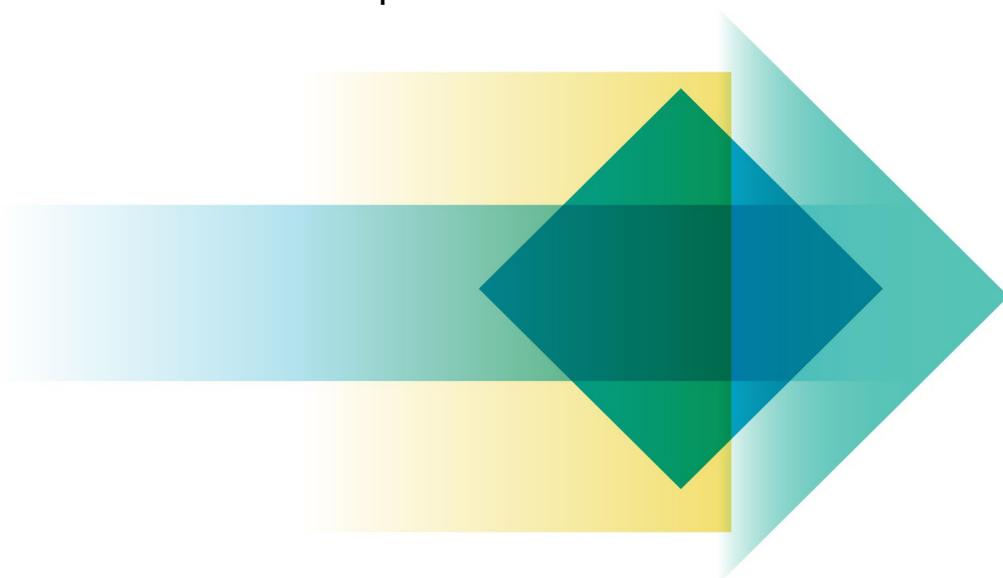


Review of the Privacy (Credit Reporting) Code 2014

Consultation Paper



6 December 2021

Contents

1.	About this review	4
1.1	This review	4
1.1.1	Why have a review?	4
1.1.2	Scope of the review	4
1.2	This consultation paper	5
1.3	How to provide comments	6
1.4	Privacy collection statement	6
2.	Australia's credit reporting landscape	7
2.1	How credit reporting is regulated in Australia	7
2.1.1	Credit reporting provisions under Part IIIA	7
2.1.2	Interaction between Part IIIA and the APPs	7
2.1.3	The CR Code	8
2.2	Who is regulated by the CR Code?	8
2.2.1	Credit reporting bodies	9
2.2.2	Credit providers	9
2.2.3	Affected information recipients	9
2.3	What information is regulated by the CR Code?	10
2.4	Recent developments to credit reporting in Australia	11
2.4.1	CR Code reviews	12
2.4.2	Variations to the Code	12
2.4.3	Mandatory Comprehensive Credit Reporting	12
3.	Overarching issues	14
3.1	Effectiveness of the CR Code	14
3.2	Form and readability of the CR Code	14
3.3	Interaction with the CCR system	15
3.4	Participation of other entities	16
4.	Governance of the CR Code	17
4.1	Code governance, oversight and awareness	17

4.1.1	Code development and ongoing monitoring of compliance	17
4.1.2	Education and awareness of the CR Code	18
4.2	Governance obligations applying to CRBs and CPs	19
4.2.1	Credit reporting agreements, audits, training and policies	19
4.2.2	Internal practices and recordkeeping	20
5.	Provisions applying to certain types of information	21
5.1	Consumer credit liability information	21
5.2	Repayment history information	22
5.3	Default information and payment information	23
5.4	Publicly available information	24
5.5	Serious credit infringements	25
6.	Protections and rights for individuals	26
6.1	Notice to individuals	26
6.2	Protections for victims of fraud	27
6.3	Use of credit reporting information for direct marketing	28
6.4	Access rights	29
6.5	Correction of information	30
6.6	Complaint handling	31
6.7	Dispute resolution processes for individuals	32
6.8	Other options to protect individuals affected by domestic abuse	33
7.	Permitted activities of CRBs and CPs	35
7.1	Information requests	35
7.2	Transfer of rights of CP	35
7.3	Use and disclosure	36
8.	Complete list of questions	38
	Glossary	40

1. About this review

In this section you can find:

- Information about the scope and purpose of this review
- Information about this consultation paper
- Directions on how to provide comments.

1.1 This review

The Office of the Australian Information Commissioner (OAIC) is reviewing the Privacy (Credit Reporting) Code 2014 (Version 2.1) (the CR Code) to decide whether and how it could be updated. This is the second independent review of the CR Code.

This Consultation Paper is aimed at eliciting feedback on the CR Code to find out what is working well and what can be improved.

The CR Code is a legislative instrument issued by the Australian Information Commissioner (the Commissioner). It applies to Credit Reporting Bodies (CRBs), Credit Providers (CPs) and Affected Information Recipients (AIRs). The CR Code supplements the provisions contained in Part IIIA of the *Privacy Act 1988* (Privacy Act) and the Privacy Regulation 2013 with respect to the handling of personal information about individuals' activities in relation to consumer credit. Importantly, a breach of the CR Code is a breach of the Privacy Act. Further information about the role of the CR Code within Australia's broader credit reporting environment is set out at section 2 of this consultation paper.

1.1.1 Why have a review?

Paragraph 24.3 of the CR Code requires the Commissioner to initiate an independent review of the CR Code every four years. As part of this review process, the OAIC is consulting stakeholders to assist in assessing whether or the extent to which revisions to the CR Code are required.

1.1.2 Scope of the review

This is a general review of all the provisions of the current CR Code.¹ As with previous reviews, the purpose of this review is to ensure that the CR Code, in its current form, achieves its purpose and is easy to read, understand and apply in practice.

This review considers the operation of the CR Code, and is not a broader review of Part IIIA of the Privacy Act. Therefore, issues about Part IIIA and how it applies to CRBs, CPs and AIRs are out of scope (except to the extent of any inconsistency between drafting of the CR Code and the requirements of

¹ Amendments to the CR Code to address financial hardship will not form part of this review. Those amendments are being considered as part of a Code variation application which is currently before the Commissioner and were the subject of a separate consultation process. See section 2.4.2.

Part IIIA). There will be a separate review of Part IIIA which will be undertaken by the Attorney-General and which should occur before 1 October 2024.²

Where issues relate to Part IIIA but may impact the operation of the CR Code, we would welcome stakeholder commentary on these issues.

1.2 This consultation paper

This consultation paper is intended to facilitate engagement in the review process. This consultation paper has been organised in two parts.

The first part comprises sections 1 and 2, which provide an overview of the review and credit reporting landscape:

- [Section 1](#) – information about the review and how to provide comments
- [Section 2](#) – information about Australia’s credit reporting landscape, including who is regulated, their obligations under the Privacy Act and the CR Code, and recent developments.

The second part comprises sections 3 to 7 and set out the key issues being explored as part of this review. These sections pose questions for stakeholders to provide input. These sections are organised thematically and have been grouped into the following sections:

- [Section 3](#) – overarching issues for consideration
- [Section 4](#) – governance of the CR Code
- [Section 5](#) – the code provisions applying to certain types of information
- [Section 6](#) – the code provisions providing for protections and rights for individuals, and
- [Section 7](#) – the code provisions which provide for permitted activities by regulated entities.

The OAIC invites comment from interested individuals, agencies and organisations on all elements and aspects of the CR Code.

Questions have been included in this consultation paper to help guide your feedback. It is not necessary to respond to every topic or question raised in the paper. Nor should you feel restricted to the topics or questions we have raised. When commenting, we encourage you to provide evidence to support your feedback, including examples, case studies, statistics, or other information.

² *Privacy Act 1988* s 25B(2).

1.3 How to provide comments

Submissions can be made by:

Email	consultation@oaic.gov.au
Post	GPO Box 5218 Sydney NSW 2001

The closing date for comments is **4 February 2022**.

We intend to make all submissions publicly available. Please indicate when making your submission if it contains confidential information that you don't want made public and why it should not be published. Requests for access to confidential comments will be determined in accordance with the *Freedom of Information Act 1982*.

Although you may lodge submissions by email or post, email is preferred. To help us meet our accessibility obligations, we would appreciate if you could provide your submission in Microsoft Word (.docx) format.

1.4 Privacy collection statement

The OAIC will only use the personal information it collects during this review for the purpose of considering the issues raised in the consultation paper. This will include sharing submissions with IIS Partners – a privacy consultancy that is assisting OAIC with this review.

2. Australia's credit reporting landscape

In this section you can find:

- A general overview of Part IIIA of the Privacy Act and the CR Code (including its purpose, the activities it covers and its main provisions)
- Contextual information, including other relevant developments and legislative reform

2.1 How credit reporting is regulated in Australia

Credit reporting is regulated under Part IIIA of the Privacy Act (Part IIIA), the Privacy Regulations 2013 and the CR Code. This section explains how those provisions and instruments interact with each other.

2.1.1 Credit reporting provisions under 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 respected. To achieve this, Part IIIA regulates the handling of personal information about individuals' activities in relation to consumer credit. It outlines:

- 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, and
- The purposes for which that information may be handled.

2.1.2 Interaction between Part IIIA and the APPs

The Australian Privacy Principles (APPs) govern the collection and handling of personal information by Australian government agencies and private sector organisations regulated by the Privacy Act. The APPs apply to the extent of any inconsistency with other legislative provisions.

Part IIIA specifically governs the collection and handling of credit-related personal information by CRBs, CPs and AIRs, and clarifies the extent to which the APPs apply to them. In brief:

- CRBs³ – the APPs do not apply in relation to credit reporting information, CP derived information and pre-screening assessments (however the APPs will apply to other types of personal information).
- CPs⁴ – in respect of handling credit information, credit eligibility information and CRB derived information, the rules set out in Part IIIA apply in addition to, or instead of, the APPs.

³ *Privacy Act 1988* s 20A.

⁴ *Privacy Act 1988* s 21A.

- AIRs⁵ – in respect of regulated information, the rules set out in Part IIIA apply in addition to, or instead of, the APPs.

The specific types of credit-related personal information noted below in respect of Part IIIA are, in turn, addressed in the CR Code. This is further set out at section 2.3 of this paper.

2.1.3 The CR Code

The CR Code provides further particularisation of the credit reporting obligations set out in Part IIIA and the Privacy Regulation 2013. It explains how CRBs, CPs and AIRs must handle credit-related personal information.

The CR Code is a legislative instrument. It is binding, which means that relevant CRBs, CPs and AIRs must follow it. A failure to comply with the CR Code is a breach of the Privacy Act.

The CR Code was first introduced in 2014 and was developed by the CR Code Developer, the Australian Retail Credit Association (ARCA). It was developed in accordance with section 26N of the Privacy Act and the OAIC's Guidelines for Developing Codes.⁶ Governance of the CR Code is discussed further in section 4 of this paper.

The CR Code was developed to meet the following objectives:

- Improve the economic effectiveness of credit reporting
- Ensure the privacy of enhanced credit reporting information
- Improve the integrity of the credit reporting information
- Improve transparency in the credit reporting process
- Set standards of conduct and practice for industry participation in the credit reporting system, and
- Provide credible monitoring and enforcement of compliance.

Key provisions in the CR Code are discussed further in sections 5 to 7 of this consultation paper, and have been grouped into the following categories:

- provisions applying to certain types of information
- provisions which provide for individuals' protections and rights, and
- provisions which permit activities of CPs and CRBs.

2.2 Who is regulated by the CR Code?

The CR Code regulates Australia's credit reporting system. The main participants in that system are CRBs and CPs and the activities of those participants must comply with the CR Code. The CR Code

⁵ *Privacy Act 1988* s 22A.

⁶ [OAIC Guidelines for Developing Codes](#).

also regulates what the Privacy Act refers to as ‘AIRs’. CRBs, CPs and AIRs are defined in the Privacy Act and described below.

2.2.1 Credit reporting bodies

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. 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. If the individual has poor credit scores, the CP might choose not to approve the individual’s application for credit. The main CRBs in Australia are Equifax, Experian and Illion.

2.2.2 Credit providers

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 and organisations like telcos 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 are also CPs, but real estate agents, general insurers and employers are not.

As noted above, 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.

2.2.3 Affected information recipients

AIRs are entities that are entitled to receive credit-related personal information under Part IIIA. This includes:

- Mortgage insurers⁷ and trade insurers⁸
- A related body corporate of a CP or an entity that assists the CP in processing credit applications⁹ or managing credit¹⁰
- An entity using the information in the course of purchasing a debt owed or purchasing a stake in the CP.¹¹

⁷ 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.

⁸ A trade insurer protects businesses from bad debts. They re-imburse CPs (e.g., a small business) when their customers are unable to pay – because of default, insolvency (or other agreed reasons).

⁹ E.g. A person that processes documents or paperwork associated with making a credit application to the CP.

¹⁰ E.g. A person who manages the credit (e.g. cash flow to a small business) on behalf of the CP in accordance with a payment schedule.

¹¹ Can include a professional legal or financial advisor of the entity.

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 (section 21N).

2.3 What information is regulated by the CR Code?

The CR Code regulates credit-related personal information. The table below lists the different information regulated by the CR Code.

Type of information	Definition
Consumer credit liability information (CCLI)	Includes the following: <ul style="list-style-type: none"> the name of the provider whether the provide is a licensee the type of consumer credit 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; and that are prescribed by the Regulations 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.
Credit eligibility information	An individual's credit reporting information and any further information a CP derives from an individual's credit reporting information
Credit information	A type of personal information which includes information: <ul style="list-style-type: none"> that identifies an individual about the amount an individual has borrowed about repayments about defaults
Credit reporting information	An individual's credit report and credit score
Credit-related personal information	Credit-related personal information means credit information, credit reporting information, credit eligibility information or regulated information, as applicable in the context.
Creditworthiness	An assessment of creditworthiness is an assessment of the individual's: <ul style="list-style-type: none"> eligibility to get consumer credit consumer credit history capacity to repay an amount of credit that related to consumer credit

Default information	<p>Information about a payment (including a payment that is wholly or partly a payment of interest) that the individual is overdue in making if:</p> <ul style="list-style-type: none"> • payment is 60 days overdue • CP has provided written notice of the overdue payment to the individual and requesting for payment • the provider is not prevented by a statute of limitations from recovering the amount of the overdue payment • overdue amount must not be less than \$150 (or if a higher amount is prescribed by the Regulations)
Payment information	A statement that payment has been made of an overdue payment that has previously been disclosed by the CP to the CRB as default information.
Repayment history information (RHI)	<p>Includes the following:</p> <ul style="list-style-type: none"> • whether or not an 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 – the day on which the individual makes that payment
Serious credit infringement	<ul style="list-style-type: none"> • act done by individual that involves fraudulently / attempting fraudulently to obtain consumer credit; or • act done by individual that involves fraudulently/attempting fraudulently to evade the obligations in relation consumer credit; or • act done by individual if: <ul style="list-style-type: none"> – a reasonable person would consider that the act indicates an intention, on the part of the individual, to no longer comply with the individual’s obligations in relation to consumer credit provided by a CP; and – CP has, after taking such steps as are reasonable in the circumstances, been unable to contact the individual about the act; and – at least 6 months have passed since the CP last had contact with the individual.

2.4 Recent developments to credit reporting in Australia

There have been a range of recent developments in credit reporting in recent years including amendments to the CR Code and amendments to other legislation that may impact the operation of

the CR Code. Those developments are relevant to understanding the CR Code in context and assessing its ongoing effectiveness.

2.4.1 CR Code reviews

Paragraph 24.3 of the CR Code requires the Commissioner to initiate an independent review of the CR Code every four years. The first independent review of the CR Code took place in 2017 but was conducted before mandatory Comprehensive Credit Reporting (CCR) was introduced. As such, that review was unable to canvas the interaction of the CR Code with CCR requirements.

This consultation paper forms part of the second independent review of the CR Code. It considers the introduction of mandatory CCR in section 2.4.3 and 3.3 of this paper.

2.4.2 Variations to the CR Code

The CR Code has been amended four times since it was first introduced in March 2014. Variation applications have been made by ARCA as the CR Code Developer.

The most recent variation application was submitted by ARCA in September 2021 and seeks to address the new financial hardship provisions introduced by the *National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Act 2021*. The Act provided for a new form of ‘financial hardship information’ to be included in the credit reporting system from 1 July 2022, and also made other changes such as the allowance for ‘non-participating CPs’ and a requirement for CRBs to give individuals their ‘credit rating’. This variation application is currently subject to consideration by the OAIC.¹²

2.4.3 Mandatory Comprehensive Credit Reporting

The move to mandatory CCR in Australia has been a gradual process. In November 2017, the Commonwealth Treasury announced that CCR would be mandated for the ‘Big Four’ banks. As of July 2018, major banks were required to share 50% of customers’ data with CRBs. This was increased to 100% in July 2019. Then earlier this year, mandatory CCR was rolled out to ‘eligible licensees’ under the *National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Act 2021*.¹³

The main effect of these reforms has been to change credit reporting in Australia from a voluntary system to a mandatory one. The 2014 Financial System Inquiry and the Productivity Commission Inquiry into Data Availability and Use recommended that the Government mandate CCR in the absence of voluntary participation.¹⁴ Mandatory CCR aims to enable CPs to better establish an individual’s credit worthiness and to enable a more competitive and efficient credit market.¹⁵

¹² As noted above, the recent variation application does not form part of the scope of this review.

¹³ Eligible Licensees is defined under s 133CN of the *National Consumer Credit Protection Act 2009*. 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, or is a body corporate of a kind prescribed by the regulations; and (b) is a credit provider.

¹⁴ [Explanatory Memorandum](#) to the National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Bill 2019, paragraph 1.6.

¹⁵ [Explanatory Memorandum](#) to the National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Bill 2019, paragraph 1.6.

Previously CPs could choose whether to provide credit information about their customers to CRBs but now 'eligible licensees' must provide the information. Therefore, a key question is whether the move to mandatory CCR has impacted the operation of the CR Code. This matter is considered in section 3.3 of this paper.

3. Overarching issues

In this section you can find:

- Key questions for this review. These are intended to help us understand how the CR Code is operating and areas for improvement
- Other general questions and issues, including in relation to the form and function of the CR Code and how they operate in practice

3.1 Effectiveness of the CR Code

This review is aimed at understanding how the CR Code is currently operating, whether the provisions remain fit-for-purpose and what revisions or updates – if any – may be needed. The OAIC is interested in stakeholders' views of the overall effectiveness of the current CR Code.

Questions – Effectiveness of the CR code

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. Does the CR Code get the balance right between the protection of privacy on the one hand and use of credit-related personal information on the other? Why or why not?

3.2 Form and readability of the CR Code

There has been ongoing discussion about the format and readability of the CR Code, with some stakeholders raising concerns about its complexity and how this impacts individuals' ability to pursue their rights. To some degree, the complexity of the Code is a product of Part IIIA of the Privacy Act which provides the 'baseline' for the CR Code. Therefore, the complexity and detail of Part IIIA necessarily impacts the complexity and detail of the Code.

Some stakeholders have suggested that the CR Code be restructured to separate provisions containing rights and protections for individuals from technical industry-related provisions. Another option could be to incorporate overarching principles into the Code which align with Part IIIA requirements but give individuals or their advocates greater certainty about individual rights under the Code. These principles could provide a lens by which the technical provisions should be interpreted. For example, it has been noted that the Australian Financial Complaints Authority (AFCA) has been applying a principle of fairness to its decision-making on credit reporting disputes which may warrant formalisation in the CR Code.

The structure and format of the CR Code takes its cue from Part IIIA and therefore is structured according to issue. Thus, rules on default information are grouped together in one paragraph, rather than being separated into what individuals may need to know and what CPs may need to know. The OAIC is interested in stakeholders' views as to whether this approach continues to be appropriate given the structure of Part IIIA has not been amended.

Questions – 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?

3.3 Interaction with the CCR system

The credit reporting system has changed significantly with the introduction of mandatory CCR. A central question for this review is whether the CR Code needs to be updated in light of changes brought about by CCR.

One point of possible friction is the 'must disclose' posture of CCR and the 'can disclose' posture of Part IIIA of the Privacy Act and the CR Code. The mandatory CCR regime requires reporting of all credit reporting information while Part IIIA and the CR Code are concerned with what information may be disclosed by a CP to a CRB. This may heighten risks of non-compliance with either regime, particularly for areas of the CR Code that are unclear or open to different interpretations.

Stakeholders have raised concerns about whether CCLI may be disclosed for guarantors under Part IIIA and the CR Code. Entities may take a conservative approach and restrict disclosure to avoid a breach of the CR Code, but in doing so risk breaching CCR laws which mandate disclosure. Other stakeholders have raised concerns that the CCR obligations will result in entities being inflexible when negotiating the resolution of financial disputes, including decisions around the removal, delay or withholding from listing defaults on credit reports.

Questions – 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?

3.4 Participation of other entities

The credit reporting landscape is changing with participation by new entities. For example, Optus is the first telecommunications company to begin participating in the credit reporting system, starting its participation in September 2021. As a telecommunications 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). The participation of telecommunications companies, and possibly utilities also, may necessitate changes to the CR Code to accommodate different account arrangements. For example, the definitions of account ‘open’ and ‘close’ dates in paragraph 6 of the CR Code may not adequately reflect telecommunications accounts where connection and disconnection of the service may be the more relevant milestones. Similarly, the definition of credit limit may need adjustment for the telecommunications provider context (where there may be no credit limit per se, but a monthly plan for services and handset payment).

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 and some are not. As with the participation of telecommunications and utilities providers, the participation of BNPL providers in the credit reporting system may necessitate changes to the CR Code to accommodate different account arrangements. For example, BNPL transaction accounts where each transaction is treated as a separate line of ‘credit’ under the Privacy Act may need to be able to be grouped together for credit reporting purposes. The meaning of ‘credit limit’ may also need adjustment in this context.

A broader issue relates to the extent of the participation in the credit reporting system of non-ACL entities and entities that are not bound by responsible lending obligations. Questions have been raised as to whether CPs should be required to have an ACL and comply with responsible lending obligations before they be allowed to access credit reporting information. Such matters may fall outside the scope of the CR Code but warrant further consideration.

Questions – Participation of other entities

8. How might the CR Code need to be updated to accommodate other entities?

4. Governance of the CR Code

In this section you can find:

- An overview of governance arrangements for the CR Code, including the development, variation and monitoring of the Code
- Information about governance obligation applying to CRBs and CPs
- Questions for stakeholders to gather views on the governance arrangements and issues raised in this section

The first independent review of the CR Code was conducted in 2017. Amongst the review's key themes was 'governance, monitoring and enforcement'. Stakeholder submissions to ARCA in 2013 in respect of developing the CR Code, and to the 2017 independent review, highlighted the importance of good governance across areas of code development (i.e. development of the CR Code and any subsequent amendments), monitoring of compliance with the CR Code and enforcement of its provisions. The OAIC is interested in stakeholders' views as to whether the current provisions in the CR Code facilitate good governance and effective monitoring and compliance.

This section of the paper is divided into two parts. The first is focused on governance of the Code itself including how it is developed, updated and overseen. The second focuses on governance requirements that apply to CRBs and CPs.

4.1 Code governance, oversight and awareness

4.1.1 Code development and ongoing monitoring of compliance

The CR Code was developed by ARCA. Considerable thought was given to the most appropriate body to act as the CR Code Developer.

The Privacy Act does not specify who can be a code developer; rather, it specifies the required activities of a code developer and the permitted contents of a written code of practice. The OAIC Guidelines for Developing Codes shed further light on identifying an appropriate code developer when the Commissioner requests that a code be developed.¹⁶ The Guidelines also include consultation requirements and outline the matters which the Commissioner will consider in reviewing a variation application to a registered code. These requirements provide important safeguards to ensure that variations to the CR Code have undergone appropriate consultation with relevant stakeholders. The Commissioner then independently assesses any application to amend the CR Code.

¹⁶ [OAIC Guidelines for Developing Codes](#).

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. 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 the Commissioner as to the scope and choice of the reviewer.

The 2017 independent review recommended 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. This recommendation was made in response to stakeholder views that the OAIC's monitoring and enforcement function could be strengthened.

The OAIC is interested in stakeholders' view as to whether additional compliance monitoring and governance provisions should be stipulated in the CR Code.

Questions – Code development and ongoing monitoring

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?

4.1.2 Education and awareness of the CR Code

The foundation for compliance with any legislative scheme is strong general awareness of key concepts and requirements, and education and other knowledge-building initiatives can assist with this. To this end, the 2017 independent review recommended that consideration be given to enhancing industry and consumer awareness of the CR Code (i.e. its foundational concepts, as well as a number of specific provisions). The OAIC has published detailed information about the CR Code on its website, however, does not conduct training for industry or individuals on the Code's application.

Some individuals may find it difficult to fully understand the complexities of credit reporting and are less likely to be across the nuances of how CRBs, CPs and AIRS collect and manage their personal information. ARCA, as code developer and the industry body with most extensive practical expertise in relation to the contents and application of the CR Code, 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.¹⁷

¹⁷ [Credit Smart website](#).

The OAIC is interested in stakeholder views on awareness of the CR Code, and the extent to which industry and individuals have access to the information they need to understand and/or apply the Code in practice.

Question – Education and Awareness

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?

4.2 Governance obligations applying to CRBs and CPs

4.2.1 Credit reporting agreements, audits, training and policies

Part IIIA of the Privacy Act requires CRBs to enter into written agreements with CPs that require the CP 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 CRBs to ensure regular independent audits are conducted to check that CPs are complying with those written agreements. The CR Code imposes some additional requirements which are contained in paragraphs 2, 3 and 23. The CR Code:

- Requires credit reporting agreements to oblige both parties to comply with Part IIIA, the Regulations and the CR Code
- Requires CRBs to establish a documented risk-based program to govern the frequency and extent of audits
- Requires CPs to allow auditor access to its records and to rectify issues identified in the audit
- Requires a CRB to take action (including terminating the agreement if reasonable) if a CP fails to meet contractual obligations
- Obliges CRBs, CPs, mortgage insurers and trade insurers to train employees that handle credit reporting information or credit eligibility information
- Requires web publication of credit reporting policies.¹⁸

Question – Credit reporting agreements, audits, training and policies

12. Are the provisions on credit reporting agreements, audits, training and policies appropriate? Should they be amended in any way? If yes, how?

¹⁸ A credit reporting policy is similar to a privacy policy but explains the entity's practices in relation to credit-related person information. CRBs, CPs and AIRs are required to have a credit reporting policy under Part IIIA of the *Privacy Act 1988*.

4.2.2 Internal practices and recordkeeping

Part IIIA of the Privacy Act and the CR Code contain provisions that require CRBs and CPs to implement internal procedures and systems to ensure compliance with Part IIIA and the CR Code and maintain information security. 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 destroyed¹⁹
- Specifies that records should be retained for a minimum of five years.

Question – Internal practices and recordkeeping

13. Are the provisions related to internal practices and recordkeeping appropriate? Should they be amended in any way? If yes, how?
-

¹⁹ CRBs and CPs must also maintain records of any consent provided by an individual, requests to establish or extend a ban period, corrections, complaints, pre-screening requests by a CP and monitoring and auditing of CPs. CPs must also maintain certain records of written notices to the individual.

5. Provisions applying to certain types of information

In this section you can find:

- An overview of provisions in the CR Code applying to certain types of information, including provisions that regulate CCLI, RHI, and default and payment information
- Questions for stakeholders to seek feedback on these provisions and issues raised

5.1 Consumer credit liability information

Part IIIA of the Privacy Act permits CRBs to collect and disclose CCLI, subject to certain conditions. CCLI – also referred to as ‘account information’ – is defined in the Privacy Act.²⁰ The CR code contains specific provisions applying to CCLI in paragraph 6. Paragraph 6 of the CR Code:

- Defines the meaning of key CCLI concepts
- Requires common descriptors for types of credit to be used by CPs when disclosing CCLI to CRBs
- Requires CPs to tell the CRB when credit is terminated or ceases to be in force.

Possible issues with how CCLI is handled under Part IIIA and the CR Code include:

- *Uncertainty about the account open date* – Paragraph 6 of the CR Code explains that ‘the day on which the consumer credit is entered into’ aligns with the 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 creation, and this creates uncertainty about which date to give to the CRB when providing CCLI.
- *Debt buyers submitting CCLI for credit accounts that are no longer active* – Where debt buyers purchase debts from the original CP, it appears that in some cases the debt buyer may continue to provide CCLI to the CRB where an account has been charged off by the original CP but not reported as closed. The effect is that debts potentially live on indefinitely in CCLI. This is at odds with data retention provisions in Part IIIA which require disposal of default information after five years.
- *Uncertainty about what CCLI may be disclosed to a guarantor* – Due to this uncertainty, some CPs take a conservative approach and disclose less CCLI to a guarantor. However, with the commencement of CCR which mandates certain disclosures, CPs may risk non-compliance with the CCR regime if they do not disclose the appropriate information.
- *Uncertainty about treatment of historic CCLI* – It is unclear 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 limit may be

²⁰ For the definition of CCLI see section 6 of the *Privacy Act 1988* and the [Glossary](#).

held and disclosed. This issue also arises in relation to other CCLI. For example, whether a CRB can/ should record both current and previous CPs.

Questions – Consumer credit liability 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?

5.2 Repayment history information

Part IIIA of the Privacy Act permits CRBs to collect RHI subject to certain conditions.²¹ CRBs and CPs are only permitted to share RHI with one another if the CP is a licensee or is prescribed by the Regulations. The CR Code contains specific provisions applying to RHI in paragraph 8. Paragraph 8:

- Clarifies aspects of the definition of RHI including what it means for payments to be overdue
- Specifies how a CP is to disclose RHI to a CRB.

Possible issues with how RHI is handled under Part IIIA and the CR Code include:

- *Some ongoing uncertainty about monthly reporting of RHI* – The CR Code specifies how CPs should determine overdue days in an RHI reporting month. It appears that the CR Code’s provisions generally support a consistent approach. However, there are some ongoing issues with shorter months potentially skewing the reporting of subsequent months.
- *Lack of provision for correction of RHI due to circumstances beyond the individual’s control* – Currently paragraph 20 allows an individual to request correction of default information if it relates to an overdue payment which occurred because of the ‘unavoidable consequences of circumstances beyond the individual’s control.’ However, the same option is not explicitly included in relation to RHI.
- *Notice to individuals about disclosure of RHI to CRBs* – It has been suggested that CPs that are reporting RHI to a CRB about their customers should notify those customers on those arrangements through their regular account statements or by SMS. CPs are required to notify individuals of certain matters at or before they collect personal information that they are likely to disclose to a CRB. Other notice requirements apply in relation to default information and serious credit infringements, but not negative RHI.

²¹ For the meaning of RHI see section 2.3 of this paper and the [Glossary](#).

Questions – Repayment history information

16. Are the RHI provisions appropriate? Should RHI provisions contained in paragraph 8 be amended in any way? If yes, how?

5.3 Default information and payment information

Part IIIA of the Privacy Act permits CRBs to collect default information (relating to overdue payments) and payment information (relating to payment of an overdue payment previously disclosed to a CRB as default information). Certain conditions apply. For example, the payment must be at least 60 days overdue, and the amount overdue must be \$150 or more. Under Part IIIA, if a CP has disclosed default information to a CRB, the CP must give the CRB payment information when the overdue amount is paid.

Paragraphs 9 and 10 of the CR Code apply to default information and payment information respectively.

Paragraph 9 applies to default information, and:

- Explains the process for when an individual has submitted a hardship request, that is that 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 section 6Q notices and section 21D(3)(d) notices²²
- Explains how overdue amounts must be reported including in cases where additional amounts have accrued since the 21D(3)(d) notice.

Paragraph 10 applies to payment information, and:

- Defines what it means for an overdue payment to be considered paid
- Requires the CP to disclose payment information to the CRB within 3 days if the individual requests this.

Possible considerations for how default and payment information is handled under Part IIIA and the CR Code include:

- *Establishing a positive obligation on CPs to request the removal of default information that has become statute barred* – Under section 6Q(1)(c) of the Privacy Act, default information does not exist where the provider is prevented by a statute of limitations from recovering the overdue payment. In some cases, defaults are listed just prior to the statute of limitations taking effect and are not removed once that date is reached. In practice, these defaults may not be removed

²² The section 6Q notice and section 21D(3)(d) notice are written notices from the CP to the individual required by the Privacy Act. The 6Q notice is to notify the individual of an overdue payment and the 21D(3)(d) notice is to notify the individual that the CP intends to disclose default information to a CRB.

until an individual realises and seeks their removal. One option would be for CPs to 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.

- *Requiring CPs to list any defaults with CRBs within a reasonable period of time* – There appear to be cases where CPs list defaults with CRBs at staggered times which has the effect of extending the period for which that default information is reported, beyond the 5 years required by Part IIIA.
- *Requiring a stand-alone section 21D(3)(d) notice* – Section 21D(3)(d) states that a CP can disclose default information about an individual if they have given the individual a notice in writing stating their intention and 14 days have passed. It appears that in some cases, the section 21D(3)(d) notice is included in other correspondence to the individual. 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.
- *Resolving uncertainty about how to report ‘new arrangement information’* – The current framing of the CR Code does not appear to easily allow for the reporting of payment information in cases 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. This may result in the CP having an ongoing obligation to report payment information for the original default amount.
- *Simplifying arrangements for removal of default information in cases of economic abuse* – Issues associated with domestic abuse are also outlined in section 6.8 of this paper.

Questions – Default information and payment information

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?

5.4 Publicly available information

Part IIIA of the Privacy Act permits a CRB to collect and disclose publicly available information if it relates to the individual’s credit worthiness and meets other requirements. Paragraph 11 of the CR Code imposes some additional requirements. In particular, paragraph 11:

- Further articulates the requirements for collecting publicly available information
- Specifies that the publicly available information must come from an agency, or a state or territory agency and that the information must be generally available to the public
- Clarifies that originating processes from a Court or Tribunal and specific judgments and proceedings are excluded from the meaning of publicly available information.

Questions – Publicly available information

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?

5.5 Serious credit infringements

Part IIIA of the Privacy Act allows a CRB to collect information about serious credit infringements. A serious credit infringement is more serious than a default in that it represents cases where an individual has fraudulently obtained credit or sought to fraudulently evade credit obligations, or no longer intends to comply with credit obligations.²³

The CR Code contains specific provisions applying to serious credit infringements in paragraph 12. Paragraph 12:

- Requires a CP to reasonably establish that the individual made false statements when disclosing a serious credit infringement to a CRB
- Sets out the reasonable steps a CP must take to contact an individual before the CP may disclose a serious credit infringement to a CRB after six months of no contact with the individual
- Requires a CRB to destroy serious credit infringement information where overdue amount is paid or the CP enters a new arrangement with the individual.

Questions – Serious credit infringements

19. Are the provisions on serious credit infringements appropriate? Should they be amended in any way? If yes, how?

²³ Serious credit infringement is defined in s 6(1) of the *Privacy Act 1988*. In this paper, see section 2.3.

6. Protections and rights for individuals

In this section you can find:

- An overview of provisions in the CR Code that protect the rights of individuals. This includes provisions that protect victims of fraud and give individuals rights to access and correct credit-related personal information held about them
- Questions for stakeholders to seek feedback on these provisions and issues raised

6.1 Notice to individuals

Part IIIA of the Privacy Act requires a CP that collects personal information to notify individuals if the CP is likely to disclose the information to a CRB. In doing so, the CP must ensure that the individual is aware of the CRBs with which the CP deals. The CR Code contains some additional notice requirements in paragraph 4. In particular, paragraph 4:

- Specifies additional information (referred to as ‘notifiable matters’) that the notice must include
- Requires the CP to explain to the individual that the CP’s website contains information about credit reporting and give the website details
- Requires the CP to give a short description of the key issues outlined on the CP’s website
- Requires the CP to make clear that the individual may ask to receive the statement in an alternative form (for example, hard copy).

A possible issue for consideration is:

- *Confusion about the difference between notice and consent* – It appears that there is an increase in the number of credit reporting complaints that have turned on notice and consent. Complainants or their representatives have argued that they did not consent to an information request (also commonly referred to as a ‘credit enquiry’). However, Part IIIA of the Privacy Act and the CR Code do not require CPs to get individual consent before making an information request. The obligation is to notify to the individual.

Question – Notice to 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?

6.2 Protections for victims of fraud

One of the main protections provided to victims of fraud is the ability to implement a ‘ban period’ during which a CRB cannot use or disclose the individual’s credit reporting information. Individuals have the right to request a ban period under Part IIIA.²⁴ 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. In particular, paragraph 17:

- Sets out actions a CRB must take if an individual asks the CRB to implement a ban period and allows the individual to ask the CRB to ask other CRBs to also implement a ban period
- Requires a CRB to tell CPs requesting credit reporting information about the individual of the ban
- Requires a CRB to notify the individual at least 5 days before the ban period is due to end and explain the individual’s rights to extend the ban period, and what, if any, information the CRB requires to support the individual’s allegation of fraud.

The length of the ban period was raised in the previous review. That review acknowledged that the ban period was set by the Privacy Act rather than the CR Code but suggested that consideration be given to the appropriateness of the current ban period and the nature and rationale for its length, particularly in comparison to other jurisdictions. There appear to be some ongoing concerns about the ban period and how it is implemented. Possible issues include:

- *Whether the ban period should apply indefinitely until an individual asks for the ban to be removed* – This is the practice in other jurisdictions including most states in the US. There has been some concern that the 21-day length of the ban period in Australia under the Privacy Act is too short for cases of fraud to be resolved by the individual and places a burden on the individual to apply for extensions. It is important to note that the length of the ban period is set by the Privacy Act and is therefore out of scope for this review. That said, it may be considered as part of the statutory review of Part IIIA of the Privacy Act.²⁵
- *The initial ban period of 21 days is arbitrary and does not correspond to the 30-day period applying to corrections* – Related to the issue above is the concern that the initial ban period length is arbitrary and should at least correspond to the 30-day period applying to corrections. This may mean that an individual has time to submit a correction request to a CP and for the CP, in processing that request, to ascertain whether fraud has occurred and whether correction is needed. As above, the length of the ban period is set by the Privacy Act and is therefore out of scope for this review but may be considered as part of the statutory review of Part IIIA of the Privacy Act.²⁶
- *The burden of proof for demonstrating fraud* – To agree to extend a ban period, the CRB must believe on reasonable grounds that the individual has been, or is likely to be, a victim of fraud. The CR Code requires the CRB to notify the individual of what information, if any, the CRB

²⁴ Privacy Act 1988 s 20K.

²⁵ Privacy Act 1988 s 25B.

²⁶ Privacy Act 1988 s 25B.

requires to support the individual's allegation of fraud. This puts the burden of proof on the individual and appears to result in some CRBs asking for a police report number. In cases where identity credentials have been lost, an individual must wait for misuse to occur before preventative measures such as extensions to ban periods may be pursued.

- *Whether the CR Code should require free 'alerting' to the individual during a ban period* – A possible option to support victims of fraud would be for the CR Code to provide for free alerting to the individual during a ban period by the CRB in relation to attempts made to access the individual's credit reporting information.
- *Lack of protection for minors* – CRBs collect and hold credit reporting information about individuals who are 18 years or older. However, some individuals over 18 years of age may not have credit information held about them until they reach their early to mid-twenties when they first apply for credit. This cohort of young people have identity credentials that may be targeted by identity thieves, however because they do not yet have credit reporting information held about them this means that they are unable to request a ban period. This matter may require resolution via updates to Part IIIA.

Questions – Protections for victims of fraud

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?

6.3 Use of credit reporting information for direct marketing

Part IIIA restricts a CRB's use of credit reporting information to facilitate a CP's direct marketing. However, at the request of a CP, a CRB is permitted to undertake pre-screening of a list of individuals provided by the CP using the CP's eligibility requirements. Paragraph 18 of the CR Code contains some additional requirements. In particular, paragraph 18:

- Limits the powers 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
- Prohibits CPs from using eligibility requirements that indicate that the individual has or may have difficulties in meeting repayments under their existing credit arrangement
- Gives individuals the right to ask a CRB not to use credit reporting information about them for direct marketing.

Question – Use of credit reporting information for direct marketing

23. Are the existing direct marketing provisions appropriate? Should they be amended in any way? If yes, how?

6.4 Access rights

Part IIIA requires CRBs and CPs to provide access to credit reporting information about an individual where it has been requested. The CR Code contains additional requirements for access in paragraph 19. In particular, paragraph 19:

- Requires 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
- Requires CRBs to make clear an individual's rights to receive their credit report free of charge in certain circumstances
- Outlines the scope and manner of access required of CRBs and CPs, including that the information be presented clearly and accessibly with supporting explanation
- Clarifies that CRBs and CPs are not required to disclose proprietary data analysis methods or computer programs when responding to access requests.

Possible considerations for how the CR Code deals with access rights include:

- *Whether 'soft enquiries' need to be more clearly accommodated within the CR Code* – This issue concerns the practice of credit reporting information being disclosed to a third party via the access provisions and provided to a CP to enable the CP to indicate to the individual whether they are likely to be eligible for credit with the CP. In these circumstances, the CP collection of credit reporting information circumvents the disclosure and collection provisions for CRBs and CPs contained in Part IIIA and the Code.
- *Whether credit reports should be accessible from all CRBs following a request to any one CRB* – In the same way that an individual may request a ban period with all CRBs through a single CRB, there is a question as to whether the same arrangement should be permitted when accessing credit reports via the access seeker provisions.
- *Whether access provisions should continue to operate during a ban period* – It can be difficult for support services to help individuals experiencing fraud or identity theft because access seeker provisions cease to operate during a ban period. This means the support service is unable to act on the individual's behalf in these circumstances to request access to their credit report. Only the individual is entitled to consent to disclosure during a ban. It is important to note that these arrangements are prescribed by Part IIIA and are therefore out of scope for this review. That said, this matter may be considered in the 2024 review of Part IIIA of the Privacy Act.

Question – Access rights

24. Are the access provisions appropriate? Should the provisions in paragraph 19 be updated in any way? If yes, how?

6.5 Correction of information

Part IIIA gives individuals correction rights, meaning that they may ask a CRB or CP to correct credit-related personal information held about them. If the CRB or CP is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the CRB or CP must take reasonable steps to correct the information. Generally, the correction must occur within 30 days.

The CR Code contains additional requirements for correction in paragraph 20. In particular, paragraph 20:

- Explains the steps a non-participating CP must take if it receives a correction request
- Sets out arrangements for when a CRB or CP must consult another CRB or CP on an access request, including how to meet the 30-day correction period
- Explains steps a CRB or CP must take if it will not be able to resolve an individual's correction request within the 30-day correction period
- Requires a CRB or CP that receives a correction request to act on it as soon as practicable
- Explains the steps a CRB or CP must take to correct information if it determines that the information is incorrect
- Provides for destruction of default information in cases where an overdue payment occurred because of circumstances beyond the individual's control
- Provides for destruction of default information if, at the time of the correction request from the individual, the CP is prevented from recovering the overdue payment by a statute of limitations
- Requires a CRB or CP to notify an individual of its decision about a correction request within 5 days of making the decision
- Sets out what the notice to the individual about the correction decision must contain
- Clarifies that corrections involving update to identification information do not need to be notified to previous recipients unless the individual requests this
- Sets out how a CRB or CP is to notify other CRBs, CPs or AIRs of the correction
- Clarifies that when an individual makes a correction request, the complaint handling provisions do not apply.

Possible considerations for how the CR Code deals with correction rights include:

- *The complexity of correction provisions* – Paragraph 20 may be difficult for some individuals to understand. Lack of understanding may undermine the ability of individuals to advocate for themselves and pursue correction of credit-related personal information.
- *Simplifying the approach to corrections involving multiple instances of incorrect information* – In some cases, particularly those involving economic abuse or fraud, corrections to credit reports may be needed across multiple credit accounts. There is a question about whether and how the CR Code should better provide for this. Current arrangements may result in an individual having to go through a separate correction process for each debt or enquiry incurred during a period of economic abuse or fraud.
- *CRB or CP unwillingness to process correction requests* – Both CRBs and CPs have correction obligations under Part IIIA. This may lead to ambiguity as to who should process a correction request and ultimately result in a CRB or CP referring an individual to another CRB or CP rather than process the correction request itself. This can be difficult in cases of fraud, for example, if a CRB tells the individual they must contact the relevant CPs to correct the information when the individual may have no knowledge of which CPs were involved in fraudulent requests. There is a question about whether the CR Code should be adjusted to address this practice and institute a ‘no wrong door’ approach to corrections.
- *Other circumstances beyond the individual’s control* – The CR Code allows for destruction of default information in cases where an overdue payment occurred because of circumstances beyond the individual’s control. Currently the CR Code gives three examples of such circumstances: natural disasters, bank errors in processing a direct debit or fraud. There is a question as to whether the list should be expanded to include domestic violence.
- *Correction timeframes* – The 30-day timeframe may be too long for individuals seeking approval for credit in order to buy a house or vehicle. Correction timeframes are set by Part IIIA of the Privacy Act and are therefore out of scope for the review. There is a question as to whether the CR Code could be amended to clarify the requirement under Part IIIA to meet the 30-day timeframe, however.

Question – Correction of information

25. Are the correction provisions appropriate? Should the provisions in paragraph 20 be updated in any way? If yes, how?

6.6 Complaint handling

Part IIIA enables an individual to complain either to a CRB or CP about an act that may breach Part IIIA or the CR Code. Under Part IIIA, the complaint must be acknowledged within 7 days and a decision made about the complaint within 30 days. The CR Code contains additional requirements for complaints in paragraph 21. In particular, paragraph 21:

- Binds CRBs and CPs not bound by other industry complaint handling requirements to comply with ISO 10002:2018(E), an international standard containing guidelines for complaints handling

- Requires a CRB to be a member of a recognised external dispute resolution scheme
- Requires a CRB or CP that is consulted by another CRB or CP about a complaint to respond as soon as practicable
- Explains 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
- Outlines notice requirements for a CRB or CP to notify other relevant entities of a complaint.

Question – Complaint handling

26. Are the provisions on complaint handling appropriate? Should the provisions in paragraph 21 be amended in any way? If yes, how?

6.7 Dispute resolution processes for individuals

The avenues available to a person who is aggrieved about the collection and handling of their credit-related personal information (whether in contravention of Part IIIA or the CR Code) and the related obligations on the relevant entities are set out in Part IIIA and the CR Code.

The Privacy Act contains prescriptive requirements for the complaint handling processes of CRBs and CPs. As with other entities bound by the Privacy Act, CRBs and CPs are required to implement practices, procedures or systems to enable the dealing with privacy-related enquiries or complaints.²⁷ In addition, Division 5 of Part IIIA sets out how CRBs and CPs must deal with privacy complaints about credit-related personal information.

CPs must also be part of a recognised external dispute resolution (EDR) scheme, such as the AFCA, to enable disclosure of credit-related personal information (including that relating to a privacy complaint) to CRBs.²⁸

The 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 personal 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.²⁹

The CR Code does not deal with making a privacy complaint to an AIR, nor does Division 5 of Part IIIA, although section 22A(2) of the Privacy Act requires AIRs to have processes and procedures in place to deal with privacy complaints. Further, an AIR may not always be an APP entity for the purposes of

²⁷ *Privacy Act 1988* ss 20B(2) and 21B(2).

²⁸ *Privacy Act 1988* s 21D.

²⁹ *Privacy Act 1988* s 40(1B).

making a privacy complaint under the general provisions of the Privacy Act, as an alternative to the credit-related privacy complaints scheme set out in Division 5 of Part IIIA.

Early views shared for this review indicated that, while designed to make privacy complaints in relation to credit-related personal 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 make it difficult for individuals to engage with the complaint process.

While the operation of Part IIIA is outside the scope of this review, the OAIC is interested in exploring whether or how the CR Code could provide clarity (and a greater sense of accessibility to individuals) around privacy complaints management. Additionally, the OAIC is interested in whether extension of the CR Code to include privacy complaints to AIRs should be explored.

Question – Dispute resolution

27. Are arrangements for dispute resolution appropriate? Should the arrangements be changed in any way? If yes, how?

6.8 Other options to protect individuals affected by domestic abuse

Supporting individuals affected by domestic abuse and helping them resolve their financial affairs can be complex. In April 2021, the Australian Banking Association (ABA) issued an industry guideline on Financial Abuse and Family and Domestic Violence which identifies certain obligations on banks for the reporting of negative credit information and payment arrangements in situations of domestic abuse.

Issues or options to support individuals affected by domestic abuse include:

- *Greater flexibility not to list or to remove negative information* – In practice, it appears that CPs regularly agree to waive a debt or not pursue payment against one account holder due to the debt being incurred in connection with domestic abuse. However, some stakeholders report that CPs often consider they cannot remove a default as they believe this is not permitted under current credit reporting obligations. There is a question about whether it is possible for the CR Code to offer greater flexibility to help resolve financial disputes involving domestic abuse.
- *Customer-based vs account-based reporting* – The credit reporting system takes an account-based approach; however, some have argued that individual-based reporting is preferable as it better supports people affected by domestic abuse. Some stakeholders have pointed out that there are circumstances where one joint borrower should not have been a borrower, should not be liable for payment or should be granted a variation without notice to the other borrower for safety reasons. In their view, an individual-based approach would support this. Currently ARCA's

Data Standards³⁰ provide for reporting on an account basis with each account holder then separately reported using the relevant account identification. This approach is intended to ensure accuracy of reporting and minimise the errors that might otherwise occur in identification of individuals; as matching by account number is less error prone. In cases where it is necessary to report different information to account holders the Data Standards provide for this by allowing an account to be 'split'.

- Other issues that arise in relation to cases of domestic abuse include:
 - security concerns when an individual uses a new address to access a credit report and does not want that address shared with the other account holder
 - burdensome corrections processes to address multiple debts and enquiries on an individual's account requiring separate corrections applications to address each matter of concern
 - problems with access and identification after an individual has fled violence
 - difficulty in removing defaults and negative RHI from a credit report.

Questions – Other options to enhance protections for individuals

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?

³⁰ ARCA has developed the [Australian Credit Reporting Data Standard and Schema](#) which set out standards for reporting credit accounts, and events relating to those accounts, between CPs and CRBs in Australia.

7. Permitted activities of CRBs and CPs

In this section you can find:

- An overview of activities of CRBs and CPs permitted by the CR Code, including provisions that regulate use and disclosure of credit-related personal information
- Questions for stakeholders to seek feedback on these provisions and issues raised

7.1 Information requests

An 'information request' is a request from a CP for credit reporting information from a CRB.

Part IIIA permits a CRB to collect certain information when receiving an information request from a CP, including the type of consumer credit or commercial credit and the amount of credit sought by the individual about whom the request is being made. In addition to this, paragraph 7 of the CR Code specifies that where the amount of credit sought is unknown, the CRB may collect and disclose information to the effect that an unspecified amount of credit is being sought from the CP.

Possible considerations associated with information requests include:

- *Misapprehension regarding information requests* – It appears that credit repairers and similar entities are considering information requests (also known as 'credit enquiries') reported in an individual's credit report as negative and similar to default information. On this basis, those entities seek to have information requests removed. Recently there has been an increase in disputes focused on having CPs remove enquiries even where those enquiries were legitimate. There is a question as to whether the CR Code should be amended to address this issue.

Question – Information requests

30. Is the provision regulating information requests appropriate? Should it be amended in any way? If yes, how?

7.2 Transfer of rights of CP

Part IIIA permits a CP's repayment rights to be transferred to another organisation which becomes the acquirer and is treated as a CP for the purposes of the credit. In addition to this, paragraph 13 of the CR Code:

- Requires both the original CP and the acquirer to notify a relevant CRB of the transfer event and respect certain conditions.

A possible issue for consideration is:

- *Transfer of credit from a fully participating CP to an entity with restricted participation in CCR* – There may be issues with credit transfer provisions in cases where the original CP is a fully participating CP (that has relationships with multiple CRBs and obligations to contribute CCR data) and the acquirer is a debt buyer with limited participation in CCR (that has a relationship with a single CRB and permission to contribute negative credit information only).

Question – Transfer of rights of CP

31. Are the provisions regulating transfer of rights of CP appropriate? Should they be amended in any way? If yes, how?

7.3 Use and disclosure

Part IIIA permits a CRB to disclose credit reporting information to CPs, mortgage insurers and trade insurers but only for certain permitted purposes. Part IIIA also places restrictions and conditions on how CPs and AIRs use and disclose credit information and credit eligibility information. Paragraphs 5.1, 14 and 16 of the CR Code contain some additional requirements.

In relation to CRB use and disclosure, the CR Code:

- Permits collection, use or disclosure of ‘credit ID information’ and ‘capacity information’
- Sets out remedial steps where credit reporting information is disclosed about the incorrect individual
- Requires CRBs to ensure a recipient of credit reporting information is aware of restrictions on use and disclosure contained in Part IIIA, the Regulations and the CR Code
- Permits CRB disclosure of credit reporting information to a CP to enable the CP to help the individual to avoid defaulting as long as certain conditions are met.

In relation to CP and AIR use and disclosure, the CR Code:

- Permits CP and AIR disclosure of ‘credit ID information’ and ‘capacity information’
- Restricts use or disclosure of credit eligibility information and regulated information for targeted marketing activities
- Permits use of information to exclude an individual from receiving direct marketing if the individual is at significant risk of defaulting
- Sets out the required form and content of a notice the CP must give to the individual if the CP refuses the individual's credit application based on credit reporting information.

Question – Use and disclosure

32. Are the provisions regulating use and disclosure appropriate? Should they be amended in any way? If yes, how?

8. Complete list of questions

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. Does the CR Code get the balance right between the protection of privacy on the one hand and use of credit-related personal information on the other? Why or why not?
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?
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?
8. How might the CR Code need to be updated to accommodate other entities?
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 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 provisions related to internal practices and recordkeeping appropriate? Should they be amended in any way? If yes, how?
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?

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 economic abuse or domestic violence?
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 obligations for use and disclosure appropriate? Should any of the provisions applying to use and disclosure be changed? If yes, how?

Glossary

Abbreviation or term	Expansion or definition
ABA	Australian Banking Association
ACL	Australian Credit Licence
AIRs	Affected information recipients; for more information about the meaning of AIR, see section 2.3.3.
ARCA	Australian Retail Credit Association
BNPL	Buy Now Pay Later
CCLI	Consumer Credit liability Information (sometimes referred to as ‘account information’); it includes the following: <ul style="list-style-type: none"> • the name of the provider • whether the provider is a licensee • the type of consumer credit • 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; and that are prescribed by the Regulations • 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
CCR	Comprehensive Credit Reporting
CP	Credit provider
CP derived information	Information received from a CP
CR Code	Credit Reporting Code
CRB	Credit reporting body
CRB derived information	Information received from a CRB
Credit eligibility information	An individual’s credit reporting information and any further information a credit provider derives from an individual’s credit reporting information
Credit information	A type of personal information which includes information: <ul style="list-style-type: none"> • that identifies an individual • about the amount an individual has borrowed • about repayments • about defaults

Credit-related personal information	Credit-related personal information means credit information, credit reporting information, credit eligibility information or regulated information, as applicable in the context
Credit reporting information	An individual's credit report and credit score
IIS	IIS Partners
Information request	A request from a CP for credit reporting information from a CRB
OAIC	Office of the Australian Information Commissioner
Part IIIA	The part of the Privacy Act that contains provisions regulating credit reporting activities.
Pre-screening assessment	An assessment done by a CRB to determine whether or not the individual is eligible to receive the direct marketing communications of the CP
Privacy Act	<i>Privacy Act 1988</i> (Cth)
Regulated information	Regulated information of an AIR means: <ul style="list-style-type: none"> • if the AIR is a mortgage insurer or trade insurer—personal information disclosed to the AIR by a CRB or CP, or • if the AIR is a related body corporate of a CP—credit eligibility information disclosed to the AIR, or • if the AIR assists the CP with processing credit applications or managing credit—credit eligibility information disclosed to the AIR by the CP, or • if the AIR is an entity using the information in the course of purchasing a debt owed or purchasing a stake in the CP—credit eligibility information disclosed to the entity by the CP
Regulations	Privacy Regulations 2013
RHI	Repayment History Information; includes the following: <ul style="list-style-type: none"> • whether or not an 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 the day on which the individual makes that payment.