abuse.

This Review acknowledges the importance, and complexity, of supporting individuals affected by domestic abuse and helping them resolve their financial affairs.

The Review sought stakeholder views on issues in the credit reporting context that are exacerbated by domestic abuse, as well as options to better support victims.

This section of the report presents findings in relation to:

- current work being undertaken in the domestic abuse space (5.6.1)
- whether individual or customer-based reporting (as opposed to account-based reporting) might address some issues experienced by domestic abuse victims (5.6.2).

5.6.1 Ongoing work

From a public policy perspective, domestic abuse in Australia is a matter of considerable concern to the community and there are a number of public policy initiatives aimed at addressing domestic abuse. For example, in June 2021, the Meeting of Attorneys-General agreed to co-design national principles to develop a common understanding of coercive control and matters to be considered in relation to potential criminalisation.[279]

Stakeholder views

Improving the capacity of the CR Code to address matters of domestic abuse was unanimously welcomed by stakeholders. Some stakeholder suggestions that reference domestic abuse in the context of improving existing CR Code provisions – for example, the application of paragraph 20.5 – are discussed elsewhere in this report (see 5.4.4 above).

In its submission, ARCA provided detailed commentary about its broader body of work in relation to credit reporting and domestic abuse, and confirmed its intention to continue pursuing this work over the coming months.[280] ARCA also outlined a variety of activities that are at various stages of completion, including proposals for industry developed guidelines and suggested amendments to the CR Code and Part IIIA.

[279] See Attorney-General's Department, *Development of national principles on addressing coercive control: terms of reference*, Meeting of Attorneys-General, 1 July 2021.

[280] See ARCA information materials supplied during consultation, Domestic abuse: background paper and Domestic abuse & the credit reporting system: summary and outcome of works undertaken by ARCA to date.

Review findings

The Review acknowledges that it is important for Australia's credit reporting framework to be fit for purpose and to be capable of addressing the difficult circumstances of those experiencing, or who have experienced, domestic abuse.

The Review also recognises that domestic abuse is an important area of public policy in Australia and cuts across a range of matters including but not limited to safety, privacy and protection of personal information, individual autonomy in decision-making and physical, emotional and financial security. Contextually, it cannot be dealt with in a vacuum and any changes to Australia's credit reporting framework need to be considered holistically as part of this larger policy question.

The Review considers that, in the meantime, ARCA's ongoing work to understand and address this issue should continue. The Review also considers that ARCA's work in this space is a good example of the positive impacts that early stakeholder engagement can have on the effective operation of the CR Code.

5.6.2 Account-based vs customer-based reporting

The credit reporting system currently takes an account-based approach, also known as 'joint accounting'. This means that information is reported against a particular account, rather than separately for each individual that is signed up to that account. This Review canvassed whether customer-based reporting, also known as 'individual' reporting, would be more supportive of individuals impacted by domestic abuse, for example, those who were coerced into signing lending documents.

Stakeholder views

Consumer advocates were strongly in favour of customer-based reporting, arguing that this is the optimal way to meet both privacy and safety objectives for at risk borrowers.[281] They suggested an alternative could be for the CR Code to allow the information of joint accounts to be split in discrete economic abuse situations where the CP and the individual agree this is the best option.[282]

Industry stakeholders argued against a general move towards customer-based reporting, citing data accuracy and cost concerns, but otherwise supported shifting to such an approach on a case-by-case basis.[283] ARCA and Experian noted that the Data Standards already support the ability to 'split' an account, so that different information may be disclosed for each account holder.

Review findings

The Review finds that stakeholders have a similar position on this issue, namely, that the credit reporting system should provide an option for customer-based reporting in cases of domestic abuse.

[281] See consumer advocates joint submission, p 52.

[282] Ibid.

[283] See ARCA submission, p 36; Experian submission, p 15; ABA submission, p 7.

The Review acknowledges that under the Data Standards there already exists a mechanism to split accounts so that different information may be disclosed for different account holders.[284]

The Review considers it important for industry stakeholders to share information with individuals and their advocates so that they are aware of their options when experiencing domestic abuse. Furthermore, it is also important that CPs and CRBs facilitate the exercise of those options.

OAIC Resolution of Practice Issue 10 – CPs and CRBs should make individuals aware of their options, such as where customer-based reporting may be available, when experiencing domestic abuse

The OAIC considers that CPs and CRBs should ensure individuals are aware of their options when experiencing domestic abuse and facilitate the exercise of those options.

For example, this may include CPs providing customer-based reporting instead of account-based reporting as an option to assist an individual to remain safe from their perpetrator, or to recover from their abuse. CRBs should also consider means to protect contact information for individuals experiencing domestic abuse where they seek to obtain a copy of their credit report.

[284] See ARCA submission, p 36.

Part 6: Permitted activities of CRBs and CPs

The Privacy Act limits who can collect credit-related personal information, and what they can do with that information.[285]

The Review was interested in hearing stakeholders' views and experiences on whether the provisions regulating permitted activities of CRBs and CPs were operating as intended. In particular, the Consultation Paper sought stakeholders' views, experiences and suggestions regarding the following:

- whether the provisions for recording 'information requests' were fit for purpose (6.1)
- whether the provisions regulating the used and disclosure of credit related personal information by CPs and Affected Information Recipients were operating as intended (6.2)
- whether the direct marketing provisions were operating effectively (6.3)
- whether any amendments were required to provisions permitting use of credit information in circumstances where another organisation has acquired the rights of the original CP (6.4).

6.1 Information requests

Under the Privacy Act, when a CP requests information from a CRB about an individual this request can be recorded by the CRB and forms part of the individual's credit information. The Privacy Act refers to this type of information as an 'information request'. This is more commonly known as a 'credit enquiry'. Paragraph 7 of the CR Code provides further particularisation of the collection, use and disclosure of information requests.

Current practice is for these credit enquiries to be recorded on an individual's credit report and to generally contain information such as when an application for credit has been made, the date of the application, the type of credit and the amount the individual applied for. Stakeholders raised concerns that this could negatively impact how prospective CPs will assess the individual for the provision of credit – for example, they might consider that the individual is trying to get multiple loans or buy too many things using credit. Individuals also are generally unaware of the impact these credit enquiries might have on their credit report.

The Review sought feedback from stakeholders about how information requests were operating in practice, and whether a 'soft enquiries' framework might have benefits in the Australian credit reporting framework.

6.1.1 Impact of information requests and 'soft enquiries'

Stakeholders advised that there has been an increase in complaints regarding information requests, or credit enquiries, that are recorded on an individual's credit report. In many cases, CPs are asked to remove enquiries even when they were legitimately recorded. This is in part caused by individuals

[285] Privacy Act, s 6G and Part IIIA Division 2, 3 and 4.

being concerned that these information requests have a negative impact on their overall creditworthiness.

The Review canvassed whether and how the CR Code could be amended to address this issue, including the feasibility of introducing a 'soft enquiries' framework. There are different definitions of 'soft' and 'hard' enquiries, but generally speaking:

- a 'soft' enquiry is one that is not recorded on the individual's credit report, such as where an individual is only seeking a quote, or to understand if they qualify for a certain product or offer
- a 'hard' credit enquiry is one that is recorded on the individual's credit report and takes place once an individual has submitted an application for credit, to allow the credit provider to determine the individual's creditworthiness.

Currently, Australia's credit reporting framework does not differentiate between a hard and soft enquiry. Current industry practice is that all credit enquiries are generally recorded on an individual's credit report regardless of their purpose.

Stakeholder views

ARCA observed that since the previous CR Code review, credit enquiry disputes have increased and become a significant feature of overall credit reporting disputes.[286] They noted that the disputes tend to be lodged by paid representatives (such as credit repair agents) and tend to treat the presence of a credit enquiry on a credit report as having a 'negative' impact or having equivalence to the presence of default information. ARCA clarified that credit enquiries generally have a minimal impact on an individual's credit score and are not equivalent to default information in terms of potential negative impact. ARCA supported the ideas of a 'soft enquiries' framework to resolve this issue, and thought it should be progressed expediently, preferably through an amendment to the CR Code, if possible.[287] ARCA noted that the use of soft enquiries is well-established in a number of overseas jurisdictions, including the UK and New Zealand.[288] Consumer advocates also submitted that individuals are very concerned about credit enquiries, and considered that the current system results in individuals being penalised for 'shopping around' for the best deal.[289]

FBAA submitted that the differentiator between whether an enquiry is recorded should depend on whether the individual has applied to a particular CP with an intention to obtain finance, and not where they are approaching multiple CPs to shop around for competitive rates.[290]

Experian considered that introducing soft enquiries would increase competition among CPs and result in better outcomes for individuals.[291] It also argued that such a provision would alleviate the concerns regarding potential misuse of the access seeker provisions by CPs and would ensure the Privacy Act is more aligned with the objectives of the Consumer Data Right in terms of empowering individuals to benefit from their own information. Experian also considered that further guidance or

[286] See ARCA submission, p 37.

[287] See ARCA submission, p 32.

[288] See ARCA submission, p 30.

[289] See consumer advocates joint submission, p 37; Legal Aid Queensland submission, p 12.

[290] See FBAA submission, p 3.

[291] See Experian submission, p 13.

processes could be provided around when a 'soft' enquiry versus a 'hard' enquiry should be recorded by a CRB. This might help alleviate this issue.[292]

Separately consumer advocates noted that there needs to be a lot more information from industry about how enquiry information is viewed and scored in a lending decision process.[293] They stated that if individuals knew that credit enquiries do not cause a lot of harm, then there would not be as many disputes.[294]

ARCA agreed with this point and considered that there should be improved consumer education and awareness of credit enquiries so that individuals appreciate that multiple enquiries are not necessarily 'negative'.[295]

TIO similarly recommended that individuals should be better informed of how credit enquiries and credit scores work.[296] It recommended giving individuals the ability to request the removal of credit enquiries, where incorrect advice was provided about the impact of the enquiry, or they were not properly notified that a CP would disclose the information to the CRB.[297]

The Communications Alliance submitted that its members also receive complaints about this issue.[298] It highlighted that the approach taken by credit repair agencies may exacerbate the issue as they take a 'scattergun' approach to having credit information removed from their client's file. The Communications Alliance suggested that the issue could be addressed through CR Code clarification, guidance and educational activities aimed at individuals, other access seekers and CPs.[299]

Other stakeholders including FBAA, EWON and Experian all submitted that concerns about credit enquiries appearing on credit reports have led to complaints and requests for their removal.[300] FBAA suggested consideration of how enquiries impact credit scores and whether this could be changed.[301] EWON supported changes to provide clarity and guidance for CRBs and CPs around the treatment of credit enquiries and their impact on credit scores.[302] Experian suggested that individuals should be educated about what a credit enquiry is, when they can be made, who can see it and what impact it has on their credit score and/or subsequent applications for credit.[303]

---

[292] Ibid.

[293] See consumer advocates joint submission, p 37.

[294] Ibid.

[295] See ARCA submission, p 39.

[296] See TIO submission, p 3.

[297] See TIO submission, p 3.

[298] See Communications Alliance submission, p 5.

[299] See Communications Alliance submission, p 6.

[300] See EWON submission, p 7; FBAA submission, p 6; Experian submission, p 15.

[301] See FBAA submission, p 6.

[302] See EWON submission, p 8.

[303] See Experian submission, p 15.

Review findings

The Review acknowledges the concerns raised by stakeholders and considers that a way of addressing these concerns would be the introduction of a 'soft enquiries' framework within the CR Code. There are clear benefits to the introduction of such a framework. These include:

- allowing individuals to have more choice, and seek tailored offerings
- ensuring individuals are not penalised (either in reality or perception) for shopping around
- promoting competition between CPs knowing that individuals can easily approach other CPs to seek the best rate available to them
- bringing the Australian credit reporting system in line with its international counterparts
- ensuring consistency across industry on how and when credit enquiries are recorded on credit reports.

The introduction of a 'soft enquiries' framework has the support of all stakeholders. Furthermore, such a framework is likely to result in a decrease in complaints from individuals (and credit repair agencies) as 'soft enquiries' will not be recorded on their credit report.

The Review considers that the CR Code is able to particularise a soft enquiries framework, in keeping with the intention of Part IIIA. This is because the Privacy Act only requires CRBs to make a written note of disclosure when it discloses information to a CP.[304] The Privacy Act does not require this written note to be made on an individuals' credit report. As such, the Review considers that the CR Code can introduce a 'soft' enquiry framework by particularising that 'soft enquiries' should not be recorded by CRBs on an individual's credit report. When developing this variation, it will be important to accurately define the circumstances that would amount to a 'soft enquiry'.

As to the stakeholder comments about the need for education around the impact of credit enquiries, the Review considers that these issues will likely be resolved by the introduction of the 'soft enquiry' framework proposed above. Notwithstanding this, the Review considers that as an interim step, it would be helpful for industry to provide underlying data about the impact that credit enquiries generally have on an individual's credit score, and how CPs consider this information when making a lending decision. The Review considers that CRBs and CPs are best placed to develop these resources and to communicate with individuals about the impact that credit enquiries have on their credit information.

Proposal 43 – Amend CR Code to introduce soft enquiries framework

Amend paragraph 7 to define soft enquiries and to require that the written note of a soft enquiry must be on a record related to an individual, but not included on the individual's credit report.

Alongside this, industry should take steps to inform individuals about the impact credit enquiries have on their overall credit report and how this is considered in lending decisions.

[304] For example, if credit information is disclosed under s 21D of the Privacy Act, s 21D(6) states that the CP must make a written note of that disclosure.

6.2 Use and disclosure of credit-related personal information by CPs and Affected Information Recipients

Part IIIA permits a CRB to disclose credit reporting information to certain third party entities, but only for certain permitted purposes.[305]

Part IIIA also places restrictions and conditions on how CPs and affected information recipients (AIRs) use and disclose credit information and credit eligibility information.[306] An AIR means a third party and can include a mortgage insurer, trade insurer or credit manager.[307] Paragraphs 5.1, 14 and 16 of the CR Code contain some additional requirements.

The Review sought feedback regarding the provisions regulating use and disclosure of credit information to AIRs.

Stakeholder views

There were very few stakeholder submissions on this topic. ARCA raised the following issues:[308]

Individuals acting in trustee capacity

ARCA identified that the increased participation in comprehensive credit reporting has resulted in an issue in the reporting of trustee information. It noted that it is possible for an individual to enter into consumer credit in their capacity as a trustee for a trust, but currently there is no means to identify them as a trustee. ARCA considered that the definition of 'capacity information' in paragraph 1.2(c) of the CR Code could be amended to include an individual in their capacity as a trustee.

CP disclosures of credit eligibility information

ARCA queried whether it was possible for a CP to disclose credit eligibility information directly to a broker under s 21G(3)(c)(i) of the Privacy Act. ARCA considered that the broader interpretation of the words *'a person for the purpose of processing an application for credit made to the credit provider'* could allow a disclosure direct from CP to broker, and could potentially be clarified in the CR Code.

Consideration of additional uses and disclosures

ARCA identified some additional uses and disclosures of credit reporting information that may be a matter for reform of Part IIIA. These include enabling CRBs to disclose credit reporting information (including identification information) to a CP to assist customer remediation under ASIC Regulatory Guidance, and enabling a CRB to alert a CP regarding bankruptcy information in relation to an existing customer.

---

[305] Privacy Act, s 6R.

[306] Privacy Act, divisions 3 and 4.

[307] Privacy Act, s 6(1).

[308] See ARCA submission, p 39.

Review findings

The Review has considered each of the above issues, and sets forward the following findings.

Individuals acting in trustee capacity

In relation to individuals acting in a trustee capacity, the Review considers that the CR Code should be amended to address this issue. It is possible for an individual to enter into consumer credit in their capacity as a trustee for a trust, however, as identified, there is currently no means to identify them as a trustee in the CR Code.

Proposal 44 – Amend CR Code definition of 'capacity information' to include an individual in their capacity as a trustee

Amend paragraph 1.2(c) relating to the definition of 'capacity information' to include an individual acting in their capacity as a trustee.

CP disclosures of credit eligibility information

In relation to CP disclosures of credit eligibility information, the OAIC's position is that a CP cannot rely on s 21G(3)(c)(i) of the Privacy Act to disclose such information to a broker as this is not the intent of this provision, which was included for credit managers. This is also because the mortgage broker is usually assisting an individual to deal with a CP or CRB and is not acting as an agent for the CP.[309] Instead, the Review considers that the Privacy Act already provides a mechanism for mortgage brokers to access credit reporting information to support individuals in their loan applications. This is provided for through the access seeker provisions (ss 6L and 21T), which require an individual's consent.

OAIC Resolution of Practice Issue 11 – mortgage brokers should use the access seeker provisions to access CEI on behalf of an individual

The OAIC considers that the current access seeker provisions are the most appropriate mechanism for mortgage brokers to access credit information on behalf of an individual. This access requires consent from the individual.

Consideration of additional uses and disclosures

In relation to consideration of additional uses and disclosures of credit reporting information, the Review considers that such matters are beyond the scope of the CR Code, and would be more appropriately considered as part of the required independent review of Part IIIA.

[309] See, for example, Equifax's website which identifies mortgage brokers as an authorised access seeker.

Proposal 45 – OAIC to raise with the Attorney-General the issue of additional uses and disclosures of credit reporting information

The OAIC will raise the issue of additional uses and disclosures of credit reporting information with the Attorney-General in preparation for the review of Part IIIA.

6.3 Direct marketing

The Privacy Act prohibits CRBs from using or disclosing credit reporting information for the purposes of direct marketing.[310] There is a limited exception where CRBs can use credit information to assist CPs to pre-screen an individual to determine if there are eligible for a certain consumer credit products.[311]

There are some additional requirements in paragraph 18 of the CR Code which:

- limit the power of a CRB to use credit reporting information to develop tools that could help it (or a CP) assess the likelihood of the individual accepting specific credit or credit variation, or to target an individual to accept specific offers
- prohibit CPs from using eligibility requirements that indicate that the individual has, or may have, difficulties in meeting repayments under their existing credit arrangement
- give individuals the right to ask a CRB not to use credit reporting information about them for direct marketing purposes.

The Review sought stakeholder feedback about whether the provisions regulating direct marketing remain appropriate.

Stakeholder views

ARCA considered the existing direct marketing provisions to be appropriate.[312] Consumer advocates also supported the current restrictions in paragraph 18.[313] They considered that while paragraph 18.2 appeared to prevent financial hardship information from being used in pre-screening activities, it would be preferable if there was an explicit prohibition in the CR Code.[314]

Experian submitted that while it broadly agrees with the restrictions, its own experience is that the pre-screening provisions are rarely used in practice and are significantly out of date.[315] It noted that the current provisions refer to lists of individuals being provided to CRBs for pre-screening prior to

[310] Privacy Act, s 20G.

[311] Privacy Act, s 20G(2).

[312] See ARCA submission, p 30.

[313] See consumer advocates joint submission, p 40.

[314] See consumer advocates joint submission, p 40; Legal Aid Queensland submission, p 14.

[315] See Experian submission, p 12.

marketing being undertaken, whereas modern day marketing (e.g. via online digital platforms) operate on an 'on-demand' basis.

Experian also pointed out that the restrictions on the use of credit information for direct marketing significantly hamper the ability of lenders to offer risk-based pricing.[316] Right now, lenders are not able to access credit information in order to offer better deals to lower risk individuals until they have formally applied for consumer credit. Experian encouraged a review of Part IIIA and the respective CR Code provisions with a view to enabling the use of risk-based pricing.

Review findings

The Review has not identified any significant issues with the direct marketing provisions.

Experian raised two issues with the provisions in terms of outdated pre-screening practices and inability to provide risk-based pricing. The Review considers that concerned stakeholders could raise the former issue as part of the future independent review of Part IIIA (noting that the Review has not received sufficient information about this issue). The latter issue can be addressed by the introduction of a soft enquiries framework into the CR Code (see Proposal 43 and **Error! Reference source not found.**1 above).

6.4 Transfer of rights

Part IIIA permits a CP's repayment rights to be transferred to another organisation where that organisation has acquired the rights of that CP. That entity is then treated as a CP for the purposes of the credit provided.[317] The CR Code requires both the original CP and the acquirer to notify a relevant CRB of the transfer event and respect certain conditions.[318]

The Review sought feedback from stakeholders about whether the current provisions regulating transfer of CP rights remained appropriate. The Review also sought input on the transfer of credit from a fully participating CP to an entity with restricted participation in CCR.

Stakeholder views

ARCA raised an issue with paragraph 13.1(b) of the CR Code which provides that, as a condition to reporting a transfer event, an original CP must have notified the individual of the transfer event.[319] It noted that the debt assignment provisions in the various state Property Law legislation are silent as to whether a notice of assignment must be given by the original CP or acquirer CP. ARCA cited ASIC guidance which provides that the notice may be given by either the original creditor or debt purchaser. On this basis, ARCA recommended that paragraph 13.1(b) be amended to provide that either the original or acquirer CP must have notified the individual of the transfer event.

[316] See Experian submission, p 12.

[317] Privacy Act, s 6K.

[318] Paragraph 13 of the CR Code.

[319] See ARCA submission, p 10.

On the matter of dealing with the transfer of credit from a fully participating CP to an entity with restricted participation in CCR, Consumer advocates noted that debt buyers should not be able to work around the reciprocity and consistency principles which underpin CCR by relying on the rights transfer rules in Part IIIA.[320] They considered that the CR Code should restrict debt buyers without an ACL from being able to access RHI.

ARCA noted that their members had little feedback on this issue, though made reference to previous discussions with the OAIC that the acquiring CP will be required to ensure data is kept up to date, including with all the CRBs who hold this data.[321]

EWON submitted that if the CR Code is amended to strengthen the default information provisions, then this may require changes to the transfer of rights provisions.[322] In particular, EWON considered that changes would likely be required to ensure acquiring CPs can comply with a positive obligation to remove a statute barred debt, and (in the event of a change to Part IIIA) adhere to any maximum timeframe for credit default listing from the due date. It also considered that the 'no wrong door' approach to corrections should consider how it is applied to original and acquiring CPs.

Review findings

On the issue of notification of a transfer event, the Review disagrees with the proposal that paragraph 13.1(b) be amended to provide that either the original or acquirer CP must have notified the individual of the transfer event. It considers that this raises a risk that neither CP will notify the individual of the transfer event and instead rely on the assumption that the other CP has undertaken notification. This may result in an individual not being informed.

On the issue of acquiring CPs with restricted participation, the Review considers that an acquiring CP without an ACL will not be able to access any additional credit information such as RHI.

Acquiring CPs will continue to be responsible for:

- ensuring that data is kept up to date, including with all the CRBs who hold this data
- responding to any correction requests from the original CP
- reporting that the credit has been closed.

However, this does not mean that an acquiring CP with restricted participation can access or disclose RHI (or financial hardship information) to a CRB. This would have the effect of circumventing the strict provisions that exist to protect this type of information from being accessed where the CP is not subject to certain restrictions including the responsible lending provisions. If individuals or entities are aware of this occurring, they should make a complaint to the OAIC.

OAIC Resolution of Practice Issue 12 – acquiring CPs must not access credit information where they are not permitted to do so

[320] See consumer advocates joint submission, p 55.

[321] See ARCA submission, p 39.

[322] See EWON submission, p 8.

The OAIC considers that an acquiring CP without an ACL must not access credit information that they are not permitted to access, such as RHI or FHI.

As to EWON's observation regarding the acquiring CP complying with default information obligations. The Review considers that this has been addressed above as we have proposed that CRBs take the lead in correcting statute barred debt (see Proposal 19 and 4.3.1).

Glossary

For a full list of stakeholders that responded to the Consultation Paper, see Appendix B.

Term or acronym	Meaning
ABA	Australian Banking Association
ACCC	Australian Competition and Consumer Commission
ACL	Australian credit licence
AFCA	Australian Financial Complaints Authority
AFIA	Australian Finance Industry Association
AIR	Affected Information Recipients
ALRC	Australian Law Reform Commission
APPs	Australian Privacy Principles (contained in the Privacy Act)
ARCA	Australian Retail Credit Association
ASIC	Australian Securities and Investments Commission
BNPL	Buy Now Pay Later
CCLI	Consumer credit liability information
CCR	Comprehensive credit reporting
Commissioner	The Australian Information Commissioner
Consultation Paper	Review of the Privacy (Credit Reporting) Code 2014 Consultation Paper, 6 December 2021
Consumer advocates	Consumer advocates that contributed to the joint submission for this Review: Financial Rights Legal Centre, Consumer Action Law Centre, Consumer Credit Legal Service (WA) Inc., Financial Counselling Australia, Uniting Communities Law Centre SA, Care (Consumer Law Program, ACT), Redfern Legal Centre, Consumer Policy Research Centre
CP	Credit provider
CPRC	Consumer Policy Research Centre
Credit Act	*National Consumer Credit Protection Act 2009*
Credit Amendment Act	*National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Act 2021*
CRB	Credit reporting body
CR Code	Privacy (Credit Reporting) Code 2014
Data Standards	Australian Credit Reporting Data Standards
EDR	External dispute resolution

EWON	Energy & Water Ombudsman NSW
FBAA	Finance Brokers Association of Australia
IIS	IIS Partners
OAIC	Office of the Information Commissioner
Part IIIA	Part IIIA of the Privacy Act
PRDE	Principles of Reciprocity and Data Exchange
Privacy Act	*Privacy Act 1988*
Privacy Regulation	Privacy Regulation 2013
Review	Independent review commencing in 2021 of the CR Code in accordance with paragraph 24.3 of the CR Code
Review of Part IIIA	Review of Part IIIA of the Privacy Act to be completed before 1 October 2024
RHI	Repayment history information
SCI	Serious credit infringements
TIO	Telecommunications Industry Ombudsman

Appendix A

Questions the OAIC asked in the consultation paper

A.1 Key issues and general questions

Key questions for this Review	
1	What provisions in the CR Code work well and should remain as they are or with minimal changes?
2	What provisions in the CR Code are no longer fit-for-purpose? Why?
3	Do the CR Code get the balance right between protection of privacy on the one hand and use of credit-related personal information on the other? Why or why not?
Form and readability of the CR Code	
4	Does the CR Code need to be amended for clarity or readability? If so, in what way?
5	Are there any CR Code provisions that are open to interpretation or prone to misinterpretation? Which provisions and how could they be improved?
Interaction with the CCR system	
6	What has been the effect of mandatory CCR on compliance with the CR Code?
7	Are there inconsistencies between CCR requirements and CR Code requirements that could be addressed via an amendment to the CR Code? How could the CR Code be amended in this context?
Participation of other entities	
8	How might the CR Code need to be updated to accommodate other entities?

A.2 Specific questions about the CR Code

Governance of the CR Code	
9	Is the current process for developing variations to the registered CR Code appropriate?
10	Should additional compliance monitoring and governance arrangements be stipulated in the CR Code?
11	Do industry and individuals have access to the information they need to understand and/or apply the CR Code in practice? If not, what amendments could be made to the CR Code to improve this?
12	Are the provisions on credit reporting agreements, audits, training and policies appropriate? Should they be amended in any way? If yes, how?
13	Are the provisions related to internal practices and recordkeeping appropriate? Should they be amended in any way? If yes, how?
Provisions applying to certain types of information	
14	Are the CCLI provisions appropriate? Should the CCLI provisions contained in paragraph 6 be amended in any way? If yes, how?
15	Are the definitions / interpretations contained in paragraph 6 appropriate? Should they be amended in any way? If yes, how?
16	Are the RHI provisions appropriate? Should RHI provisions contained in paragraph 8 be amended in any way? If yes, how?
17	Are the default information and payment information provisions appropriate? Should the provisions contained in paragraphs 9 and 10 be updated in any way? If yes, how?
18	Are the provisions regulating use of publicly available information appropriate? Should they be amended in any way? If yes, how? Is the meaning of publicly available information adequately clear?
19	Are the provisions on serious credit infringements appropriate? Should they be amended in any way? If yes, how?
Protections and rights for individuals	
20	Are the provisions regulating how individuals are notified that their information will be provided to a CRB appropriate? Should they be amended in any way? If yes, how?
21	Are the protections for victims of fraud appropriate? Should the provisions contained in paragraph 17 be updated in any way? If yes, how?
22	Should there be further obligations on CRBs to alert individuals of enquiries received on a credit report during a ban period?
23	Are the existing direct marketing provisions appropriate? Should they be amended in any way? If yes, how?
24	Are the access provisions appropriate? Should the provisions in paragraph 19 be updated in any way? If yes, how?

25	Are the correction provisions appropriate? Should the provisions in paragraph 20 be updated in any way? If yes, how?
26	Are the provisions on complaint handling appropriate? Should the provisions in paragraph 21 be amended in any way? If yes, how?
27	Are arrangements for dispute resolution appropriate? Should the arrangements be changed in any way? If yes, how?
28	How could the CR Code be amended to enhance protections for individuals?
29	How could the CR Code be amended to better support people affected by domestic abuse?
Permitted activities of CRBs and CPs	
30	Is the provision regulating information requests appropriate? Should it be amended in any way? If yes, how?
31	Are the provisions regulating transfer of rights of CP appropriate? Should they be amended in any way? If yes, how?
32	Are the provisions regulating use and disclosure appropriate? Should they be amended in any way? If yes, how?

Appendix B

Stakeholders who made submissions

Stakeholders who made submissions
Afterpay
Australian Banking Association
Australian Privacy Foundation
Australian Finance Industry Association
Australian Retail Credit Association
Communications Alliance
Consumer advocates joint submission: • Financial Rights Legal Centre • Consumer Action Law Centre • Consumer Credit Legal Service (WA) Inc. • Financial Counselling Australia (FCA) • Uniting Communities Law Centre (CCLCSA) • Care (Consumer Law Program, ACT) • Redfern Legal Centre • Consumer Policy Research Centre
Consumer Policy Research Centre
Energy & Water Ombudsman NSW
Equifax
Experian
Finance Brokers Association of Australia
IDCARE
Peter Lauer
Legal Aid Queensland
Telecommunications Industry Ombudsman

Appendix C

Stakeholders who attended roundtable discussions/meetings

Stakeholders who attended roundtables
Afterpay
Australian Banking Association
Australian Financial Complaints Authority
Australian Institute of Credit Management
Australian Prudential Regulation Authority
Australian Retail Credit Association
Australian Security and Investments Commission
Brighte
Care Financial Counselling
Commonwealth Bank
Consumer Action Law Centre
Consumer Credit Legal Service (WA)
Consumer Policy Research Centre
Equifax
Finance Brokers Association of Australia
Financial Counselling Australia
Financial Counselling Victoria Inc.
Financial Counsellors Association of WA
Financial Rights Legal Centre
IDCARE
Latitude Financial
Legal Aid Queensland
Talefin
Telecommunications Industry Ombudsman
Thorn Group
Women's Legal Service Victoria (representing Economic Abuse Reference Group)