AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

Senate Standing Committee on Economics
PO Box 6100
Parliament House
Canberra ACT 2600
Via email: economics.sen@aph.gov.au

23 May 2018

Senate Standing Committee on Economics,

Please find enclosed, answers to Questions on Notice from the Australian Retail Credit Association, following the recent Senate Committee hearing into the *National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill*.

If you have any questions about this submission, please feel free to contact me on [redacted] or at [redacted]

Yours sincerely,

[redacted]

Mike Laing
Executive Chairman

Senate Economics Legislation Committee

Inquiry into the National Consumer Credit Protection Amendment

(Mandatory Comprehensive Credit Reporting) Bill 2018

QUESTIONS ON NOTICE

1. Broader use of data & privacy

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

Credit-related information is one of the most strictly regulated forms of personal information under the *Privacy Act*, which imposes strong controls on **what** data may be supplied into the credit reporting system, who may **access** that information, and the **uses** to which that information may be put. These controls extend to both the 'raw data', and to any personal information derived from that data – such as credit scores – by either the credit reporting body or credit provider.

Part IIIA of the *Privacy Act* (Part IIIA), and the *Privacy (Credit Reporting) Code* (CR Code), a legislative instrument made under the Act, set out the safeguards that currently apply to how credit-related information – including CCR data - is handled.

The Bill adds to these protections – particularly around the security of credit reporting information held by credit reporting bodies.

ARCA's submission, in section (2)(iii), to the *Senate Standing Committee on Economics* dated 20 April 2018 details the consumer rights and protections that apply under Part IIIA and the CR Code.

Importantly, in respect of CCR data – which includes consumer credit liability information (CCLI) and repayment history information (RHI) – the law imposes additional safeguards compared to other forms of credit information. For example, RHI may only be reported, accessed or used by a credit provider that holds an Australian Credit Licence (under the *National Consumer Credit Protection Act*). Credit providers, such as phone, gas and electricity companies, are unable to access this information.

Part IIIA also provides consumers clear rights to correct and complain about data that may be wrong. Consumers are given the right to obtain a free copy of their credit report each year from each of the credit reporting bodies.

In respect to data security safeguards, the Privacy Act and CR Code already impose requirements on both credit reporting bodies and credit providers to take reasonable steps to protect credit-related information from misuse, interference and loss, and from unauthorised access, modification or disclosure (see, respectively, section 20Q and section 21S Privacy Act). The law also currently requires credit reporting bodies to ensure that regular audits of credit providers are conducted by an independent person to determine whether credit providers are taking the required actions.

The draft Bill strengthens the data security safeguards under Part IIIA as it will require a more robust level of security at credit reporting bodies than exists currently. The Bill adds a new layer of protection, by amending the Privacy Act to require credit reporting bodies to store comprehensive credit information in Australia or to use a cloud service certified by the Defence Department. Credit providers must be satisfied the credit reporting body meets those new Privacy Act requirements.

b) What purposes is CCR data allowed to be used for?

Legislative framework for the use of CCR data

Credit reporting bodies and credit providers are prohibited from using or disclosing CCR data for any purposes unless **specifically** permitted by the Privacy Act. We explain the structure of the relevant provisions of the Privacy Act in our response to (1)(d).

First, it is important to note that the types of businesses which can access CCR data (and any other credit reporting information) is strictly limited. Permitted businesses include the credit provider, agents of the credit provider assisting with the application for or management of the credit, and businesses involved in securitisation and lender's mortgage insurers. In effect, the Privacy Act only permits businesses that have a genuine connection to the process of issuing and managing credit to access the CCR data. As noted above, a 'credit provider' may include businesses that sell things on credit, such as phone, gas and electricity providers, however those credit providers are not able to access repayment history information.

The Privacy Act **explicitly** provides that real estate agents, general insurers and employers are **not** credit providers, and therefore the businesses cannot access the consumers credit reporting information – including information derived from the credit information, such as credit scores.

The Privacy Act sets out the **situations** in which the credit reporting body may give information to a credit provider (see sections 20E and 20F) and also the **purposes** for which they credit provider may use or disclose that information (see sections 21G and 21GH).

In summary, a credit provider can access and use credit reporting information for the following purposes:

- To assess an application of a borrower (and any associated guarantor)
- To assist with collecting overdue payments
- To assist an individual to avoid defaulting on his or her credit obligations
- For internal management purposes of the credit provider – this would include purposes such as improving the credit provider's risk management and responsible lending processes.

The CCR data (and other credit reporting information) **cannot** be used for marketing purposes – this includes any things such as creating mailing lists, cold calling by either the credit reporting body or credit provider or selling marketing databases to third parties. This extends to information derived from the credit information – such as credit scores.

The situation in Australia is very different to that in the United States, where it is common place for businesses to purchase marketing lists from the credit bureaus.

The Privacy Act permits a limited use of credit reporting information by a credit reporting body to offer a 'pre-screening' service to credit providers. This is a safeguard to ensure that offers of credit are not sent to consumers who, because they already have defaults and other adverse information on their credit report, are unlikely to be approved if they take up the offer and apply for the product. It is important to note that this does **not** involve the use of the credit reporting information as a 'mailing list'. In order to utilise this service, the credit provider must already have a list of consumers to whom it is able to send marketing material under the *Australian Privacy Principles* (APPs). By using this pre-screening service, the marketing offer is simply not sent to the consumers who are screened out and the credit provider does not receive any information about the consumers on the credit provider's marketing list.

In addition, the pre-screening process also provides that:

- The credit reporting body must not use any CCR data in the pre-screening – it is limited to using 'negative only' data (e.g. defaults, bankruptcy information). See subsection 20G(2)(c) Privacy Act.
- The credit provider must not nominate eligibility criteria for the offer that would direct the offer to consumers who may be experiencing financial difficulty – that is, the law **prohibits** credit providers targeting vulnerable consumers with high cost credit offers. See paragraph 18.2 CR Code.
- A consumer may tell a credit reporting body not to use their credit reporting information for this purpose. See subsection 20G(5) Privacy Act.

In-practice use of CCR data by credit providers and consumers

CCR data – being consumer credit liability information and repayment history information – is an extremely powerful source of data to assist with the proper assessment of consumer credit applications. CCLI provides strong incremental value, however RHI provides even more value over-and-above CCLI.

Credit decisioning involves two related concepts. In order to work out the probability that a consumer will not repay a loan, the credit provider looks at both the 'capacity' of the borrower and the 'propensity to repay' of the borrower.

The propensity to repay refers to the innate behavioural characteristics of the borrower which influence whether that borrower is likely to pay back. It is the result of a combination of a number of factors, including capacity, but also other factors such as how a borrower prioritises loan repayments as compared to, for example, discretionary spending. For example, two consumers with almost identical income and expense profiles (i.e. similar capacity) may have very different chances of paying back the loan. Over the years, credit providers have recognised that a consumer's propensity to repay new debt is predicated heavily by the way they have repaid other debts (i.e. repayment history information). It has long been recognised that at an industry level the credit reporting

system plays an important role in minimising the cost of credit defaults which must be recovered from consumers who do repay loans[1].

In addition, the availability of CCR data – both CCLI and RHI – will assist credit providers meet their responsible lending obligations. We note that the introduction of the CCR data sets was an outcome of work undertaken by the Australian Law Reform Commission (ALRC) in producing the report *For Your Information: Australian Privacy Law and Practice,* Report 108, 208. In that report, the ALRC directly tied the expansion of the permitted credit reporting data sets to include CCR –more specifically RHI - on the proviso that lenders be subject to an explicit responsible lending obligation (see, for example, paragraph 55.177 of Report 108).

The way in which CCLI will assist those process is generally understood – that is, the credit report will give credit providers an independent source of truth to help verify the extent of the consumer's existing liabilities.

The availability of RHI also assists credit providers meet their responsible lending obligations. For example, the law requires the credit provider to take reasonable inquiry and verification steps regarding the applicant's income and expenses. If the credit provider takes those steps and the RHI on the consumer's credit report shows that the consumer is up to date, the credit provider can be comfortable that the inquiries and verification are sufficient. However, if the RHI shows that the consumer has been missing payments, then – depending on the extent of the missed payments – the credit provider may be put on notice that despite their 'reasonable' inquiries, there may be something in the borrower's life that is causing them to struggle and the credit provider should make further inquiries. That is, what is 'reasonable' may change if the credit provider can see that the consumer is struggling with their current fixed liabilities. This is known as 'scalability' – which is a key concept under responsible lending (see, for example, RG209.19 in ASIC' Regulatory Guide 209 Credit Licensing: Responsible Lending Conduct)

The availability of RHI is also an important tool for consumers who have previously had poor credit history (e.g. a default or court judgement on their credit report). Traditionally, a default or court judgement has acted as a 'black mark' and has prevented the consumer from obtaining finance from mainstream lenders, even if the defaulted debt has been repaid.

This is because the data over many years has shown that any type of 'black mark' is a very strong indicator that the consumer may not repay new debt. Of course, this does not mean that every consumer with a previous 'black mark' will default on new credit. However, given the nature of credit, it takes a lot of 'good' loans to compensate for one 'bad' loan. In the absence of RHI, credit providers have not had a tool to distinguish

[1] World Bank. 2011. *General principles for credit reporting (English)*. Washington, DC: World Bank. http://documents.worldbank.org/curated/en/662161468147557554/General-principles-for-credit-reporting

between consumers who have had a black mark but are now back-on-track, and those who are likely to have further poor credit history.

The availability of RHI will now provide credit providers with that tool and will open up the potential for consumers with a black mark to re-enter the mainstream credit market much quicker – without having to wait for 5 years for the black mark to fall off their credit report.

c) *Will credit reporting bodies or credit providers be able to use CCR data (even if depersonalised) across other business elements not related to credit assessment? If so, under what circumstances?*

As noted in our response to (1)(b) and expanded upon in (1)(d), credit reporting bodies and credit providers are not permitted to use or disclose CCR data, or personal information that is derived from that data, for any purpose unless specifically permitted by Part IIIA. These purposes are limited to the assessment and management of the particular credit product offered to the consumer, and for internal management purposes such as improving the credit provider's risk management and responsible lending processes.

We address the use and disclosure of de-identified data in our response to (1)(d).

d) *Could either credit reporting bodies or credit providers use depersonalised data, derived data etc. and on-sell or combine this data with other data sources? Is there any legislative or regulatory barrier to prevent credit reporting bodies from legally partnering with Google, Facebook etc. to legally provide "insights" to companies?*

For the purposes of answering this question, ARCA understands that the reference to providing "insights" to companies refers to purposes, such as marketing, which are not connected to the assessment or management of consumer credit. We note that the proper assessment or management of credit may require the disclose of CCR data to external parties. For example, Part IIIA permits disclosures to providers of lender's mortgage insurance to assess the application for insurance.

Use and disclosure (i.e. 'onsale') of derived data

Under the Privacy Act, derived data (e.g. credit-related information that is 'combined' with other information) is subject to all the same restrictions that apply to the raw data. See ARCA's response to (1)(b), above for a description of those restrictions.

Accordingly, the restrictions in the Privacy Act and CR Code would not permit the use or disclosure (i.e. the 'onsale') of derived data by either the credit reporting body or credit provider - we provide further detail below when we explain the terms 'credit reporting information' and 'credit eligibility information'.

We note that a credit reporting body may be part of a group of companies that includes other companies that are involved in the collection, use and disclosure of non-credit related forms of personal information. If that is the case, the data held by the credit

reporting body would need to be ring-fenced and not shared with those other companies. Those other companies would be subject to the APPs in respect of the personal information held by them, which apply generally to the collection, use and disclosure of personal information (other than credit reporting information).

Explanation of 'credit reporting information' and 'credit eligibility information'

The raw data held by a credit reporting body is known as 'credit information' (s6N Privacy Act) – of which CCR data are types. Together, the credit information and any information derived from that credit information by the credit reporting body is known as '**credit reporting information**' (see section 6 Privacy Act).

The legislation then establishes what a credit reporting body may do with 'credit reporting information'. Importantly, section 20E(1) of the Privacy Act states (emphasis added):

> *Prohibition on use or disclosure*
>
> *(1) If a credit reporting body holds **credit reporting information** about an individual, the body must **not use or disclose** the information.*

Part IIIA then lists the specific purposes and circumstances in which the credit reporting body **may use or disclose** the information. That is, unless the law specifically permits the use or disclosure, it is prohibited. This is in contrast to the Privacy Act's treatment of other forms of personal information, which can be used or disclosed in any circumstances provided the individual has given consent (see Principle 6 of the APPs).

Where the credit provider receives 'credit reporting information' from the credit reporting body, that credit reporting information and any information derived from that information by the credit provider is known as '**credit eligibility information**' (see section 6 Privacy Act).

Section 21G (1) of the Privacy Act states (emphasis added):

> *Prohibition on use or disclosure*
>
> *(1) If a credit provider holds **credit eligibility information** about an individual, the provider must **not use or disclose** the information.*

Again, Part IIIA then lists the specific purposes and circumstances in which the credit provider may use or disclose the information.

Use and disclosure (i.e. 'onsale') of de-identified data

The Privacy Act does not generally restrict a business' use of de-identified data.

Part IIIA, however, imposes more strict obligations in respect of credit reporting information than apply to other forms of personal information. In particular, Part IIIA directly restricts a credit reporting body's ability to use deidentified credit reporting information (see section 20M Privacy Act).

Part IIIA only permits the de-identified information to be used for the purposes of conducting research into credit. The Information Commissioner has issued *Privacy (Credit Related Research) Rule 2014* which provide that the de-identified data may only be used for purposes of conducting research in relation to credit, which involves the management and development of credit services, developing fraud, anti-money laundering and counter terrorism tools, assisting responsible lending and other purposes for the general benefit of the public. Again, it is unusual for the law to restrict a company's use of de-identified information in this way and demonstrates the higher standard to which the credit reporting system is held.

e) *Credit providers & data*

- *Will any credit provider be able to purchase credit reports on individuals? If not, which ones will be allowed to access reports? Why will they be given access?*

  A credit provider is not able to purchase a credit report on an individual unless that individual has applied for credit with the credit provider or has an existing credit contract. Where the individual has an existing credit contract, the circumstances in which the credit provider can access their credit report are strictly limited (as set out in ARCA's response to 1(b)).

- *What in your view will be the kind of cost that credit providers will have to pay to access these reports? (range is okay if they don't want to get specific)*

  ARCA is not privy to the commercial pricing terms between credit providers and credit reporting bodies.

- *Under what circumstances could a credit provider request a report on an individual?*

  ARCA notes that its response to 1(a) - (d) address the questions below that relate to the circumstances in which an individual's credit report may be accessed. We have provided additional information below where the question has not been previously addressed.

  - *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?*
    - *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?*

Part IIIA requires a credit provider to take steps to protect credit reporting information held by the credit provider from misuse, interference and loss, and from unauthorised access, modification or disclosure. Credit providers that are authorised deposit-taking institutions will also be subject to the Australian Prudential Regulatory Authority's prudential requirements relating to data security.

In addition, we note also that credit providers are obliged to destroy or de-identify credit eligibility information it holds once it is no longer needed for any purpose for which that information may be used or disclosed by a credit provider (see subsection 21S(2) Privacy Act). This would mean that the credit provider could not simply permit copies of credit reports to be simply stored indefinitely on computer systems.

- *Can these reports be passed between employees within credit providers in your opinion? For what purposes?*

  As noted in our response to 1(a) – (d), the law strictly limits the uses for which credit reporting information, and information derived from that information, can be used. The rules relating to protecting data from misuse, interference and loss, and from unauthorised access, modification or disclosure will also apply to the credit provider's own employees. In the context of APP 11 (which imposes similar obligations to section 21S Privacy Act), the Information Commissioner has stated, "'Unauthorised access' of personal information occurs when personal information that an APP entity holds is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity[4] or independent contractor…" (see APP Guidelines, APP11, www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information).

2. Data security

a) What requirements are placed on credit reporting bodies currently in terms of data security?

A credit reporting body must take reasonable steps to protect credit reporting information from misuse, interference and loss, and from unauthorised access, modification or disclosure – see section 20Q Privacy Act. The Bill enhances those obligations by requiring a more robust level of security at credit reporting bodies than exists currently. The Bill adds a new layer of protection, by amending the Privacy Act to require credit reporting bodies to store comprehensive credit information in Australia or to use a cloud service certified by the Defence Department. Credit providers must be satisfied the credit reporting body meets those new Privacy Act requirements.

ARCA's submission to the *Senate Standing Committee on Economics* dated 20 April 2018 further details, in section (2)(iv), the data security obligations that apply to a credit reporting body – and also outlines, from a practical perspective, the limited security implications of the additional data being introduced to the system as a result of the Bill.

Importantly, we note that credit providers (especially the majors – which as ADI's), are subject to APRA's prudential expectations and will embed data security standards into contracts with their suppliers, including credit reporting bodies.

b) *Do you have independent third party audits of your systems for both data security and proper use of data? Who are these reports given to? To what standards are they conducted against? Who pays for these independent reports? Please provide a recent report – acknowledging that sensitive elements contained in the report can be redacted.*

We note that ARCA is neither a credit provider or credit reporting body and does not hold consumer data, and we do not have access to the audit reports requested.

Section 20Q of the Privacy Act – and expanded upon in paragraph 23 of the CR Code – requires a credit reporting body to include provisions relating to data security in their contracts with a credit provider and also to ensure regular audits are done on the credit provider by an independent person of those obligations.

As noted in (2)(a), as a matter of policy, credit providers (especially the major banks) will embed security standards into contracts with their suppliers, including credit reporting bodies.

c) *What new requirements around auditing and data security will be in this bill?*

In addition to the additional security measures described above, the Bill (in the proposed s133CZC) imposes an obligation on both the banks subject to the mandatory requirements, and the eligible credit reporting bodies to provide an audited report to the Minister in regard to the supply of the mandatory data.

ASIC may also direct the bank or credit reporting body to produce an audit report in relation to compliance with the compliance with the mandatory obligations (see proposed section 133CZG).

d) *If there were to be a data breach at a credit reporting body – assuming this legislation is passed and the rest of the legislative and regulatory framework stays the same – what are the requirements on reporting the breach? When is notification of the breach required? To whom? Is it made public? Who makes this decision? Are there different tiers of breaches that have different approaches? (e.g. are small breaches treated one way, large breaches another?)*

- *What fines/penalties/legal action could result if a breach was to occur?*

The Notifiable Data Breach regime (under Part IIIC of the Privacy Act) came into effect in February of this year. This regime would apply to a credit-related data breach by either the credit reporting body or credit provider.

The regime requires an entity to notify individuals and the Information Commission about a breach if it has reasonable grounds to believe that it has experienced an 'eligible data breach' – this is a breach that is likely to result in serious harm to **any** individual whose personal information is involved in the breach (i.e. the extent of the breach is not relevant provided that there could be serious harm to at least one individual). This must be done as soon as practicable.

If an entity *suspects* that that there has been an eligible data breach, it must undertake reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected.

Penalties for breach

Depending on the circumstances of the breach, the credit reporting body may be subject to penalties under Part IIIA. Examples could include for failing to maintain the security of credit-related information under s20Q or, if there was a breach and the credit reporting body failed to notify individuals affected and the OAIC, for breaching the obligations of the notifiable data breach regime. In each case, this would constitute an 'interference with privacy of an individual' under s13 of the Privacy Act and is subject to penalties. We otherwise suggest that the Office of the Australian Information Commissioner would be best placed to provide detail on the available penalties for data breaches.

e) *What kinds of requirements will credit providers, and particularly the major banks be likely to place on credit reporting bodies through contractual arrangements?*

As noted in ARCA's response to (2)(a) and in our submission dated 20 April 2018, as a matter of policy, credit providers (especially the majors) embed data security standards into contracts with their suppliers, including credit reporting bodies. Contracts are not finalised until these standards are accepted. For ADI lenders, these requirements will be informed by APRA's prudential requirements. However, it is important to note that the effect of the large banks imposing their own security requirements on credit reporting bodies is that the **highest** standard set by the banks becomes the de facto default minimum standard that a credit reporting body must comply with across its whole business.

Chart on the benefits of comprehensive credit reporting for consumers

In response to Senator Ketter's question regarding studies on the benefits of comprehensive credit reporting for consumers, I referred to a chart that summarised some academic research on the subject. I offered and Senator Ketter requested a copy of that chart, which I include below.