Australian Banking Association

24 May 2018

Senator the Hon Chris Ketter
Senate Standing Committee on Economics
Department of the Senate
Parliament House
Canberra ACT 2600
By email: Economics.Sen@aph.gov.au

Dear Senator Ketter

Inquiry into the National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018.

Thank you for providing the Australian Banking Association (ABA) with the written questions on notice.

Our responses follow.

1. Data security

   a) If there is a data breach with one of the credit reporting bodies – will your members who are suppliers of data be notified? When? Under what circumstances?

On 22 February 2018 amendments to the Privacy Act commenced, creating a mandatory Notifiable Data Breaches (NDB) scheme.

Section 26WK of the Privacy Act requires an entity, which would include a credit reporting body (CRB), to do certain things if the data breach is an "eligible data breach".

An "eligible data breach" is defined in s.26WE of the Act. Briefly, if the CRB experienced a data breach i.e. unauthorised access to or unauthorised disclosure of individuals' credit information or loses this information, and this would likely result in serious harm to those individuals, this is an "eligible data breach".

The CRB must, as soon as practicable, prepare a statement about the breach and provide a copy to the Commissioner. The statement must contain recommendations for affected individuals on how they should respond to the data breach. If other entities are affected the statement may identify and set out their contact details.

The ABA is not party to the terms of the individual agreements entered into between member banks and their CRBs.

Generally, the ABA expects banks to have robust agreements with CRBs which confirm the obligations of a CRB under the mandatory NDB scheme, including notifying their credit provider client.

The Office of the Australian Information Commissioner (OAIC) has published comprehensive guidance for industry on their obligations under the mandatory NDB scheme at https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response.

Under ss. 20N and 20Q of the Act, a CRB which collects or holds credit reporting information, must take such steps as are reasonable in the circumstances to protect the information is accurate, up to date and complete, protected from misuse, interference and loss and from unauthorised access, modification or disclosure.

Further, a CRB must enter into agreements with credit providers that require the credit providers to protect credit reporting information that is disclosed to them from the same events and ensure that regular audits are conducted by an independent person to determine whether there is compliance with those agreements and if suspected breaches are identified, to deal with them.

The Bill (if enacted) will add a further requirement to s.20Q that if a CRB holds credit reporting information, the body must store the information in Australia or an external Territory or using a service that is listed by the Australian Signals Directorate of the Defence Department as a Certified Cloud Service under the program known as the Information Security Registered Assessors Program or which meets the conditions specified in the registered CR Code.

b) What regulatory environment are you expecting to enforce this bill?

There was some surprise that the mandatory regime had been brought under the Credit Act since the originating framework for comprehensive credit reporting (CCR) is found in the Privacy Act, and supplemented by regulations and the Privacy (Credit Reporting) Code 2014 (CR Code). This suggests a further regulator, the Australian Securities and Investments Commission (ASIC), will need to familiarise itself with the Privacy Act and its concepts. This will include ensuring there is an alignment of interpretation between the OAIC and ASIC.

The primary regulatory environment is Part IIIC (which the Bill will create) and Part IIIA of the Privacy Act, the regulations and the CR Code. The Bill includes further measures (see below).

a. What do you understand will be ASIC's responsibility?

ASIC regulates and enforces the provisions of the National Consumer Credit Protection Act (NCCP) and the National Credit Code (NCC) which include the financial hardship provisions in the NCC. The provisions of the Australian Securities and Investments Commission Act may also be relevant. Under the Bill, ASIC will have a role with respect to ensuring compliance with the mandatory credit reporting scheme and the auditing requirements.

ASIC will have additional powers under the Bill to regulate the proposed mandatory regime on the large authorised deposit-taking institutions (ADIs). The Bill envisages that the regulations may require a credit provider or a CRB to give ASIC specified information. Under the Bill ASIC's new powers and role can be summarised as a role to:

- Determine the meaning of supply requirements by legislative instrument.
- Approve technical standards for supplying credit information.
- Review notices relating to a CRB's compliance with s.20Q of the Act regarding security requirements.
- Appoint auditors to prepare audit reports required by the Bill.
- Direct a credit provider or CRB to lodge a written statement containing specified information about each provider's compliance with the Bill. This power includes an ability for ASIC to require the provider to provide written statements on a periodic basis. This power includes these written statements to be audited before being given to ASIC.

- Ensure compliance with the mandatory credit reporting scheme and the auditing requirements.

b. What do you understand will be OAIC's responsibility?

OAIC regulates and enforces the credit reporting provisions in Part IIIA of the Act; the mandatory NDB scheme in Part IIIC of the Act, and the CR Code. This will include regulation of CRBs.

The CR Code clarifies aspects of the credit reporting obligations in Part IIIA of the Privacy Act and the Privacy Regulations 2013. It is included on the Codes Register under s.26M of the Privacy Act. For background, the CR Code is a written code of practice about credit reporting, and is an important part of the regulatory framework for the CCR system in Australia introduced by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

We understand the OAIC will continue to regulate the Privacy Act and relevant regulations and Codes, including providing guidance to industry, such as their guidance relating to repayment history information.

c. Do you expect the regulator/s to be auditing the credit reporting bodies for data usage, data privacy etc.? What do you expect the regulators to be doing?

It is expected that OAIC would investigate concerns with the information collection and disclosure by CRBs to credit providers as provided for in the Act, particularly where the OAIC is aware of individuals' complaints or concerns about the information handling of credit reporting information. During the hearing, the Australian Information Commissioner mentioned that her office is reviewing their audit framework because of the proposed introduction of the mandatory CCR regime on the large ADIs.

Under the current framework, the Information Commissioner can request a CRB commission an independent review of its operations and processes to assess compliance by the CRB with its obligations under Part IIIA, the regulations and the CR Code. The Commissioner can request this every 3 years, or more frequently (see paragraph 24 of the CR Code).

The ABA suggests that the OAIC may be better positioned to advise the extent to which audits of CRBs are likely and in what circumstances.

d. Do you expect the regulators to be auditing credit providers as well, including your members? Why/why not? What do you expect them to be looking for?

As stated above, there are requirements under the Act for independent audits to be conducted of credit providers' handling of credit reporting information, including the quality of that information. The current framework is confined to CRBs to conduct audits of credit providers. By contrast, CRBs need to establish a documented risk-based program to monitor a credit provider's compliance with their obligations under Part IIIA, incorporated into agreements with the CRB. Paragraph 23 of the CR Code sets out more details of the intended risk-based program, which includes instructions for how the CRB is to publish the audit results on its website.

c) Westpac said in their submission that they want to see regulations on reciprocity and data exchange to be effective – that credit reporting bodies are governed by the same restrictions that credit providers are subject to – do you anything to add to this comment?

Westpac's submission referred to the Principles of Reciprocity Data Standards (PRDE) which is the governance framework that is meant to operate in a voluntary CCR regime. We note that the PRDE is referenced in the Bill's Explanatory Memorandum in relation to credit providers only. Those ADIs contributing voluntarily will need to adhere to contracts with the CRBs only. The PRDE will need to be clearly referenced in regulations to govern both credit providers and CRBs to ensure that there is not an inadvertent creation of two separate credit reporting frameworks. There should be an alignment of the frameworks i.e. for the voluntary participating ADIs and one for the framework for the mandatory CCR regime. Importantly, the PRDE also incorporates governance to ensure CRBs and credit providers comply with the data standards.

The ABA's members are well placed to make the types of submissions made by Westpac. There is a strong incentive for banks to be satisfied that credit reporting information, which a bank provides to a CRB, is secure and handled in accordance with the law. This is information about a bank's customers which the bank needs to ensure is safe, secure and handled lawfully. This is consistent with a bank's duty of confidentiality owed to its customers.

2. Broader use of data & privacy

a) Between current legislation and this proposed legislation – what safeguards exist about how CCR related data would be handled?

Part IIIA of the Privacy Act sets standards for use or disclosure of credit information by the CRB and the credit provider. The current legislation also sets out additional requirements for CRBs and credit providers to make a "written note" of specified use or disclosure of credit information. A "written note" documents details of the use or disclosure such as date and relevant section of the Privacy Act that authorises the relevant use or disclosure. Some examples of the current legislation include:

- Section 20F regulates in what circumstance a CRB can disclose credit information to a credit provider.
- Section 20G regulates how CRBs can use or disclose credit reporting information for direct marketing purposes. It is worth noting that consumer credit liability information (CCLI) and repayment history information (RHI) are two components of CCR information currently prohibited from such use.
- Section 21G sets the scene for how credit providers can use or disclose credit information.

The Bill, unlike the current legislation, does not go to the level of granular detail of how credit information is to be used or disclosed. The Bill does look to regulate supplies of mandatory or ongoing credit information, including introducing exceptions for a credit provider not to supply mandatory or ongoing credit information if it holds a reasonable belief that the CRB is not complying with s.20Q requirements.

Division 4 of the Bill requires both the bank and the CRB to separately provide audited compliance reports to the Minister. ASIC is empowered to appoint auditors for these purposes.

b) What rules are there around what credit report providers can use the data for?

Credit reporting providers are commonly known as CRBs as used throughout these answers. As CRBs are member organisations of the Australian Retail Credit Association (ARCA), the ABA suggests that ARCA may be better placed to respond to this question.

Provisionally, the ABA can provide an indication from the rules of the Privacy Act relating to CRB's use of credit information as follows:

- Section 20E sets out how a CRB can use or disclose credit reporting information. A CRB is permitted to use credit reporting information in the course of carrying on the body's credit reporting business.
- Section 20F contains a table of permitted CRB disclosures to a credit provider.
- Section 20G contains a list of permitted uses for direct marketing purposes. Note that CCLI and RHI components of CCR information are restricted for this purpose. CRB is also prohibited from using an individual's information for direct marketing purposes if that individual has informed the CRB not to use their information for that purpose.
- Section 20M deals with permitted use or disclosure of de-identified credit reporting information.
- Section 20W deals with retention periods for specific sets of credit information.

A service provided by CRBs to credit providers is known as 'derived credit information', which is permitted under s.20E of the Act by which this information has any bearing on an individual's credit worthiness; and that it is used, has been used or could be used in establishing the individual's eligibility for consumer credit.

This can be used to create a credit score and for other derived information such as the total number of credit enquiries by the individual. Any information derived by a CRB from Credit Information (CI) is defined as Credit Reporting Information in the Act. Restrictions on use and disclosure of this data is consistent with CI.

- As you understand, could credit reporting bodies use the data (even if depersonalised) across its other business elements?

It is possible, as long as CRBs comply with s.20M of the Privacy Act and Privacy (Credit Related Research) Rule 2014. This ruling also stipulates that the CRB will need to publish its management of de-identified information in accordance with s.20B, i.e. in their privacy policy. Therefore, individuals and credit providers would expect that if CRBs disclose de-identified information across their other related entities, that this is specifically disclosed in a CRB's privacy policy. A CRB (as defined in the Act) must have an Australian link (defined in the Act) and a privacy policy documenting its management of credit reporting information.

In relation to credit reporting information, the legislation is very clear that the information cannot be used or disclosed outside of the CRB and outside of its very limited purposes.

Section 20M limits the use of depersonalised information by a CRB for the purposes of credit research. It follows that this depersonalised information cannot be shared outside of the CRB for this purpose.

- Are you concerned that "insights" derived from the combination of data that your members supply could be on-sold to other parties without your knowledge?
  - Will this form part of the contracts your members negotiate with credit reporting bodies?
  - Do you envisage a situation where credit reporting bodies might offer to pay some kind of "royalty" fees to your members who supply the data to make these third party sales acceptable? Would your members ever consider accepting these kinds of arrangements?

The ABA understands that a bank's agreement with the CRB limits the use to which personal information can be put, but expressly permits a CRB to use that information as permitted by the Privacy Act.

As stated above, s.20M restricts the use and disclosure of CI and any information derived from CI (known as Credit Reporting Information if derived by the CRB, and Credit Eligibility Information if derived by the credit provider) to things such as application assessment, collection of overdue payments, helping to prevent the customer from defaulting, and other uses or disclosures as provided in the Commissioner's rules made under s.20M.

Under s.20G pre-screening is limited to using only negative data, and only to assess whether the individual is eligible to receive the communication. De-identified use cases are restricted under s.20M.

These restrictions ensure there is no clear opportunity for CRBs to bulk sell information supplied by the credit provider.

A bank could negotiate provisions in a CRB Service Agreement to prevent a CRB from disclosing insights developed from the bank's supplied data. A consequence of this may be the bank is unable to receive insights created from other banks' supplied data. The result is that if the bank prevented CRBs from deriving insights from data supplied by the bank, this would restrict innovation by CRBs, which would reduce the value to the bank of information from the CRBs.

c) Credit providers & data

- Do you expect some of your smaller members would voluntarily supply data as well if this legislation is passed? How many, and in what timeframe? How will they benefit?

The ABA is advised that a number of banks, other than the four major banks, have projects in train to participate in the CCR regime.

The ABA expects this will occur sooner or once the Government's objective of the reporting of the critical mass of data has been achieved. Please refer also to my evidence at the Committee hearing on 15 May 2018.

- What in your view will be the kind of cost that your members will have to pay to access these reports? (range of pricing is acceptable)

This is a matter about which the ABA has no knowledge or information. This is a commercial in confidence matter for each bank. It would be preferable for this question to be asked of CRBs.

- Under what circumstances could a credit provider request a report on an individual?
  - Only if the individual approaches the member and requests credit?

Under the Privacy Act a credit provider can't request a credit report for a consumer credit related purpose (application for consumer credit), commercial credit related purpose, credit guarantee related purpose, securitisation purpose, mortgage insurance purpose, and a trade insurance purpose. In the case of an application for commercial credit the credit provider is permitted to access a consumer report on the business proprietors' performance of their consumer credit facilities.

  - Could a member pay for a report if the member has had contact with, but not received a request for credit from, an individual?

No. As described above a CRB is prohibited from providing to a credit provider a report except in very limited circumstances.

  - Are there any circumstances where a member of your organisation could purchase a report on an individual with no prior contact of the individual? (if so, could someone conceivably purchase credit reports on everyone in Australia?)

No, as confirmed above.

- Could direct "cold call" marketing occur as a result of this legislation? Under what circumstances?
  - Given "credit scores" developed by credit reporting bodies are a derived number based on CCR data, is it possible that one of your members could request a CRB to contact individuals (e.g. via a mail out) within a given credit score range and invite them to apply for a particular credit product? Can this happen today? Could this happen if the CCR legislation is passed?

Although this can happen today, under the existing pre-screening provisions of the Act, this activity only applies to information generally described as 'negative information'. The Bill will have little impact.

The current framework under the Privacy Act prohibits a CRB from using or disclosing CCLI and RHI for the purposes of direct marketing.

Therefore, members should expect that CRBs will quarantine CCLI and RHI to ensure it is not included in its scoring algorithms. As mentioned above, CRBs are currently prohibited from using CCLI and RHI in its pre-screening activity for direct marketing purposes. Credit providers would seek to obtain such a guarantee from the CRB to satisfy itself before accepting such a service.

The CR Code sets further restrictions on CRBs to use credit reporting information to facilitate direct marketing. For example, CRBs are prohibited from using credit reporting information for the purposes of developing any tool for provision to a credit provider to assist with assessing the likelihood that an individual may accept an invitation to apply for credit or an invitation to apply for a variation of credit.

On the basis of the above, we do not expect direct cold call marketing to be any different to what occurs today.

- Once a report is paid for and received, how is it transmitted? e.g. will it be emailed as a pdf?

Not by email. Generally, a secure data transmission (xml) and/or web access. Access to credit reporting data would be achieved through password protected secure portals which utilise internal credit provider systems and CRB provided software connections.

- Could one of your member organisations store this credit report on their own computer systems? Or are there electronic measures that stop the copying/storage of these reports?

This is possible. The general information protection and use and disclosure requirements under the Privacy Act are understood to continue to apply to this information.

- Can these reports be passed between employees of your member organisations?

Yes but only to those employees authorised to receive the reports. Any use within an entity, or disclosure between entities within the organisation must be logged with the 'written notes' requirements of the Act. Further, the Privacy Act regulates the misuse of customer information.

- Can the data contained in these credit reports be sent on to third parties? If so, under what circumstances?

Sections 21J to 21N contain provisions for disclosure to third parties. In addition, credit providers can disclose de-identified information to third parties. CRB Service Agreements prevent the disclosure by a credit provider of a CRB's intellectual property and commercially sensitive information (for example, credit scores) to competitors.

- Can any derived data (that is, data derived from information contained in credit reports) be sold/sent to third parties? If so, what kinds of information? Under what circumstances?

Any disclosure of derived information is subject to the same restrictions that apply to 'raw' information received from CRBs. Credit providers may use any information in the consumer credit report if it is not prohibited by the Privacy Act. For example, if a credit provider obtained an individual's credit report for a consumer credit related purpose, the credit provider can use any information in the individual's credit report to assess the consumer credit application, or for internal management purposes of the provider that are directly related to the provision or management of consumer credit by the provider.

As indicated above, the current legislation contains strict rules when a credit report may be used by a credit provider. Banks have controls around use and storage of the credit reporting data which are intended to prevent the misuse and unauthorised disclosure of these data.

3. Review

a) Westpac in its submission said that they want to see CCR expanded to all credit providers and for this to be in the review – does you have any comments to add?

The Government is open to including other credit providers at a later date. There appears to be no mechanism to monitor which other credit providers will participate or how quickly this occurs.

As stated above, the ABA is advised that a number of banks, other than the four major banks, have projects in train to participate in the CCR regime. These banks may begin to participate in the CCR regime sooner than when the Government's objective for a critical mass of data has been achieved.

The Bill (in s.133CZL) creates a statutory review provision, with a review to be completed by 1 January 2022. It is open to the parliament to prescribe what should be included in this review.

Yours sincerely

[Signed]

Ian Gilbert
Executive Director, Legal and Regulation