5 April 2019

Australian Securities and Investments Commission
By email: ePaymentsCode@asic.gov.au

To whom it may concern,

Consultation Paper 310 – Review of the ePayments Code: Scope of the review

illion (formerly Dun & Bradstreet Australia and New Zealand) welcomes the opportunity to provide this submission to the Australian Securities and Investments Commission (ASIC) regarding the scope of its upcoming review of the ePayments Code (the Code).

As noted in Consultation Paper 310 (CP 310), the review aims to assess the Code's fitness for purpose in light of recent financial technological innovation and digital technology uptake since ASIC's previous review was undertaken in December 2010. This submission will focus on one specific aspect of the Code that requires updating when considering these technological developments and changes in consumer behaviour.

Digital Data Capture (DDC), often referred to as 'screen scraping', is the process whereby a consumer directs a trusted third party service to retrieve their data as displayed in a web application. DDC is used widely in the financial services sector by lenders, financial management applications, personal finance dashboards, and accounting products to retrieve customer data. It is a critical mechanism to empower consumers and facilitate competition in provision of consumer credit.

At present, the Code does not provide clear guidance in relation to pass code security requirements and in the circumstance of a customer knowingly providing their account logon details to a third party, such as a data aggregator. illion recommends that ASIC's review of the Code includes clarification on this point.

This submission will begin by providing an overview of illion's business and subsequently discuss the need for clarification on pass code security requirements within the Code. We will also outline the important role DDC technology is currently playing, and will continue to serve at least into the medium-term as the new Open Banking regime is established and implemented.

We note that CP 310 represents only the initial step in the development of an updated ePayments Code, and we look forward to closely engaging with ASIC throughout this process over the coming months. If there are any questions or concerns arising from this submission, please feel free to contact me at any time

Yours sincerely,

Steve Brown
Director - Bureau Engagement

1. About illion

illion is a data and analytics business, operating in Australia since 1887. 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. Our data assets, combined with our end-to-end product portfolio and proprietary analytics capabilities, enable us to deliver trusted insights to our customers and facilitate confident and accurate decision making.

illion is highly invested in the Australian market with over 130 years of data history and experience. This experience, combined with in-depth research, advanced analytics capabilities, and a comprehensive view of the data landscape, has made illion the market leader in Australia.

We also make this submission on behalf of our subsidiary, illion Open Data Solutions (formerly Proviso), the leading aggregator of banking data in Australia. illion Open Data Solutions specialises in automated bank data retrieval and analysis, and will 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. The need for clarification on pass code security requirements as part of ePayments Code review

The current version of the ePayments Code does not provide clear guidance as to which party is liable for unauthorised transactions made via a customer's account, if the customer has knowingly provided their account logon details to a third party, such as a data aggregator. This is a significant technological and market development since the last major review of the Code and should rectified as part of this ASIC consultation process.

In the contemporary context, DDC technology operates as an important secure data transfer tool that is widely used to deliver substantial value to consumers and data holders across the entire financial services industry. The technology enables lenders to better understand prospective customers and thereby fulfil their responsible lending obligations under the *National Consumer Credit Protection Act 2009* (Cth). DDC is valued by consumers who find it a convenient and hassle-free way of providing information to a potential credit provider.

As a consequence, DDC allows a greater pool of consumers to access appropriate credit, given the increased visibility that lenders have of a potential borrower's income and expenditure via DDC – this includes enhanced accuracy and minimisation of fraud risk. Other market participants, predominantly smaller lenders and fintechs, also rely on this form of technology to offer their services in a broader industry context where there is significant information asymmetry with larger players. DDC technology is therefore making a significant contribution to the competitive dynamics in the current market. As noted by ASIC in an August 2016 submission to the Productivity Commission's *Inquiry into Data Availability and Use*, "provided security concerns can be addressed, consumers should not be disadvantaged by their use of legitimate account aggregation services."[1]

[1] Australian Securities and Investments Commission, *Productivity Commission Inquiry into Data Availability and Use: Submission by the Australian Securities and Investments Commission* (August 2016) p 3 [9].

In illion's experience, some major lenders are raising the provisions of clause 12 of the ePayments Code as a reason for not permitting DDC, with the rationale that customers would thereby be in breach of the Code and therefore may be liable for any losses arising from an unauthorised transaction. There are a number of disadvantages to consumers arising from this situation. For example, preventing data sharing via DDC results in greater inconvenience to customers when applying for a financial product, prevents customers from assimilating multiple products into a single interface and thus does not allow for a more complete view of personal finances, and does not allow a prospective lender to gain a more holistic understanding of the consumer's previous repayment behaviour over a given period.

Under the current version of the Code, clause 12 provides that users must not voluntarily disclose passcodes or record passcodes on a device unless the user makes a reasonable attempt to protect the security of the information.[2] The Code defines a 'reasonable attempt' in this context to include hiding or disguising a passcode, keeping a passcode record in a securely locked container, or preventing unauthorised access to an electronically stored passcode.[3] There is little doubt that data security has significantly advanced since the 2010 review of the Code or that the security framework offered through illion Open Data Solutions provide a significantly more robust shield against unauthorised access than the measures outlined in clause 12. For this reason, we suggest that clause 12 of the Code be amended to clarify that the sharing of account logon details with secure third party aggregators such as illion Open Data Solutions does not constitute a breach of the Code.

3. The ongoing importance of DDC technology

In the period leading into the introduction of CDR/Open Banking, DDC is the most secure, efficient and convenient means of collecting and transferring customer account data with consumer consent. Following the full implementation of the proposed Open Banking regime, there will still be significant use cases for DDC technology where it can and should coexist with Open Banking. The transition to Open Banking will occur over an extended time period and the extent to which the regime will be adopted by smaller market participants is yet to be known. In this "split" environment DDC plays a crucial role. This continued utility relates to real-time data provision, simplicity of customer onboarding, level and quality of data availability, and will also provide a redundancy fail-safe, for example, in a period during which an ADI's application program interface (API) is offline. illion believes DDC technology will also provide an important benchmark to assess the performance of Open Banking, at least during its establishment phase.

illion Open Data Solutions currently facilitates access to over 150 financial institutions' transactional information, including a number of smaller entities. We envisage it will take a considerable period of time before all of these organisations provide access to their customers' data through the published API and that therefore there will be an important role for DDC services at least into the medium term.

illion is therefore of the view that DDC technology should be recognised and facilitated under the updated version of the ePayments Code, and permitted to operate in conjunction with Open Banking. As acknowledged in the 2017 *Review into Open Banking*, "banning [DDC] would remove an important market-based check on the design of Open Banking."[4] Banks, conversely, should not be

[2] Australian Securities and Investments Commission, ePayments Code (effective March 2016) cl 12.2.
[3] Australian Securities and Investments Commission, ePayments Code (effective March 2016) cl 12.3.
[4] Scott Farrell, *Review into Open Banking* (December 2017) p 84.

prevented from consenting to the use of DDC by reason of a lack of clarity in an outdated ePayments Code.

In CP 301, ASIC is correct in anticipating that, following the commencement of Open Banking, account aggregator services will remain relevant and offer a "valuable tool for consumers and commercial organisations", particularly when considering the phased implementation of Open Banking that will initially offer only 'read only' access.[5] We agree with this point and believe that DDC technology will be phased out over time in accordance with market forces, but in the interim, should continue to operate in parallel to the CDR framework beyond 1 July 2019 as a useful value-adding technique.

Recommendation on scope of ePayments Code review

illion therefore recommends that the ePayments Code review by ASIC should be used as an opportunity to update the pass code security requirements to recognise the role played by DDC technology, and clearly articulate this issue within the next version of the Code. This change will provide significantly greater clarity to lenders and other financial service providers, as well as benefiting consumers.

[5] Australian Securities and Investments Commission, *Consultation Paper 310: Review of the ePayments Code: Scope of the review* (March 2019) pp 17-18 [60].