illion
Formerly Dun & Bradstreet

7 September 2018

Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

Dear Mr McAuliffe,

Consultation – Exposure Draft: Treasury Laws Amendment (Consumer Data Right) Bill 2018

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 Treasury regarding the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (the Exposure Draft).

illion is a strong supporter of the implementation of a Consumer Data Right (CDR) in Australia. The CDR framework will provide substantial benefit to financial services consumers, transforming the way they 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 Treasury's consultation into the Exposure Draft, following the release of the *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 steven.brown@illion.com.au.

Yours sincerely,

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).

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 Exposure Draft is only the initial 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 Australian Competition and Consumer Commission (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.

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

3. Specific Comments on the Draft Exposure Materials

Scope of CDR Data

There is considerable emphasis in the explanatory materials on the broad application and inherent flexibility of the CDR framework. The Exposure Draft defines CDR data as information "specified in, or … within a class of information specified in, an instrument designating a sector" or information "wholly or partly derived" from this original class of information.[1] This inclusive definition has a cascading effect in practice, whereby value-added data sets may be caught within the scope of the legislation. A practical example of this may be a behavioural score that is assigned to a consumer by a credit provider for the purpose of more effectively managing their account.

illion would caution against the inclusion of value-added data sets or aggregated data sets from the scope of the CDR framework. As a data insights and analytics business, illion produces complete and actionable business information from raw data, to assist businesses such as major lenders to provide suitable customer outcomes and mitigate risk. Access to quality data forms the foundation of our continued success in this role. However, continued innovation and investment in data analytics depends on the existence of commercial incentives and we therefore consider that value-added customer data sets and aggregated data sets should be excluded from the CDR framework scope and within the consumer data rules.

Accreditation Process

Under the proposed framework, a Data Recipient Accreditor (initially the ACCC) will be responsible for the accreditation of entities to the CDR system.[2] The explanatory materials specify that accreditation will be based on criteria established in the consumer data rules, to provide flexibility across different sectors.[3] illion supports the proposal to permit accreditation under a tiered risk-based model, which we understand will consider the activities undertaken within a designated sector, any risk attached to specific applicants, and any risk attached to specified classes of CDR data.[4]

This framework will minimise barriers to entry for accreditation applicants, while ensuring that higher-risk entities or entities undertaking higher-risk activities will be required to meet a more robust accreditation standard. A tiered risk-based accreditation model is therefore in the consumer's interest and offers greater confidence in the accreditation process. It also delivers sufficiently stringent controls to ensure customer protections around data security. As a leading provider of data analytics services, illion maintains a robust approach to privacy and security concerns, in accordance with relevant legislation, standards and technologies.

Under the accreditation model, however, we suggest that the consumer data rules concerning accreditation take into consideration existing standards and licences, and that previously accredited entities are subject to reduced accreditation requirements under the CDR framework. For example, the accreditation process should recognise ACL accreditation whereby a 'responsible person' is

[1] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Sch 1, item 1, s 56AF(1)-(3).
[2] Ibid Sch 1, item 1, s 56CE.
[3] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Explanatory Materials p 16.
[4] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Sch 1, item 1, s 56BF(1).

appointed. Similarly, the accreditation process should recognise existing accreditation under the international standard for information security management, ISO27001. This existing standard demonstrates that an organisation has already developed and implemented effective risk management protocols; data security systems; and compliance practices.

We agree that this flexibility will suitably manage the risks associated with a third party holding consumer data. However, illion would stress the requirement for in-depth stakeholder consultation on a sector-by-sector basis by the ACCC prior to the setting of accreditation criteria in the consumer data rules, to ensure that individual sectors of the economy have the opportunity to provide input and tailor the rules to accommodate the features, interests and limitations across different sectors.

Reciprocal Obligations

Under the proposed framework, the ACCC is empowered to specify different rules relating to different classes of CDR system participants across different sectors, including how participants can disclose, share and use data.[5] illion supports the comprehensive sharing of data relating to wide-ranging categories of product information, including transaction data and product type (such as interest rates or loan terms). We highlight the need to ensure reciprocal sharing of data, so that all accredited data recipients are required to share transaction data in compliance with a customer's direction under the CDR framework.

The Future of Screenscraping Technology beyond 1 July 2019

Screenscraping technology is an important data transfer tool that has been used consistently to deliver substantial value to consumers and data holders across the entire financial services industry. Screenscraping delivers a number of benefits to the consumer. For example, it enables consumers to conveniently provide their identity to others when applying for a financial product; it provides a more complete view of a consumer's finances by assimilating multiple products into a single interface; and enables a greater understanding of the individual's previous repayment behaviour over a given period. The technology also enables lenders to better understand prospective customers and thereby adhere to their responsible lending obligations under the *National Consumer Credit Protection Act 2009* (Cth). This, in turn, allows a greater pool of consumers to access appropriate credit, given the increased visibility lenders have via screenscraping. Other market participants also rely on this form of technology to offer their services (predominately in the fintech industry and data aggregation services). We firmly believe that consumers must continue to have a right to share their data in this way

illion is of the view that screenscraping should not be disallowed under the CDR framework, and should continue to operate in conjunction with Open Banking - as acknowledged in the Farrell Report, "banning [screenscraping] would remove an important market-based check on the design of Open Banking."[6] Banks, conversely, should not have the ability to block screenscraping. Through our subsidiary Proviso, illion provides access to over 150 financial institutions transactional information. We envisage it may take some period before all of these organisations provide access to their

[5] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Sch 1, item 1, s 56BC.
[6] Scott Farrell, Review into Open Banking (December 2017) https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf p 84.

customers' data through the published API and therefore there will be an important role for screenscraping services in the medium term.

The explanatory materials state that consumers, data holders and accredited entities are the three key participants in the CDR framework. However, it also acknowledges that "the system is flexible and may also provide … for interactions between consumers and non-accredited entities."[7] The Exposure Draft further specifies that consumers will be able to direct their CDR data to be provided to a non-accredited entity.[8] illion does not take issue with this. However, material published by Treasury in May 2018 states that "[t]he information technology systems required under the [CDR] will block non-accredited entities from accessing data."[9] It remains unclear whether screenscraping technology will continue to be permitted under the proposed CDR framework.

The Farrell Report did not form a specific recommendation on screenscraping practices, instead concluding that "Open Banking should not prohibit or endorse 'screenscraping', but should aim to make this practice redundant by facilitating a more efficient data transfer mechanism."[10] We are concerned around the lack of clarity on this point, and are seeking further information on whether this technology would continue to operate in practice. Specifically, we are seeking further clarity 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 framework beyond 1 July 2019 as a useful value-adding technique.

We suggest that 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.

CDR Privacy Framework

The privacy safeguards outlined in the Exposure Draft and explanatory materials reflect the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Cth), yet also encompass business data rather than only that of individuals. The Exposure Draft also creates a lower threshold for information protected under the privacy safeguards than information covered under the APPs, by specifying that relevant information must "relate" to an individual, whereas information must be "about" the individual under the APPs.

These measures provide robust security measures with respect to the collection, use and disclosure of CDR data. Noting that further detail will be provided in the consumer data rules, illion does not take issue with the majority of privacy measures presently outlined in the Exposure Draft. However,

[7] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Explanatory Materials p 9.
[8] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Sch 1, item 1, s 56BC.
[9] Treasury, *Consumer Data Right Booklet* (May 2018) https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf p 8.
[10] Scott Farrell, *Review into Open Banking* (December 2017) https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf p x.

we are seeking clarification on the application of Safeguard 2 (Anonymity and pseudonymity) and Safeguard 4 (Dealing with unsolicited CDR data).

CDR Privacy Safeguard 2 (Anonymity and pseudonymity)

The explanatory materials state that, while a consumer will be able to utilise a pseudonym in relation to their CDR data, "it is expected that the ACCC will make consumer data rules which prohibit the use of a pseudonym for [the banking] sector."[11] illion fully supports this position. We consider pseudonymity in the banking sector to increase the risk of identification fraud and consequently support the provision not to allow consumers to conceal their identity.

CDR Privacy Safeguard 4 (Dealing with unsolicited CDR data)

We understand that 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* or APPs), or the order of a court or a tribunal, requires the recipient to preserve the data. illion is supportive of this measure but requests further clarification regarding how it applies to the role of an intermediary such as Proviso.

Interpretation

illion understands the term 'unsolicited' to simply include material that has been accidentally received by an entity. illion has no objection to the destruction of such data in order to ensure no unintended consequences result from accidental transfer, and fully supports Safeguard 4 according to this second interpretation.

The term 'solicits' is defined in the *Privacy Act* as follows:

> an entity solicits personal information if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.[12]

'Unsolicited', however, is not defined in the *Privacy Act.* The Office of the Australian Information Commissioner (OAIC) has provided some guidance on the interpretation of 'unsolicited' in a privacy context. The OAIC considers that "unsolicited personal information is personal information that an APP entity receives but has taken no active steps to collect."[13] The following examples are provided:

- misdirected mail received by an entity
- correspondence to Ministers and Government departments from members of the community, or other unsolicited correspondence to an entity
- a petition sent to an entity that contains names and addresses
- an employment application sent to an entity on an individual's own initiative and not in response to an advertised vacancy

[11] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Explanatory Materials p 36.
[12] *Privacy Act 1988* (Cth) s 6(1).
[13] Office of the Australian Information Commissioner, *Chapter 4: APP 4 — Dealing with unsolicited personal information* v 1.0 (February 2014) https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information#unsolicited-personal-information.

- a promotional flyer containing personal information, sent to an entity by an individual promoting the individual's business or services.[14]

Under this interpretation, 'unsolicited CDR data' simply refers to data which an entity has taken no active steps to collect. We support this safety measure according to this interpretation. However, to ensure clarity on this point, we are seeking further understanding of the definition of 'unsolicited CDR data' and suggest that a clear definition is provided for in the final draft of the Bill.

CDR Fees

The explanatory materials state that "[t]he consumer data rules may also establish that a fee is payable in relation to the disclosure of certain class or classes of information under the CDR."[15] 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 access. Any fees must be fairly set and not distort the market.

[14] Office of the Australian Information Commissioner, *Chapter 4: APP 4 — Dealing with unsolicited personal information* v 1.0 (February 2014) https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information#unsolicited-personal-information.
[15] Treasury Laws Amendment (Consumer Data Right) Bill 2018, Exposure Draft Explanatory Materials p 21.