Attorney-General's Department response to written questions on notice

Questions received from Senator Chris Ketter, Deputy Chair of the Economics Legislation Committee as part of the Inquiry into the *National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018*.

1. Use of data

a) What protections / safeguards are in place about how CCR data can be used?

b) If a credit reporting body was to analyse CCR related data and then on-sell anonymised data or other "insights" to third parties (i.e. not CCR data itself, but other data or information derived from the dataset), are there any protections in this legislation or in existing legislation for that kind of activity?

- Would these kind of arrangements need to be disclosed to anyone?
  - E.g. Credit providers who supply the data or regulators?
  - If so, under what circumstances?

- How much thought generally have you given to this issue about how credit reporting bodies could use this CCR data, combine it with other data, and find ways to generate revenue out of it?
- Is there anything stopping a credit reporting body partnering with Google, Facebook and finding legal ways to combine CCR data with other data to help companies improve their marketing for example? What would stop this from happening? Or at the very least, if it does happen, will there be some level of awareness/oversight?

c) Credit providers & data

- Under what circumstances could a credit provider request a report on an individual?
  - Only if the individual approaches the member and requests credit?
  - Could a credit provider pay for a report if the member has had contact with, but not received a request for credit from, a credit provider?
  - Could a credit provider purchase a report with no prior contact of the individual? (if so, could a credit provider purchase credit reports on everyone in Australia?)
  - Could direct "cold call" marketing occur as a result of this legislation? Under what circumstances? What might the outcomes be?
    - Given "credit scores" developed by credit reporting bodies are a derived number based on CCR data, is it possible that a credit provider could request a credit reporting body 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?
  - Could credit providers conceivably store credit reports on their own computer systems? Or are there electronic measures that stop the copying/storage of these reports?
  - Can these reports be passed between employees within credit providers in your opinion? For what purposes?

Attorney-General's Department response to question 1

The *Privacy Act 1988* (**Privacy Act**) sets out the regulatory model for credit reporting information including use and disclosure, de-identification of credit reporting information, using credit reporting information for marketing purposes, and how this information must be protected from unauthorised access or misuse.

Background

Part IIIA of the Privacy Act provides the statutory basis for limitations on how credit reporting information may be used. Credit reporting information means credit information or 'CRB derived information' and broadly extends to any information that has a bearing on an individual's credit worthiness or could be used to establish an individual's eligibility for consumer credit.

The handling of credit reporting information and certain other types of information by credit reporting bodies (**CRBs**) is prescribed by the rules set out in Part IIIA, Division 2. These rules apply specific requirements on how these types of information are handled by CRBs, and as such, apply rather than the Australian Privacy Principles (**APPs**).

In relation to credit information and certain other types of information handled by credit providers, the rules set out in Part IIIA, Division 3 apply in addition to, or instead of, the relevant APP. Where there may be doubt about the relationship, relevant provisions in Division 3 include a subsection setting out how the provision interacts with the APPs (see, for example, subsection 21B(7), or subsection 21C(2)).

Use and disclosure

Use and disclosure by a CRB

Subdivision D of Division 2 of Part IIIA of the Privacy Act specifies how credit information may be used and disclosed by CRBs. Broadly, there is a general prohibition on the use or disclose of this information (subsection 20E(1)), unless an exception applies. CRBs may only use credit reporting information 'in the course of carrying out the CRB's credit reporting business' (or if the use is required or authorised by an Australian law or court/tribunal order, or if the use is prescribed in regulations).

A CRB may not disclose credit reporting information unless the disclosure falls within a permitted CRB disclosure under section 20F of the Privacy Act, the disclosure is to another CRB with an Australian link, or if the disclosure is to an external dispute resolution body or enforcement body (there are further restrictions on this disclosure in subsection 20E(3) of the Privacy Act).

A permitted CRB disclosure is a disclosure to a credit provider, mortgage insurer or trade insurer that falls within a circumstance permissible in the table provided in section 20F. This section includes eight permissible situations where a CRB may disclose an individual's credit reporting information. Situations permissible in the table include examples such as where the credit provider requests the information for a consumer credit related purpose (which is a narrowly defined term) of the provider in relation to the individual. Each of the scenarios relate to a provider's ability to assess an individual's either initial or ongoing ability to meet their obligations under a consumer credit contract.

Use and disclosure by a credit provider

A credit provider may only collect credit information about a person in compliance with the APPs, or via the permitted CRB disclosure mechanism in section 20F. Once the credit provider obtains that information, it is then considered to be 'credit eligibility information'. Credit eligibility information includes both credit reporting

information and information derived by the credit provider about an individual. If the credit provider collects personal information that they are likely to disclose to a CRB, the credit provider must, either at the time, or before the disclosure, notify the individual of the name of contact details of the body to whom the information will be disclosed, together with any other matters specified in the Credit Reporting Code.

Section 21G of the Privacy Act prohibits the credit provider from using or disclosing credit eligibility information unless that use or disclose falls within an exemption. There are limited circumstances in which the credit provider can use credit eligibility information (specified in section 21H) or disclose credit eligibility information (specified in sections 21J-21N).

Using credit reporting information for direct marketing

Section 20G of the Privacy Act sets the restrictions on credit reporting information being used for direct marketing. Subsection 20G(1) provides a general prohibition on CRBs using credit reporting information for the purposes of direct marketing unless an exemption applies.

Broadly, section 20G only allows a CRB to use credit reporting information for direct marketing purposes if the information used does not include consumer credit liability information or repayment history information, and the CRB uses the information to assess whether or not the individual is eligible to receive the direct marketing communications of the credit provider ('pre-screening'). Under subsection 20G(5), an individual may request that a CRB not use their credit reporting information for this purpose.

Where a CRB uses credit reporting information for a pre-screening assessment, the CRB is restricted from providing the credit provider on whose behalf the CRB conducted the assessment, with the results of the assessment. The CRB may only disclose the assessment to an entity with an Australian link who is not the provider for marketing purposes under section 20H. An example of this is where a credit provider wishes to send promotional material to eligible customers. The credit provider may contract a CRB to assess which customers are eligible to receive the offer using criteria specified by the credit provider. The CRB conducts the assessment and then provides that information to the mailing house (being separate from the credit provider), to provide the offer to eligible customers. The CRB must not provide the mailing house with the information of consumers who have notified the CRB that they opt out of having their information used for direct marketing purposes. The CRB must also not inform the credit provider of the results of the assessment. This means the credit provider does not have information on which customers from their original list either received, or did not receive, the offer.

Use of de-identified credit reporting information

Use or disclosure of de-identified credit reporting information is restricted under section 20M of the Privacy Act. Subsection 20M(1) provides a general prohibition that if a CRB de-identifies credit reporting information, the CRB must not use or disclose that information unless an exemption applies.

The only exemption that applies to subsection 20M(1) is specified in subsection 20M(2), which allows a CRB to use or disclose de-identified information if that use or disclosure is for the purposes of conducting research in relation to credit and the CRB complies with rules made by the Australian Information Commissioner.

The Australian Information Commissioner may make rules (under subsections 20M(3) and 20M(4)) that relate to whether or not the research is research in relation to credit, the purposes of conducting the research, consultation about the research, and how the research is conducted. These are the *Privacy (Credit Related Research) Rule 2014* which only allows research to occur in limited circumstances including: assessment,

development or management of new credit services; developing methodologies to combat fraud and money laundering; assisting responsible lending obligations; or any other general benefit to the public.

2. Regulatory Environment

a) What expectations does AGD have in which agencies will be regulating and enforcing the CCR scheme?
    - What does AGD understand OAIC's role to be in terms of regulating and enforcing comprehensive credit reporting?
    - What does AGD understand ASIC's role to be in terms of regulating and enforcing comprehensive credit reporting?
    - Are there any other regulators who have an interest/responsibility that we need to be made aware of?

b) Would it be fair to say that much of the regulation/enforcement will be up to the OAIC?
    - On the proactive enforcement side
        - If this legislation was passed:
    - How frequently would you expect auditing to occur on credit reporting bodies? What about credit providers?
    - What should the OAIC look for? Be specific.
    - Testimony given at the hearing indicated that the OAIC is reliant on third party reports and takes action based on the results of these reports. Has AGD reviewed this arrangement and whether third party reporting sufficiently uncovers privacy non-compliance? What concerns would AGD have about such arrangements, if any?
    - Will things like selling/providing data to third parties who shouldn't be allowed access be included in the type or auditing that you would expect to be carried out?
    - What powers does the OAIC have to gather information? What are the penalties if the entity does not comply, or not comply in a full and timely way with the OAIC? Does AGD believe this is sufficient?
    - If risks were identified – what powers does the OAIC have to make sure that the entities address the risks? What happens if an entity does not comply in a timely way, or to the degree expected? Does AGD believe this is sufficient?
    - Does AGD hold any concerns about limitations the OAIC might 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?
    - On the reactive (breach/non-compliance) side of regulation:
    - Has AGD conducted any review of the OAIC in the regulation of financial data and enforcement of legislative requirements? Does AGD believe the allocation of responsibilities, enforcement powers, resourcing and penalties for the OAIC are sufficient for regulating comprehensive credit reporting?
    - 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?
        - Who would they notify?
        - In what timeframe?
        - Are the credit providers informed?
        - Is any of this information made public? When? Who makes these decisions?
    - What offences could be triggered in the event that, after this legislation was passed, that a credit reporting body was responsible for a data breach leading to CCR data to enter the public domain? What are the maximum penalties that could be applied for each of these offences?

- What is the average range of penalties that have been historically applied?
- Did AGD consider either setting additional offences and penalties or increasing existing penalties for these kinds of breaches? What level/s were considered?

c) Resourcing
   - Do you believe the OAIC's and ASIC's resourcing and powers (number of staff, expertise of staff etc.) is sufficient to enforce this legislation and other existing enforcement requirements?
   - If it turns out to be the case that the regulators are not properly equipped, would AGD agree that a lack of enforcement or looking for non-compliance reduces the value of consumer protections that are written down in legislation? And given it is financial data that is being regulated here, that the stakes are very high?

Attorney-General's Department responses to question 2

The Office of the Australian Information Commissioner (OAIC) and the Australian Securities and Investments Commission (**ASIC**) have joint responsibility for the regulation of mandatory comprehensive credit reporting.

Role of ASIC in mandatory comprehensive credit reporting

Under the proposed legislation, ASIC will be responsible for ensuring that entities required to supply credit reporting information do so within the prescribed timeframe. ASIC will also be responsible for ensuring that CRBs do not do so in a manner that is inconsistent with any regulations made under the proposed legislation. The *National Consumer Credit Protection Act 2009* (**Credit Act**) provides for a range of powers available to assist ASIC in its role in monitoring, enforcement, information-gathering and investigation.

Oversight of ASIC's roles and functions is a matter for the Treasury portfolio.

Role of the OAIC in consumer credit reporting

The OAIC has an existing role in regulating credit reporting through its existing functions of ensuring that CRBs and credit providers comply with their requirements under the Privacy Act (including the credit reporting requirements in Part IIIA). The proposed legislation does not alter the OAIC's existing functions.

The OAIC is an independent statutory body that has powers conferred on it under the *Australian information Commissioner Act 2010* (**AIC Act**), the *Freedom of Information Act 198*2 and the *Privacy Act 1988*. Powers and functions relevant to consumer credit reporting are contained in the Privacy Act. The Privacy Act and the AIC Act confer broad powers on the Commissioner (via the OAIC) in relation to monitoring, investigation and enforcement. Under the Privacy Act, the Commissioner has powers under Division 1, Part V including powers to:

- Conduct investigations (including 'own motion' investigations) (s40)
- Obtain information and documents (s44)
- Examine witnesses (s45)
- Conduct compulsory conferences and require attendance (ss 46-47)
- Refer matters to other relevant authorities (s50)

AGD and OAIC have been consulted through the development of the proposed legislation and AGD considers that the powers conferred on the OAIC are appropriate for the OAIC to be able to effectively regulate the credit reporting sector after the introduction of mandatory comprehensive credit reporting. As a regulatory body

whose functions include regulating government compliance with the Australian Privacy Principles, it is critical to the effectiveness of the OAIC that it is independent in determining how it exercises its roles and functions.

AGD actively engages with the OAIC to ensure that it has appropriate resources to be able to effectively perform its roles and functions.

Security of Information and application of Notifiable Data Breach scheme to CRBs

CRBs are required to protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure (section 20Q of the Privacy Act). A consequential amendment as part of the Mandatory Comprehensive Credit Reporting Bill will introduce additional security requirements on CRBs that they store credit reporting information on either a server physically located in Australia or on a cloud service certified by the Australian Signals Directorate.

Should a CRB experience a data breach, the Notifiable Data Breaches (**NDB**) scheme under Part IIIC of the Privacy Act places requirements on entities specifying how they must respond to a data breach. An entity (including a CRB) is required to notify both the OAIC and affected individuals if the breach is likely to result in serious harm to any of the individuals to whom the information relates. Once the OAIC is notified, they have discretion as to whether regulatory intervention is required and what form that should take.

Whilst noting that not all data breaches would necessarily amount to a contravention of the entities' obligations under the Privacy Act, the OAIC has discretion to investigate whether a contravention of the Privacy Act has occurred and take any regulatory action it considers appropriate. Where an entity either fails to notify the OAIC or affected individuals under the NDB scheme or contravenes a substantive requirement under the Privacy Act, the Information Commissioner has the power to:

- accept and enforce an undertaking from an entity
- make and enforce a determination against an entity, including a determination for an entity to provide compensation, or
- apply to the Federal Court for a civil penalty order in the case of serious or repeated non-compliance, which attracts maximum penalties of $2.1 million for a body corporate.

AGD does not hold information on the monetary value of actions taken pursuant to these powers.

3. Other

a) In the event that one of the credit reporting bodies is sold or becomes insolvent, what happens to the data? Can it be sold?

Attorney-General's Department responses to question 3

As noted in AGD's response to question 1, a CRB is prohibited from disclosing credit reporting information (whether individual information or as part of a larger data-set) unless an exemption applies. Under section 20E of the Privacy Act, the only class of entity to whom a CRB would be able to provide credit reporting information would be another CRB with an Australian link. The second CRB receiving this information would continue to be bound by the restrictions in Part IIIA of the Privacy Act relating to what they can use the information for, and to whom they may disclose that information. This prevents credit reporting information from leaving the credit reporting regulatory framework in the event of a CRB insolvency or bankruptcy.