Senator Chris Ketter – Questions on notice – illion & Experian Senate Economics Legislation Committee – Inquiry into the National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018

Questions	Response
1. Broader use of data & privacy	
a) Between current legislation and this proposed legislation – what safeguards exist about how CCR data would be handled?	CCR is a dataset that currently exists, as enabled and governed by the amendments to the Privacy Act 1988 that were effective from March 2014. This data will be safeguarded in accordance with this legislative framework and existing industry standards and practices.
b) What purposes is CCR data allowed to be used for?	CCR data is subject to the same permitted uses as all other credit information. These are specifed in Part IIIA of the Privacy Act and, in essence, provides for data to be used for credit assessment for personal credit and the collection of payments that are overdue where they relate to personal credit.
c) Will your companies be able to use CCR data (even if depersonalised) across other business elements?	CCR data (even if depersonalised) is subject to the same permitted (i.e. limited) uses as all other credit information. These are specified in Part IIIA of the Privacy Act.
d) Do you use depersonalised data, derived data etc. (for example, credit scores) and on-sell or combine this data with other data sources? Is there any legislative or regulatory barrier to prevent you from legally partnering with Google, Facebook etc. to legally provide "insights" to companies which in part are based on information obtained from CCR data?	Depersonalised data is used for research in relation to Credit purposes as is permissible under the Privacy Act (s20M). This research will influence the design of products and services we provide to our customers. There are currently no restrictions on who we may engage with as commercial customers but we confirm there are strict limitations in the Privacy Act in relation to how Credit Reporting Information including CCR data is used and with whom it may be shared - this is limited to Credit Providers and Access Seekers where an access seeker is a person/entity assisting an individual to deal with a Credit reporting Body or Credit Provider.
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?	The Bill does not alter the existing Privacy Act in this regard. A credit provider can purchase credit reports from illion if there is a valid contract in place between illion and the credit provider, and the credit provider acknowledges and attests to its compliance with its privacy obligations. Access to illion's credit reports is limited to permissible uses under the Privacy Act.
What in your view will be the kind of cost that credit providers will have to pay to access these reports? (a range is acceptable)	The price per report varies widely. We are aware of some smaller institutions paying other vendors over $10 report; while illion's pricing is commercially sensitive, its average pricing is a fraction of this figure. Australian prices are amongst the highest in the world, given the nascent state of CCR. We expect the increased competition brought about by mandatory CCR to bring the price down significantly and credit providers to have a choice of competing bureaus with similar strengths.

Under what circumstances could a credit provider request a report on an individual?	The Bill does not alter the circumstances in which a credit provider can request a report on an individual. A credit provider can purchase credit reports from illion to assess an application for credit from an individual or to assist an individual avoid defaulting on an existing credit account. A consumer must consent to this access.
• Only if the individual approaches the member and requests credit?	Yes, provided the credit providers make the required disclosures (as specified in the Privacy Act) to the individual about obtaining a credit report.
• 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?	Yes, provided the credit providers has an existing credit relationship with the individual, and the credit provider requests the credit report for a permissible purpose as specified in the Privacy Act. Typically, this scenario will be where the credit provider is accessing credit information for the purpose of collecting overdue payments.
• 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?)	No.
• Could direct "cold call" marketing occur as a result of this legislation? Under what circumstances? What might the outcomes be?	No, this legislation does not alter the strict controls that have been in place since 2014. The Privacy Act specifically prohibits the use of credit reporting information (which includes CCR) for direct marketing purposes. Additionally, the pre-screening provisions in the Privacy Act specificlly prohibit the use of CCR data for permitted prescreening assessments.
o 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?	The Bill does not alter the strict controls that have been in place since 2014. The pre-screening provisions under the Privacy Act do not allow for a credit reporting body to contact individuals for direct marketing purposes. The proposed legislation does not alter this.
• 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?	Yes, as is curently the case, credit providers have record keeping obligations, as well as obligations to safeguard personal information, including credit reports, from misuse and inappropriate access. Additionally, credit providers have obligations under the Privacy Act to provide mechanisms for individuals to access or request corrections to credit information held by the credit provider.
• Can these reports be passed between employees within credit providers in your opinion?	As is already the case, credit providers have obligations to safeguard personal information, including credit reports, from misuse and inappropriate access.
2. Data security	
a) What requirements are placed on your companies currently in terms of data security?	Under the Privacy Act there are stringent requirements for the safeguarding, management, and destruction of personal information, including CCR data. Additionally, our customers regularly assess our information security procedures and practices to confirm they meet their own security requirements. This is undertaken to a very high standard, and evolves as technology and threats evolve.

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.	Yes - link to http://dnb.com.au/independent-review.html. As a credit reporting body, illion is subject to the provisions of the Privacy Act. illion's compliance with its obligations is independently reviewed every three years with full reporting to the Office of the Australian Information Commissioner. This Privacy Act review is conducted by the external auditor. The most recent review was conducted in June 2017. In addition, the audits are also conducted on financial and general security controls annually. A summary of these results can be made available to customers upon request. Our customers also conduct on-site reviews of our security infrastructure.
c) What new requirements will be in this bill?	None.
Illion – you say in your submission that the addition of major banks withholding data on grounds of suspected non-compliance is superfluous – can you explain?	illion already holds substantial personal information from the major banks, and this is already subject to stringents security and use obligations under the Privacy Act. Our submission raised a concern that it was possible that a bank could withhold their CCR data without providing a reason or providing an opportunity for the CRB to address their concerns.
d) If there were to be a data breach at one of your companies – assuming this legislation is passed and the rest of the legislative and regulatory framework stays the same – what are the requirements on your companies to report the breach? When do you report? To whom? Is it made public? Who can make this decision? Are there different tiers of breaches that have different approaches? (e.g. are small breaches treated one way, large breaches another?)	Notifiable Data Breach legislation came into effect on 22 February 2018. This legislation applies to all personally identifiable information including CCR. This legislation introduced a regime whereby breaches are reportable if they reach a prescribed threshold with regards to potential impact on the individuals effected. The obligation under this legislation is to notify both the individuals whose privacy is breached and the Office of the Australian Information Commissioner. The data breach legislation provides that the decision as to whether the breach is notifiable is an internal business decision. The threshold to establish if the breach is notifiable is not based on quantity or volume but instead on the potential impact to the individuals concerned.
What fines/penalties/legal action could result if a breach was to occur?	[from https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/guide-to-oaic-s-privacy-regulatory-action/oaic-regulatory-action-guide-introduction.pdf] As outlined in the Privacy regulatory action policy, the Privacy Act confers a range of enforcement and other regulatory powers on the Commissioner. These are based on an escalation model and include enforceable undertakings, injunctions and obtaing a civil penalty order from a court.
e) Will this data be stored in Australia in each of your companies? Or will it be stored overseas? What regulations are required in each of these instances?	Yes, this CCR data already is and will continue to be stored in Australia. Our data centres are located in Melbourne with DR (Data Recovery) site in Sydney. The collection, holding, use, and disclosure of this data is already governed by the Privacy Act.
f) What kinds of requirements will credit providers, and particularly the major banks be likely to place on your companies through contractual arrangements?	In general we do not believe credit providers will impose additional requirements on credit reporting bodies, given the CCR data is simply an additional data set connected to information that is already shared with credit reporting bodies by credit providers. It is possible however that some banks may impose additional security measures on the bureau as a means of delaying their move to CCR, hence our response to question 2 (c) above.