Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au
GPO Box 5218 Sydney NSW 2001
P +61 2 9284 9800 F +61 2 9284 9666
E enquiries@oaic.gov.au
Enquiries 1300 363 992 TTY 1800 620 241
ABN 85 249 230 937

Our reference: D2018/005515

Senator Jane Hume
Chair, Senate Standing Committees on Economics
Parliament of Australia

By email: economics.sen@aph.gov.au

Dear Senator

Response to questions on notice from the public hearing of 15 May 2018

Please find below responses to questions taken on notice at the public hearing of the Senate Economics Legislation Committee on 15 May 2018 for the Committee's Inquiry into the National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018 (the Bill).

1. Enforcement if this legislation was passed

a) If risks were identified during a proactive audit—what powers do you have to make sure the entities address the risks? What happens if an entity does not comply in a timely way, or to the degree that you expect?

The Australian Information Commissioner has a power under s 33C of the *Privacy Act 1988* (the Privacy Act) to conduct an assessment of whether information held by an entity is being maintained and handled in accordance with the credit reporting provisions of Part IIIA of the Privacy Act and the Privacy (Credit Reporting) Code 2014 (Version 1.2) (the CR Code). An assessment may enable the OAIC to identify privacy risks and areas of non-compliance, and may include recommendations as to how an entity might reduce risks or address areas of non-compliance. Following the assessment, the OAIC makes further inquiries of assessed entities, regarding implementation of recommendations in the assessment report.

There may be circumstances where the OAIC considers it appropriate to take further regulatory action as a result of an assessment, such as conducting a Commissioner Initiated Investigation (CII).[1] When deciding whether to take further regulatory action, the OAIC will refer to the OAIC's Privacy regulatory action policy[2] and Guide to privacy regulatory action.[3]

[1] *Privacy Act 1988*, s 40(2)

[2] <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>

[3] <https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/>

A CII may result in the Commissioner accepting an enforceable undertaking from the entity (s 33E) or making an enforceable determination (ss 52, 55A and 62). In the event of serious or repeated interferences with privacy, the Commissioner may also apply to the Federal Court for a civil penalty order of up to $420,000 for individuals, or up to $2.1 million for corporations.[4]

There are also a number of third party audit requirements under the Privacy Act and the CR Code.

Under s 20N(3) of the Privacy Act, a credit reporting body (CRB) must enter into agreements with credit providers (CPs) requiring the CPs to ensure that credit information that they disclose to the CRB is accurate, up-to-date and complete. The CRB must also ensure that regular audits are undertaken by an independent person to determine whether those agreements are being complied with, and identify and deal with suspected breaches of those agreements.

Under s 20Q(3) of the Privacy Act, a CRB must enter into agreements with CPs that require the providers to protect credit reporting information that is disclosed to them by the CRB under this Division from misuse, interference and loss, and from unauthorised access, modification or disclosure. The CRB must also ensure that regular audits are conducted by an independent person to determine whether those agreements are being complied with, and identify and deal with suspected breaches of those agreements.

Paragraph 23 of the CR Code provides further information about the audit requirements in ss 20N(3) and 20Q(3), including requirements to rectify issues identified in the audit, and action that may be taken where a CP fails to meet its contractual obligations to comply with Part IIIA, the Privacy Regulation 2013 (Privacy Regulation) and the CR Code.

Under paragraph 23.11(o) of the CR Code, a CRB must publish on its website annual reports including information about the CRB's monitoring and auditing activity during the reporting period including the number of audits conducted, any systemic issues identified and any action taken in response.

Under paragraph 24.2 of the CR Code, every 3 years, or more frequently if the Commissioner requests, a CRB must commission an independent review of its operations and processes to assess compliance by the CRB with its obligations under Part IIIA, the Privacy Regulation and the CR Code. The CRB must consult with the Commissioner as to the choice of reviewer and scope of the review. The review report and the CRB's response to the review report must be provided to the Commissioner and made publicly available. Independent reviews were conducted on CRBs in accordance with para 24.2 in 2017.

The Commissioner may have regard to information made available under paragraphs 23.11(o) and 24.2 of the CR Code, in considering any regulatory action. When deciding whether to take further regulatory action, the OAIC will refer to the OAIC's Privacy regulatory action policy and Guide to privacy regulatory action.

---

[4] *Privacy Act 1988* (Cth), s 80W.

b) Are there any concerns about limitations you have in proactive enforcement (e.g. legislative limitations) that you would like to mention to this committee in the context of considering the passage of CCR legislation?

To date the OAIC's enforcement powers have been adequate to achieve regulatory objectives.

2. If this legislation was passed and the remaining legislative and regulatory environment stayed the same—can you outline what action credit reporting bodies would have to undertake if there was a suspected data breach?

a) Do they notify you? Any other agencies/regulators?

The Notifiable Data Breaches (NDB) scheme commenced on 22 February 2018 and is designed so that 'eligible data breaches' are notified to affected individuals and the Australian Information Commissioner. An 'eligible data breach' occurs when an entity has reasonable grounds to believe that there was unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.[5]

The NDB scheme extends to CRBs that hold credit reporting information.[6] If a CRB is aware of reasonable grounds to believe that there has been an eligible data breach, it must promptly notify individuals at risk of serious harm and the Commissioner about the eligible data breach.

If a CRB only has reasonable grounds to suspect that there may have been an eligible data breach, it must carry out an assessment of whether there are reasonable grounds to believe that an eligible data breach has occurred. A CRB must take reasonable steps to complete the assessment within 30 calendar days after becoming aware of the grounds that caused it to suspect the eligible data breach.[7]

The NDB scheme does not itself require an entity to notify another agency or regulator of the eligible data breach. A CRB would need to consider separately whether the circumstances of a data breach triggers requirements under other legal obligations to notify other agencies or regulators.

The OAIC has published detailed resources on the operation of the NDB scheme.[8]

b) In what timeframe?

Once a CRB has reasonable grounds to believe an eligible data breach has occurred, they must notify individuals and the OAIC of certain matters as soon as practicable.[9]

---

[5] *Privacy Act 1988* (Cth), s 26WA.

[6] *Privacy Act 1988* (Cth), s 26WE(b).

[7] *Privacy Act 1988 (Cth),* s26WH(2)

[8] Resources are available on the OAIC website for regulated entities <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme> and individuals <https://www.oaic.gov.au/individuals/data-breach-guidance>.

[9] *Privacy Act 1988* (Cth), s 26WK(2) and s 26WL(3).

The Commissioner generally expects entities to notify individuals at risk of serious harm about an eligible data breach expeditiously.[10]

c) What information about the breach is disclosed to you?

When a CRB has reasonable grounds to believe an eligible data breach has occurred, it is required under s 26WK(3) to provide the Commissioner with a statement that includes:

- the identity and contact details of the entity
- a description of the eligible data breach
- the kind or kinds of information involved in the eligible data breach
- what steps the entity recommends that individuals take in response to the eligible data breach.

The CRB must also notify individuals of the contents of the statement.[11]

d) Are the credit providers informed?

The NDB scheme does not specifically require that CRBs notify CPs of eligible data breaches that occur.

e) Is any of this information made public? When? Who makes these decisions?

If it is practical for the CRB to notify all individuals to whom the relevant information relates, or only those individuals at risk of serious harm, the CRB must take such steps as are reasonable in the circumstances to notify those individuals with the contents of the statement.[12]

In the event that it is not practicable for the CRB to notify affected individuals directly about an eligible data breach, the NDB scheme requires that the CRB publish a copy of the statement to the Commissioner on its website, and take reasonable steps to publicise the contents of the statement.[13]

f) What action do you take on notification? Do you carry out an investigation?

The Commissioner acknowledges receipt of all data breach notifications, and assesses notifications for compliance with the NDB scheme. The Commissioner may seek additional information from the reporting entity on containment of the beach and rectification steps. The Commissioner may also open an investigation and considers whether to do so in

---

[10] *Data breach preparation and response—A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* (Data breach preparation and response guide), p 51. Available at <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>.

[11] *Privacy Act 1988* (Cth), s 26WL(2).

[12] *Privacy Act 1988* (Cth), s 26WL(2)(b), (c).

[13] *Privacy Act 1988* (Cth), s 26WL(2)(c).

accordance with the OAIC's Privacy regulatory action policy and Guide to privacy regulatory action.

An individual may also complain to the Commissioner alleging an interference with their privacy by an entity, whether or not they have received a notification that their personal information has been involved in an eligible data breach.[14]

g) How long does the investigation take?

The OAIC handles data breach notifications in accordance with its Privacy Regulatory Action Policy. The OAIC aims to resolve 80% of data breach notifications with 60 days, and to finalise 80% of CIIs within eight months.[15]

For the 2016–17 financial year, the OAIC:

- finalised or escalated to a CII 92% of voluntary data breach notifications within 60 days
- finalised 84% of CIIs within 8 months.[16]

h) Who are the findings presented to? Is any of it made public?

The OAIC has undertaken to publish quarterly statistical information about notifications received under the NDB scheme to assist entities and the public to understand the operation of the scheme.[17]

If the Commissioner opens a CII following receipt of a data breach notification, the OAIC may publish a report of the investigation on its website. When deciding whether to communicate information about a data breach notification or a CII publicly, the OAIC has regard to the communications approach outlined in our Privacy regulatory action policy.

i) What fines/enforcement action could result? What are the maximum penalties? Which agencies other than your own could take action?

The Commissioner has a number of enforcement powers to ensure that entities meet their obligations under the NDB scheme. If the Commissioner becomes aware of an eligible data breach, but the agency or organisation has not undertaken the required notification, the Commissioner can direct the entity to notify individuals and the OAIC.[18]

Additionally, a failure to conduct an assessment of a suspected data breach, to notify individuals or the OAIC about an eligible data breach, or to comply with a direction by the

---

[14] *Privacy Act 1988* (Cth), s 36.

[15] Office of the Australian Information Commissioner Portfolio Budget Statement 2018–19, available on the website of the Attorney-General's Department at <https://www.ag.gov.au/Publications/Budgets/Budget2018-19/Pages/Portfolio-Budget-Statements-2018-19.aspx>.

[16] OAIC Annual Report 2016–17, p 43.

[17] For example, see Notifiable Data Breaches Quarterly Statistics Report January to March 2018 <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#quarterly-statistics>

[18] *Privacy Act 1988* (Cth), s 26WR

Commissioner, is also an interference with an individual's privacy.[19] An individual may make a complaint about an interference with their privacy in relation to their own personal information, or the Commissioner may open an investigation on his or her own initiative.

The Commissioner's other enforcement powers include accepting an enforceable undertaking from the entity (s 33E) and making an enforceable determination (ss 52, 55A and 62). In the event of serious or repeated interference with the privacy of an individual,[20] the OAIC may also apply to the Federal Court for a civil penalty order of up to $420,000 for individuals, or up to $2.1 million for corporations.[21]

As noted above, in deciding whether to exercise enforcement powers in relation to a contravention of the NBD scheme, the Commissioner will have regard to the OAIC's *Privacy regulatory action policy* and *Guide to privacy regulatory action*.

The OAIC is unable to comment on the enforcement powers of other government agencies.

3. Resourcing

a) How many staff do you have currently?

The OAIC has a full-time equivalent staff (FTE) of 74.7 as at 22 March 2018.

b) How many would you say are assigned to privacy compliance in the financial sector?

The OAIC is currently structured into two Branches that work across all three regulatory functions of the OAIC (privacy, freedom of information and information policy). While the OAIC has a number of subject matter experts in relation to the financial sector, any staff may be required to carry out functions in relation to the financial sector from time to time.

In relation to privacy, the Regulation and Strategy Branch assists the Commissioner to carry out their proactive regulatory functions: guidance, monitoring, advice and conducting assessments.[22] As at 22 March 2018, the Regulation and Strategy Branch had 18.21 FTE carrying out these functions in relation to all regulated entities.

The Dispute Resolution Branch as at 22 March 2018 had 21.34 FTE handling privacy complaints, notifiable data breaches, conducting Commissioner initiated inquiries or investigations in relation to all regulated entities.

In addition, the enquiries section of the OAIC had 6.13 FTE as at 22 March 2018, providing phone and email assistance to the public across all the OAIC's functions.

---

[19] *Privacy Act 1988* (Cth), s 13(4A)

[20] *Privacy Act 1988* (Cth), s 13G.

[21] *Privacy Act 1988* (Cth), s 80W(5).

[22] The Commissioner's functions are set out in sections 27, 28, 28A and 28B of the *Privacy Act 1988* (Cth) and assessments are conducted under s 33C of the Privacy Act.

The Communications and Coordination Section of the OAIC had 5.70 FTE as at 22 March 2018, providing media, communications and stakeholder engagement and consultation across all the OAIC's functions.

The OAIC forms project teams typically of 5 staff to develop and implement new programs of work which include subject matter and operational expertise from across the agency, supported by a Senior Executive Service (SES) level sponsor. The OAIC also engages consultants to provide expertise where required. For example, in 2017, the OAIC engaged PricewaterhouseCoopers (PwC) to conduct an independent review of the operation of the CR code, as required under para 24.3 of the CR Code.[23]

c) How does the finance sector stack up against other industries in terms of privacy breaches?

In the 2016–17 financial year, the OAIC received 2,494 privacy complaints.[24] The table below sets out the numbers of complaints across industries for 2016-17.[25] A complaint is an allegation of an interference with the privacy of an individual/s and does not indicate a finding of a breach of privacy.

Sector	Number of complaints
Finance (including superannuation)	364
Health service providers	278
Australian Government	253
Telecommunications	204
Credit Reporting Bodies	147
Retail	129
Utilities	114
Online services	107
Insurance	94
Business/Professional Associations	88

[23] Para 24.3 of the CR Code states 'the Commissioner will initiate an independent review of the operation of this CR Code within 3 years of the date of the commencement of this CR Code.'

[24] OAIC annual report 2016–17, p 18, available on the OAIC website at <https://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201617/>.

[25] OAIC annual report 2016–17, p 62.

In addition, the OAIC has received the following notifications under the NBD scheme in Part IIIC of the Privacy Act, from its commencement on 22 February 2018 until 31 March 2018:[26]

Top 5 industry sectors	NDBs received
Health service providers	15
Legal, Accounting & Management services	10
Finance (incl. superannuation)	8
Education	6
Charities	4

d) What is your estimate of how many FTEs you require to properly carry out all of your responsibilities across the board? (not simply the finance industry)

The OAIC prioritises its discretionary work in accordance with its Privacy regulatory action policy. The OAIC also works to achieve regulatory outcomes that are efficient and effective.

Following confirmation of the OAIC's appropriation in the May 2018 budget, the OAIC is conducting an analysis of future requirements.

e) How many are you planning to assign to managing CCR?

The OAIC forms project teams to develop and implement new programs of work typically of 5 staff which include subject matter and operational expertise from across the agency, supported by an SES level sponsor. The OAIC also engages consultants to provide expertise where required.

The exercise of statutory functions arising from the CCR system would be handled by staff who carry out functions in relation to any entities regulated by the Privacy Act. Discretionary regulatory action will be undertaken in accordance with the OAIC's Privacy regulatory action policy.

Please also refer to the answer to question 3(b).

f) Will these staff be drawn away from other areas if there is no increase in your budget? If so, what work gets dropped?

The OAIC will continue to carry out its statutory functions. The OAIC prioritises its discretionary work in accordance with its regulatory action policies. In relation to privacy complaints made by individuals, the OAIC considers each complaint made in accordance with legislative requirements. The OAIC has adopted a performance measure of finalising 80% of privacy complaints within 12 months.[27]

---

[26] *Notifiable data breaches quarterly statistics report January to March 2018*, available on the OAIC website at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>.

[27] OAIC Corporate Plan 2017-2018, <https://www.oaic.gov.au/about-us/corporate-information/key-documents/corporate-plan-201718#activity-1-4-resolve-privacy-complaints>.

g) Are there any plans from Government to increase your funding so you can manage this new CCR regime? What changes in resourcing resulted from the recent budget?

Plans to increase OAIC funding to manage the CCR regime is a matter for the Government.

In the 2018–19 Budget the OAIC received $13.496 million under Appropriation Bill (No. 1) 2018–19 and $0.860 million under Appropriation Bill (No. 2) 2018-19. This includes $3.639 million to undertake privacy regulatory work for the National Consumer Data Right.

h) Of the staff assigned

How many will be assigned to proactive enforcement work?
How many will be assigned to reactive enforcement work (complaints, enquiries, investigations)?

Please refer to the answer provided to question 3(b) above.

i) Are there any other staffing or resourcing concerns that you would like to mention that are not covered in the questions above?

Please refer to answers to the questions above and evidence provided to the Committee on 15 May 2018.

4. Can you go through your concerns in page 6 & 7 of your submission where you raised concerns about the drafting of provisions that allow credit providers to not disclose mandatory information where there may be security risks?

The OAIC appreciates the importance of taking reasonable steps to ensure credit information is secure, and this is reflected in the requirements of s 20Q of the Privacy Act, which places obligations on CRBs to take reasonable steps to secure credit reporting information[28] as well as the additional requirement in proposed sections 133CS and 133CV of the Bill.

Proposed section 133CV in the Bill provides an exception to the ongoing supply requirements where the licensee reasonably believes that the CRB is not complying with section 20Q of the Privacy Act at a particular time, and certain notification requirements are met.

Proposed section 133CV(4) in the Bill states:

> Subsection 21U(2) of the Privacy Act 1988 does not require a 29 licensee to give a credit reporting body notice of a correction of 30 certain information if:
>
> (a) subsection (1) of this section is providing the licensee with an exception from a requirement under subsection 133CU(1) of this Act; and

[28] Under s 20Q of the privacy Act, if a CRB holds credit reporting information, the body must take reasonable steps to protect the information from misuse, interference and loss and from unauthorised access, modification or disclosure.

(b) that requirement is to supply the corrected information to the credit reporting body;

unless the reason under subsection 21U(1) of the Privacy Act 1988 for the correction is that the information is inaccurate, and it was inaccurate when earlier supplied to the credit reporting body under this Division.

Section 21U(1) of the Privacy Act places obligations on CPs to take reasonable steps to correct credit information that is inaccurate, out-of-date, incomplete, irrelevant or misleading. Section 21U(2) of the Privacy Act provides that where a CP corrects information in this way, it must, with some limited exceptions, notify CRBs to which it has previously given the information about the correction.

An effect of proposed section 133CV(4) of the Bill appears to be that other CPs may obtain information from the relevant CRB that is out-of-date, incomplete, irrelevant or misleading. The OAIC's concern is that CPs may then make credit worthiness decisions on the basis of poor quality information. The quality of credit reporting information is of fundamental importance to individuals, given the significant consequences that may flow, in terms of future access to credit, from an adverse credit report.

As noted in the OAIC's submission to the Committee dated 24 April 2018 and evidence provided to the Committee on 15 May 2018, the OAIC appreciates the intent of not mandating disclosures of credit information where there may be security risks. However, the OAIC suggests this could be achieved by limiting the mandated supply requirements under the Bill, without limiting the correction requirements under the Privacy Act. This would mean that an eligible licensee would not be required to disclose information about individuals as envisaged under the Bill, while preserving the data quality protections in the Privacy Act.

Additional questions from Hansard

1. Hansard page 8

Senator KETTER: Do you have an audit template that we could have a look at? And do you have one ready to go under the new legislation?

Ms Falk: We've got guidance on our website which sets out our guide to conducting what we call assessments under the Act but, for all intents and purposes, are audits. It goes through our methodology in terms of how we identify the audit subject, the kind of document review that we would undertake, the fieldwork that we would undertake and then our reporting process. Of course, I will make that available to the committee.

Response

Chapter 7 of the OAIC's Guide to regulatory action policy outlines the OAIC's approach to conducting assessments under s 33C of the *Privacy Act 1988* (Cth).

2. Hansard page 8

Senator KETTER: Can you tell me briefly the powers that you have to gather information and what the penalties are if an entity doesn't comply?

Ms Falk: At a high level, we have compulsive powers. Section 44 of the Privacy Act allows the commissioner to require information to be provided, and there are consequences for the nonprovision of that information. There's also the ability to search premises, enter premises and so on. In terms of the power to require information, it's a penalty provision if it's not complied with. There is also the ability to conduct compulsory conferences, the power to examine witnesses and so on. In terms of the compulsive powers, there is some limitation on the ability to use those compulsive powers, depending on which function the commissioner is exercising. But that's how they operate at a high level. I'd be very happy to provide the committee with information from our regulatory action policy and guide, which goes through that information and those compulsive powers in more detail if that would assist.

Response

In relation to an investigation arising from a complaint or on the Commissioner's initiative, s 44(1) of the Privacy Act provides that, if the Information Commissioner has reason to believe that a person has information or a document relevant to an investigation, the Commissioner may give to the person a written notice requiring the person:

> (a) to give the information to the Commissioner in writing signed by the person or, in the case of a body corporate, by an officer of the body corporate; or
>
> (b) to produce the document to the Commissioner.

Section 66 of the Privacy Act provides for an offence for refusing or failing, without reasonable excuse, to give information or to answer a question or produce a document or record when so required under the Privacy Act.

In relation to an investigation arising from a complaint from an individual, s 46(1) of the Privacy Act provides that, for the purposes of performing the Commissioner's functions in relation to a complaint, the Commissioner may, by written notice, direct:

> (a) the complainant;
>
> (b) the respondent; and
>
> (c) any other person who, in the opinion of the Commissioner, is likely to be able to provide information relevant to the matter to which the complaint relates or whose presence at the conference is, in the opinion of the Commissioner, likely to assist in connection with the performance of the Commissioner's functions in relation to the complaint;
>
> to attend, at a time and place specified in the notice, a conference presided over by the Commissioner.

Failure to comply with a notice given under s 46(1), or failure to attend such a conference from day to day, is an offence under s 46(2).

Section 68 of the Privacy Act provides that, for the purposes of the performance by the Information Commissioner of his or her functions under the Privacy Act, a person authorised by the Information Commissioner in writing may, at any reasonable time of the day, enter premises occupied by a regulated entity (including a CRB or CP) and inspect any documents that are kept at those premises and that are relevant to the performance of those functions.

Further information about the Commissioner's investigative powers is contained in the OAIC's Privacy regulatory action policy and Guide to privacy regulatory action.

Yours sincerely

Angelene Falk
Acting Australian Information Commissioner
Acting Privacy Commissioner

25 May 2018