



12 October 2018

Australian Competition and Consumer Commission
23 Marcus Clarke Street
Canberra ACT 2601

To whom it may concern,

Consultation – Consumer Data Right Rules Framework

As a major Credit Reporting Body in the Australian credit landscape, illion (formerly Dun & Bradstreet Australia and New Zealand) welcomes the opportunity to provide this submission to the Australian Competition and Consumer Commission (ACCC) regarding the Consumer Data Right (CDR) Rules Framework consultation paper.

illion is a strong supporter of the implementation of a CDR in Australia. The CDR will provide substantial benefit to the Australian economy, transforming the way financial services consumers interact with the banking system by providing the ability and tools to safely share data with different lenders, other financial institutions and fintech companies. In doing so, consumers will be able to access the most appropriate and economical financial products to suit individual needs. Likewise, granting access to consumer data will ensure providers will be able to offer innovative products at more competitive rates. illion believes that intermediaries, such as credit reporting bodies, will be critical to the practical implementation of the CDR in Australia, beginning with Open Banking.

We therefore welcome the ACCC's consultation into the proposed CDR Rules Framework, following Treasury's *Review into Open Banking in Australia* with recommendations for the implementation of an Open Banking regime as part of the CDR in Australia.

If there are any questions or concerns arising from this submission, please feel free to contact me at any time at [REDACTED].

Yours sincerely,

A handwritten signature in black ink, appearing to be "Steve Brown", written in a cursive style.

Steve Brown
Director- Bureau Engagement

1. About illion

illion is the leading independent provider of data and analytics products and services across Australasia. The organisation's consumer and commercial credit registries make up a central component of Australia and New Zealand's financial infrastructure and are used to deliver end-to-end customer management solutions to clients. Using extensive credit and commercial databases, we assist banks, other financial services providers and other businesses to make informed credit and risk management decisions, and help consumers access their personal credit information.

We also make this submission on behalf of subsidiary Proviso, the leading aggregator of banking data in Australia, which has recently become part of illion. Proviso will continue to play a key role in the financial ecosystem under Open Banking with products and services for consumers, businesses, fintechs and authorised deposit-taking institutions (ADIs).

Additionally, we make this submission on behalf of Credit Simple, an illion fintech business which assists consumers in accessing their credit score online, with no fees attached. Credit Simple also works with banks, energy companies, insurance providers and telecommunications providers to present consumers with new product offers based on their credit profile.

2. Outline of this Submission

illion is a strong supporter of the Government's initiative to implement the CDR in Australia, and agrees that it will provide consumers with greater control over their own data and the ability to access more competitive deals across different sectors.

We note that the CDR Rules Framework is only one step in a hierarchy of changes required in a multi-tiered regulatory framework to implement the CDR in Australia. This hierarchy will include new legislation to outline the objectives and foundational principles of the CDR; designations made by the Minister to apply the CDR to different sectors, such as Open Banking in the banking sector; consumer data rules set by the ACCC in consultation with the Office of the Australian Information Commissioner (OAIC) to detail the application within each sector; and standards to apply specific and technical detail to give effect to the CDR's application in each sector, such as the Open Banking Standards to be set by the CSIRO's Data61 as a Data Standards Body (DSB).

illion therefore welcomes further in-depth consultation which will undoubtedly be required throughout the coming months to realise the full implementation of the CDR and Open Banking. As such, the present submission will only address specific points in the proposed Rules Framework which are of particular relevance to illion at this stage, or which we believe require further explanation or amendment.

3. Specific Comments on the CDR Rules Framework (Part B)

3.1 General obligations and structure of the rules framework

illion is a strong supporter of the introduction of the CDR in Australia and broadly supports the proposed CDR Rules outlined in the ACCC's consultation paper. The implementation of the CDR will have enormous consumer benefits, ranging from increased control over personal data to greater competition and product innovation in the financial services market.

We envisage that illion will maintain obligations under the CDR regime as an accredited data recipient; Credit Simple will hold obligations as an accredited data recipient; while Proviso will hold obligations as an outsourced service provider and third party data recipient.

3.2 Sharing data with third party recipients

illion supports the proposed rule that an accredited data recipient may only collect and use a consumer's data if it has obtained the consumer's consent, and only in accordance with that consent. Further discussion of consumer consent can be found below at 3.8.

We agree that fees should not be charged by a data holder for the disclosure or use of specified data. illion supports the imposition of fees only in relation to value-added data sets, while the disclosure of regular CDR data should remain free for consumers to transfer and access. Any fees must be fairly set and should not distort the market.

3.3 CDR consumer – who may take advantage of the CDR?

The ACCC has proposed that, under the first version of the CDR Rules, consumers will be able to direct a bank to share their data only if they are a current customer of that bank, and only if they use online banking.

illion is of the view that consumers should be able to share data regardless of their status as a current or former bank customer. In practice, consumers may need to access past data going back several years, for example, when engaging a financial advisor. We submit that it would be contrary to the public interest if people were effectively pushed to remain with a specific lender in order to authorise sharing of their own data. For consumers to experience the full benefits of Open Banking, there should not be restrictions based on where an individual currently banks. However, we acknowledge the issues to be resolved prior to enabling this access, such as the authentication process for former customers and the timeframe over which former customers may seek to share their data. We propose that the Rules allow former customers to access their past banking data for up to 12 months after account closure, and that this available data should cover the 24 months preceding the closure of their account.

Additionally, we propose that the Rules allow offline customers to participate in the CDR regime, in order to ensure all consumers are able to realise the full benefits of Open Banking, regardless of whether consumers use online banking. This is particularly relevant for older Australians.

3.4 Data holder – who is obliged to share data?

The ACCC has proposed that the four major banks will fall within the scope of the initial phase of the CDR Rules, but that related brands will be exempt from the first version. illion supports this proposition, assuming that all bank subsidiaries are brought within the scope of the Rules after 12 months. We also suggest that non-ADI lenders are required to share their data under Open Banking, after a similar timeframe has elapsed.

illion would take this opportunity to stress the value of screenscraping technology, which we believe should not be disallowed under the CDR Rules Framework and should continue to operate in conjunction with Open Banking. Screenscraping is a safe, secure and efficient method for a consumer to gain a clear understanding of their actual financial position. Further clarity must be provided on whether the information technology systems required under the CDR will result in screenscraping becoming non-viable. illion is of the view that screenscraping should continue to operate in parallel to the CDR regime beyond 1 July 2019 as a useful value-adding technique. We envisage it may take some time before all relevant organisations provide access to their customers' data through the published API, and therefore there will be an important role for screenscraping services in the medium term. Until Open Banking can provide an equal level of service to consumers and businesses, we suggest that screenscraping is considered a viable, value-adding technique and not restricted via the CDR Rules Framework.

The ePayments Code, used to regulate consumer electronic payment transactions, could be amended to provide clarity on screenscraping technology and protect consumers who are engaged with businesses using this technology. Following the full implementation of Open Banking, there may still be significant use cases for screenscraping where it can and should coexist with the former. This continued utility may relate to real-time data provision; simplicity of customer onboarding; level and quality of data availability; and provide a redundancy fail-safe, for example, in a period during which an ADI's API is offline. illion believes screenscraping will also provide an important benchmark to assess the performance of Open Banking, at least during its establishment phase.

3.5 Data sets – what data is within scope?

illion agrees with the ACCC's proposition to exclude data which results from "material enhancement by the application of insights, analysis or transformation by the data holder", as per the recommendations of Treasury's *Review into Open Banking in Australia*.¹

We firmly support the ACCC's efforts to implement comprehensive data sharing via the CDR, and would stress the necessity to share *complete* sets of customer data. That is, all legitimate use cases must not be precluded from the scope of CDR data to be shared under the Framework by data holders. To this end, the ACCC's CDR Rules Framework should be set broadly enough to encapsulate different dimensions of all use cases. For example, income and expenditure verification information, if shared by data holders, can be used by a consumer (with the assistance of a comparator) to accurately identify more favourable offers – leading to improved competition between lenders and more innovative offers in the market. It is essential that data holders are not prohibited from sharing these types of use cases, as reduced data transparency will ultimately weaken competition and

¹ Treasury, *Review into Open Banking: giving customers choice, convenience and confidence* (December 2017) pp 38-39.

minimise consumer benefits to be realised via the CDR. We support the ACCC's proposition to postpone the inclusion of identity verification assessment outcomes until reforms are made to anti-money laundering laws, but stress the need to include this data set as soon as practical following reform.

The consumer metadata associated with different transactions should form part of the transaction data to be shared in the first version of the CDR Rules. In addition to metadata such as geolocation and transaction time, we suggest that device type would be a useful metadata set to include. For example, device type information could be used to develop a read service which notifies consumers if an unknown device attempts a transaction. Metadata should be provided in a de-identified format to mitigate against risk of fraud.

illion believes further detail and clarity must be provided regarding how reciprocity arrangements will operate in practice under the CDR Rules. We agree with the ACCC's view that reciprocity raises inherently complex issues, given that the CDR is consumer-focused and is not a simple 'quid pro quo' arrangement between data holders. This issue requires further attention, and is important to ensure all participants have access to shared data. Under present comprehensive credit reporting (CCR) arrangements, reciprocity exists to ensure recipients share data with entities that provide it. In practice, this only ensures that the major four banks are subject to reciprocity principles under CCR. We suggest that reciprocity principles should be developed by the ACCC with a view to creating a customer-centric model whereby the major lenders are required to share data with smaller CDR participants (such as accredited data recipients or third party recipients) with the customer's consent. We suggest this is incorporated into the first version of the rules, and welcome further consultation on the issue of reciprocity.

3.6 Accreditation

illion is broadly supportive of the accreditation process proposals outlined in the consultation paper. We consider that a single, general tier of accreditation should be developed by the ACCC initially, using objective benchmarks to determine whether an applicant is able to manage CDR data in accordance with relevant privacy safeguards. In time, the introduction of lower tiers of accreditation with reduced requirements will facilitate access for other entities to particular types of CDR data, or data with additional restrictions.

We believe that the division between tiers should be based on risk associated with an applicant, the activities undertaken within a designated sector, and any risk attached to specific classes of CDR data. A tiered, risk-based accreditation model is in the consumer's interest and offers greater confidence in the accreditation process overall, and ensures that higher-risk entities will be subject to more robust accreditation standards.

illion is satisfied it will meet the proposed accreditation requirements outlined in the consultation paper. For example, we will meet the requirement to be a 'fit and proper' person to receive CDR data; we have appropriate and proportionate systems in place to meet all requirements under the legislation and standards; we are a member of the Australian Financial Complaints Authority (AFCA); and we hold the appropriate insurance relevant to the management of CDR data.

We do, however, suggest that the consumer data rules concerning accreditation take into consideration existing standards and licences, and specify that previously accredited entities are subject to reduced accreditation requirements under the CDR Rules Framework. For example, the

accreditation process should recognise ACL accreditation whereby a ‘responsible person’ is appointed. Similarly, the accreditation process should acknowledge existing accreditation under the international standard for information security management, ISO27001. This existing standard demonstrates that an organisation has previously developed and implemented effective risk management protocols; data security systems; and compliance practices. The process should also acknowledge prior accreditation under the Information Security Registered Assessors Program (IRAP), recognising an applicant’s system security controls. Finally, it should be noted whether an applicant is an existing provider to a tier 1 financial service provider, having met robust information security standards.

We also emphasise the need to ensure appropriate resources are allocated to the accreditation process; we are aware that international jurisdictions which have implemented a similar regime have experienced a backlog of applications, with unintended detrimental impacts for providers and, ultimately, consumers.

3.7 The Register

illion supports the introduction of a public Register, administered by the ACCC, to disclose all relevant information to consumers.

3.8 Consent

With regard to joint and complex accounts with multiple account holders, illion agrees that all account holders should have the ability to provide their individual consent to share joint data under the CDR regime, or withdraw consent. Clear notification of any changes will be required, and we encourage the ACCC to consider the impacts these arrangements may have on individuals from a non-English speaking background, vulnerable consumers, or those with limited financial literacy.

We agree that customer consent to share or use personal and financial data should be unbundled, informed, freely given, specific, express and obtained in a straightforward manner, with a simple withdrawal process attached. Similarly, data that has been received accidentally should be destroyed in order to prevent unintended consequences from its disclosure, provided its destruction does not contravene an Australian law (excluding the *Privacy Act 1988* or the Australian Privacy Principles (APPs)), or the order of court or tribunal.² Further discussion on the destruction of unsolicited data is found below at 3.13.

Consent permitting the sharing or use of de-identified customer data, however, should be regulated differently. De-identification involves the removal of direct identifiers, the removal of information which could contribute to re-identification, and/or the introduction of safeguards in the data access environment to manage any risk associated with data being re-identified.³ Data analytics businesses use de-identified information to develop an accurate, wholistic understanding of consumer behaviour, patterns, and unmet needs. More broadly, de-identified data is used by companies and governments (through statutory bodies such as the Australian Bureau of Statistics) to understand

² As discussed in Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft and Explanatory Materials.

³ For further information, see Office of the Australian Information Commissioner, *De-identification and the Privacy Act*, <https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act>.

national economic, social and environmental patterns. For example, the NSW Government established the Data Analytics Centre in 2015 to “deliver innovation in service provision and improve outcomes by generating new perspectives on complex problems”.⁴ De-identified data therefore facilitates greater comprehension of the market, leading to improved product design and innovation, resulting in better products and services for the benefit of consumers while protecting the privacy of individuals and organisations. Data-enabled innovation has obvious positive impacts on competition, driving prices down.

Due to the robust security measures required to use and store de-identified data, and the ensuing consumer benefits, we propose that the CDR Rules Framework authorises the storage and use of de-identified data subject to bundled consumer consent. We believe that the consumer must be able to easily decide whether their redundant data is de-identified or destroyed, and that the CDR Rules Framework should not mandate the destruction of redundant data.

illion agrees with the ACCC proposition to make rules which will prohibit the on-selling of data and use of CDR data for direct marketing purposes. However, we recommend that the CDR Rules permit on-selling or marketing if the consumer’s express consent is obtained.

3.9 Authorisation and authentication process

illion agrees with the ACCC’s suggestions in relation to authorisation and authentication processes.

3.10 Providing consumer data to consumers

We consider that consumers should have the ability to make requests for direct disclosure of their CDR data in a timely, efficient and convenient way, and that consumers should be able to nominate specific CDR data as part of their request.

3.11 Making generic product data generally available

illion agrees with the ACCC’s suggestions in relation to rules that will require data holders to make generic product data available via an API, according to standards set by the DSB.

3.12 Use of data

The ACCC proposes to make rules requiring accredited data recipients to identify to a consumer the uses for which their data can be put, with their express consent. Similarly, the ACCC proposes to make rules to facilitate the transfer of data from accredited data recipients to non-accredited entities if directed to by a consumer, and rules to permit an accredited data recipient to disclose data to an outsourced service provider if the outsourcing arrangement is disclosed to the consumer during the consent process.

illion supports the above proposals, however, would suggest that once a consumer has provided their consent for an accredited data recipient to de-identify their data, further consent should no

⁴ See NSW Treasury, *Data Analytics Centre*, <https://www.treasury.nsw.gov.au/projects-initiatives/data-analytics-centre>.

longer be required under the CDR Rules. Once consumer data is fully de-identified, there are no privacy concerns attached to its use or analysis and for this reason the consumer should not be required to provide their consent following the de-identification process.

3.13 Rules in relation to privacy safeguards

Measures outlined by the ACCC provide robust security protections with respect to the collection, use and disclosure of CDR data. In particular, illion strongly supports the prohibition of the use of a pseudonym by a consumer in Open Banking (Privacy Safeguard 2), noting the increased risk of identification fraud.

Privacy Safeguard 4 seeks to ensure that any CDR data received in the absence of solicitation must be destroyed, unless an Australian law (excluding the *Privacy Act 1988* or APPs), or the order of a court or a tribunal, requires the recipient to preserve the data. The ACCC has acknowledged that in the case of an intermediary model, an accredited intermediary will receive data on behalf of an ultimate accredited recipient, despite not having solicited the data originally. The intermediary may be required to retain the data for a period in this situation. illion suggests that the CDR Rules are framed in such a way to allow flexibility and exceptions for this scenario, so that CDR data received by an intermediary in the absence of solicitation is not subject to Privacy Safeguard 4, provided that an accredited data recipient is the ultimate recipient.

3.14 Reporting and record keeping

illion agrees with the ACCC's suggestions in relation to reporting and record keeping.

3.15 Dispute resolution

illion agrees with the ACCC's suggestions in relation to dispute resolution processes.

3.16 Data Standards Body

illion agrees with the ACCC's suggestions in relation to the DSB.