



Our reference: D2018/003609

Senator Jane Hume
Chair, Senate Standing Committees on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Senator

National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide comments to the Senate Standing Committees on Economics (the Committee) on the National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018 (the Bill) and Explanatory Memorandum (EM). The OAIC also acknowledges the engagement it has had with Treasury staff in the development of this Bill.

The Bill would give effect to the Australian Government's announcement on 2 November 2017 to legislate mandatory comprehensive credit reporting (CCR) to come into effect by 1 July 2018. The OAIC understands that the measures set out in the Bill are intended to allow credit providers that are eligible licensees¹ to obtain a comprehensive view of a consumer's financial situation, enabling a credit provider to meet its responsible lending obligations.² They are also intended to provide consumers with better access to consumer credit and to demonstrate their credit worthiness.³

Robust information handling practices will be essential to ensure the success and sustainability of this initiative. The protections contained in Part IIIA of the *Privacy Act 1988* (Cth) (the Privacy Act), the Privacy (Credit Reporting) Code 2014 (Version 1.2) (the CR Code) and the Privacy Regulation 2013, regulated by the OAIC, provide an important framework for ensuring that risks to personal information are appropriately mitigated.

While the OAIC welcomes that the Bill generally preserves these existing privacy protections,⁴ the mandating of CCR will result in a significantly increased volume of credit information in

¹ An 'eligible licensee' is defined in s 133CN of the Bill.

² EM, para 1.11.

³ EM, para 1.12.

⁴ Sections 133CP, 133CR, 133CU, 133CSm 133CV, and 133ZCK.

the consumer credit reporting system. This will require proactive oversight and accountability for participants in the scheme.

This submission outlines the OAIC's regulatory oversight of the consumer credit reporting system. It also suggests the Committee consider the impact of a potential limitation of privacy protections in the Privacy Act in 133CV(4) of the Bill.

About the Office of the Australian Information Commissioner

The OAIC is an independent Commonwealth statutory agency established by the Australian Parliament through the *Australian Information Commissioner Act 2010* (Cth). The role of the OAIC is to bring together three functions:

- privacy functions through regulating the handling of personal information under the Privacy Act and other legislation
- freedom of information functions, including access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth)
- information management functions, as set out in the *Australian Information Commissioner Act 2010* (Cth).

The integration of these three interrelated functions into one agency provides the OAIC with a unique perspective, as it seeks to balance the right to privacy with broader information policy goals, such as ensuring that data is recognised as a national resource, and that it can be made available for uses in the public interest. The OAIC is a key advisory body on privacy and information management, drawing on our domestic and international networks to shape how organisations and Australian government agencies (APP entities)⁵ harness emerging technologies and data practices to improve the lives of Australians.

Consumer credit reporting and the Privacy Act

The consumer credit reporting provisions in the Privacy Act are intended to facilitate an efficient credit reporting system, while ensuring that the privacy of individuals is respected.⁶ As noted in the EM to the Bill,⁷ Part IIIA of the Privacy Act currently allows for, but does not mandate, comprehensive credit reporting. This followed changes to the Privacy Act in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), commencing in March 2014, which meant that five new types of credit-related personal information could be held in the credit reporting system.⁸ The move to more comprehensive credit reporting was

⁵ APP entities include most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses: *Privacy Act 1988* (Cth), s 6(1).

⁶ The objects of the Privacy Act, in s 2A, include 'to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected.'

⁷ EM, paras 1.26–1.32.

⁸ *Privacy Act 1988* (Cth), s 21D(3)(c)(i). For example, credit providers that hold an Australian credit licence under the *National Consumer Credit Protection Act 2009*, could disclose to a credit reporting body, information about an individual's repayment history. Further information is available in the OAIC's *Privacy business resource 3: credit reporting—what has changed?*,

accompanied by enhanced privacy protections relating to notification, data quality, access and correction, and complaints.⁹

For example, Part IIIA of the Privacy Act and the CR Code outline:

- the types of personal information that credit providers can disclose to a credit reporting body (CRB), for the purpose of that information being included in an individual's credit report (for example, identification information, default information, consumer credit liability information and repayment history information about the individual¹⁰)
- the entities that can handle that information
- the purposes for which that information may be handled
- the circumstances in which credit information may be used and disclosed
- data quality and correction requirements, and
- information security requirements.

Part IIIA and the CR Code also permit individuals, on request, to access their credit reporting information or credit eligibility information from a credit provider or a CRB (some limited exceptions apply). A CRB must give the individual access to their consumer credit report, including information derived from the information in that report, for free once every twelve months, and where the individual has been refused credit or where the request for access relates to a correction request.¹¹

The OAIC is aware of concerns raised by regulated entities and consumers about financial hardship and the consumer credit reporting system and understands that this will be an area of interest to the Committee. Financial hardship is regulated under the *National Consumer Credit Protection Act 2009* (Cth) (the NCCP Act) and the National Credit Code in schedule 1 of the NCCP Act. Concurrently, credit providers have obligations under the Privacy Act in regards to the way they report information about an individual's repayment history to CRBs. To enhance clarity, the OAIC has published guidance about the reporting of RHI and default information in circumstances of financial hardship.¹² The OAIC has also published guidance about the meaning of 'repayment history information' where a consumer credit contract is varied or an arrangement, known to industry as an indulgence, is in place.¹³

available on the OAIC website at <<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-3-credit-reporting-what-has-changed>>.

⁹ The OAIC's consumer-facing resources, outlining the changes to the consumer credit reporting system, are available on the OAIC website at <<https://oaic.gov.au/individuals/privacy-fact-sheets/credit-reporting/>>.

¹⁰ See definition of 'credit information' in s 6N of the Privacy Act.

¹¹ *Privacy Act 1988* (Cth), s 20R(5); Privacy (Credit Reporting) Code 2014, para 19.

¹² See *Privacy fact sheet 34: Repayment history information and your credit report*, available on the OAIC website at <<https://www.oaic.gov.au/individuals/privacy-fact-sheets/credit-reporting/privacy-fact-sheet-34-repayment-history-information-and-your-credit-report>>, and *Privacy fact sheet 38: Hardship assistance and your credit report*, available on the OAIC website at <<https://www.oaic.gov.au/individuals/privacy-fact-sheets/credit-reporting/privacy-fact-sheet-38-hardship-assistance-and-your-credit-report>>.

¹³ <<https://oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/businesses/what-does-the-term-due-and-payable-mean-in-the-definition-of-repayment-history-information>>

As the Committee would be aware, the Australian Government announced a review of the operation of financial hardship arrangements on 28 March 2018, to be led by the Attorney-General's Department.¹⁴ The OAIC will participate in that review.

OAIC oversight of the credit reporting system

The OAIC welcomes that the existing privacy protections under Part IIIA and the CR Code, will generally apply to exchanges of credit information required under the Bill.¹⁵ The OAIC also notes the amendment to s 20Q(3) of the Privacy Act, which would require CRBs to store credit reporting information in Australia, or use a service listed by the Australian Signals Directorate, or in accordance with any CR Code requirements.¹⁶

The protections contained in the Privacy Act and the CR Code, provide an important framework for ensuring that risks to personal information are appropriately mitigated. While the existing privacy framework will help facilitate public trust in this initiative, robust information handling practices will be essential to ensure the success and sustainability of this initiative, given it will result in a significant increase in the volume of information in the consumer credit reporting system.

The Privacy Act confers on the Commissioner a range of privacy regulatory powers. These include powers that allow the OAIC to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred. The OAIC's *Privacy regulatory action policy* outlines the manner in which privacy regulatory activity is undertaken and the circumstances in which information about regulatory activity may be communicated publicly.¹⁷ The OAIC's functions and powers relevantly include:

- developing guidance about the operation of the Privacy Act—such as the *Guide to securing personal information* referred to in the EM¹⁸
- advising regulated entities about the operation of the Privacy Act¹⁹
- conducting assessments (audits) to identify privacy risks and recommend ways to reduce these risks²⁰
- handling enquiries and investigating complaints from individuals about possible interferences with privacy²¹

¹⁴ <<https://www.attorneygeneral.gov.au/Media/Pages/Review-of-financial-hardship-arrangements-28-March-2018.aspx>>

¹⁵ See s 133CZK and Explanatory Memorandum, para 1.20. See also, ss 133CP, 133CR(1)(c), 133CR(3)(c), 133CU(e), 133CS and 133CV.

¹⁶ Item 11 of the Bill.

¹⁷ <<https://oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>>

¹⁸ *Privacy Act 1988* (Cth), s 28. See also EM, para 154.

¹⁹ *Privacy Act 1988* (Cth), s 28B(1).

²⁰ *Privacy Act 1988* (Cth), s 33C.

²¹ *Privacy Act 1988* (Cth), s 36.

- conducting Commissioner initiated investigations (CII) about potential interferences with privacy of an individual²²
- making a public determination in a complaint investigation or a CII and, where necessary, bringing proceedings to enforce the determination²³
- accepting enforceable undertakings and, where necessary, bringing proceedings to enforce these undertakings²⁴
- seeking a civil penalty from the courts in the case of a serious or repeated interference with privacy, or in the case of a breach of certain credit reporting provisions.²⁵

The Bill envisages active oversight by the OAIC, particularly of security issues arising in the mandatory comprehensive credit reporting system. For example, the Bill requires an eligible licensee to provide a notice to the OAIC to engage exceptions to the bulk supply and ongoing supply requirements under ss 133CS and 133CV where the eligible licensee has a reasonable belief that a CRB is not meeting its obligations under s 20Q of the Privacy Act (discussed further below). The OAIC's *Privacy regulatory action policy* indicates how the OAIC may respond to these notices.

An increased volume of credit information in the system will require proactive oversight and accountability for participants in the scheme. To enhance consumer trust in the scheme, it will be important to ensure the OAIC is resourced to exercise its functions to effectively oversee the handling of credit information in the system. This will include, where necessary, taking regulatory action in response to a notice under ss 133CS or 133CV, which may require a rapid response from the OAIC in order to minimise any impacts on the consumer credit reporting system.

Exceptions to the supply requirements in the Bill

Sections 133CS and 133CV, in item 4 of the Bill, provide exceptions to the bulk supply and ongoing supply requirements, where an eligible licensee has a reasonable belief that a CRB is not complying with its security obligations under s 20Q of the Privacy Act. Section 20Q requires a CRB that holds credit reporting information to take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The intent of these provisions of the Bill is to ensure that 'a licensee's ability to have its own security requirements for the information it discloses is not weakened.'²⁶

²² *Privacy Act 1988* (Cth), s 40(2).

²³ *Privacy Act 1988* (Cth), ss 36, 40 and 52.

²⁴ *Privacy Act 1988* (Cth), s 33E.

²⁵ *Privacy Act 1988* (Cth), s 80W.

²⁶ Explanatory Memorandum, para 1.57.

Correction notices under s 21U(2) of the Privacy Act

Section 133CV(4) in the Bill would limit the operation of requirements regarding notices of correction in s 21U(2) of the Privacy Act, where the exception in s 133CV applies,²⁷ unless:

- the reason for the correction was that the information is inaccurate
- the information was inaccurate when earlier supplied to the CRB under the supply requirements of the Bill.

The Privacy Act provides important protections for individuals, in ensuring that decisions about individual's credit worthiness are based on accurate, up-to-date, relevant information.²⁸ Section 21U(1) of the Privacy Act requires a credit provider that holds credit information or credit eligibility information²⁹ about an individual to take reasonable steps to correct that information if the provider is satisfied it is inaccurate, out-of-date, incomplete, irrelevant or misleading. Section 21U(2) generally requires a credit provider to give written notice to certain other recipients (such as CRBs) of the information that has been corrected under s 21U(1). This obligation is intended to ensure that other recipients, such as CRBs, are aware of the correction and can take appropriate action to update their own records—noting that CRBs have similar obligations to correct credit reporting information they hold.³⁰ As recipients of an individual's credit information may be making significant credit related decisions affecting individual (or, in the case of CRBs, providing the information to other recipients who are making such decisions), it is important that any corrections are transmitted quickly and efficiently.³¹

Section 21U(2) of the Privacy Act requires notices of corrections for a number of reasons, including where the credit information or credit eligibility information is inaccurate, out-of-date, incomplete, irrelevant or misleading. The effect of s 133CV(4) appears to be that information held by CRBs may remain out-of-date, incomplete, irrelevant or misleading—representing a potentially significant impact on individuals' expectations of data quality under the Privacy Act. This impact does not appear to be addressed in the Statement of Compatibility with Human Rights in the EM, nor explained in the EM.³²

While the OAIC appreciates the intent of not requiring an eligible licensee to disclose mandatory credit information to a CRB where there may be security risks, we suggest that it would be preferable to achieve this by limiting the mandated supply requirements under the Bill, rather than limiting the correction requirements under the Privacy Act. This would mean that an eligible licensee would not be required to disclose information about individuals under the NCCP Act, while preserving the data quality protections in the Privacy Act—noting

²⁷ That is, where the licensee reasonably believes the CRB is not complying with its security obligations under s 20Q of the Privacy Act and other conditions are satisfied.

²⁸ Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, pp 163, 179–180.

²⁹ See section 6(1) for definition of 'credit eligibility information'.

³⁰ *Privacy Act 1988* (Cth), ss 20S–20U.

³¹ Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, pp 179–180.

³² EM, para 1.118.

that from a consumer's perspective, credit worthiness decisions will still be made based on this information despite security concerns.

If this suggestion is not adopted by the Committee, the OAIC suggests that at a minimum, the EM explain how the impact on individuals' expectations of privacy under s 21U(2) is reasonable, necessary and proportionate measure in light of the intended policy objective. This may then allow the Australian Parliament to assess whether, in the circumstances, a limitation of the correction provision in s 21U of the Privacy Act, is reasonable, necessary and proportionate in the circumstances.

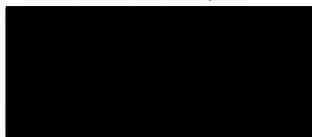
Finally, the basis for exempting CPs from the notice requirement under s 21U(2), but not to the notification requirements under 21W(2)(c) (which follows a correction made at the individual's request), is also not clear to the OAIC.³³ This may be a matter that could be clarified by the Committee.

Obligation to disclose 'payment information' in s 21E of the Privacy Act

Section 21E of the Privacy Act requires a credit provider that has disclosed default information to a CRB, to disclose 'payment information'³⁴ to that CRB if an amount of the overdue payment is paid. In the OAIC's view, a CP would need to continue to disclose payment information to a CRB under s 21E, even if it is not mandated to supply this information under s 133CV. However, to provide additional clarity, it may be useful for the interaction between s 133CV in the Bill and s 21E of the Privacy Act to be explained in the EM.

The OAIC is available to provide further information or assistance to the Committee as required.

Yours sincerely



Angelene Falk
Acting Australian Information Commissioner
Acting Privacy Commissioner

24 April 2018

³³ Section 21V of the Privacy Act enables an individual to request the correction of certain information, including credit information about the individual, and the credit provide must correct that information if the credit provider is satisfied that it is inaccurate, out-of-date, incomplete, irrelevant or misleading. Section 21W sets out the notice requirements that apply where the credit provider corrects, or does not correct, an individual's personal information.

³⁴ *Privacy Act 1988* (Cth), s 6T.