5 July 2021

Australian Securities and Investments Commission

By email: ePaymentsCode@asic.gov.au

Dear Sir/Madam,

Consultation Paper 341 – Review of the ePayments Code

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 Securities and Investments Commission (**ASIC**) regarding its review of the ePayments Code (**the Code**).

As noted in Consultation Paper 341 (**CP 341**), the review intends to assess the functionality and reach of the Code and, in particular, its voluntary nature. This primary purpose of this submission is to address the appropriateness of existing verification mechanisms, their operation within the Code, and the new landscape incorporating the Consumer Data Right.

Digital Data Capture (**DDC**), often referred to as 'screen scraping', is the process whereby a consumer consents to the collection of their screen display data from an application so that it may be translated and displayed via a second application, and accessed by a trusted third party such as illion.

DDC is used widely in the financial services sector by lenders, mortgage brokers, personal finance management solutions and accounting products to retrieve customer data. It is a critical mechanism to empower consumers and facilitate competition in provision of consumer credit.

In our original submissions dated 5-April-2019 and 18-January-2020, we highlighted the Pass code security requirements (**PSRs**) as the specific aspect of the code that, in illion's opinion, required updating to consider technological developments and changes in consumer behaviour that have occurred since the original code was prepared.

We are therefore pleased that changes are being considered, but we remain concerned that should PSRs be retained in the code the requirements remain ambiguous and may be used to restrict consumers ability to utilise their data in a digital sharing economy.

It is vital that regulatory reforms in our sector satisfy consumer demands and continue to foster an environment that enables agile data solutions.

About illion

illion is the leading independent provider of data and analytics business across Australasia. 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 in the banking and finance industry and facilitate confident and accurate decision making. illion is highly invested in the Australian market with over 130 years of data history and experience. illion is also strong supporter of the implementation of a CDR in Australia and we have recently been accredited as an Accredited Data Recipient for both our Open Data Solutions and Credit Simple businesses.

The need for certainty and the role of Digital Data Capture technology within the Code

The shift to an online economy is driving an explosion in the volume and complexity of data. This trend is creating an increasing need for central registries that can be depended on to securely collate, house, verify, filter and manage valuable datasets, and then convert these into accurate insights to power real-time decision making and risk management.

illion plays a central role in aggregating, verifying, and facilitating the flow of the data which powers the economy. illion's digital infrastructure underpins all of life's most important purchasing decisions — from telco and utility accounts, to mortgages and car loans, and many more. Our solutions ultimately enable businesses and consumers to make critically important yet highly complex decisions with confidence.

illion has consistently stated that 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.

In illion's experience, major lenders are raising the provisions of clause 12 of the ePayments Code as a reason for not permitting DDC, with the rationale that customer 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.

We recognise and value the level of consideration that ASIC has afforded to the role of DDC technology; notably, in its submission to the Productivity Commission's 2016 inquiry into Data Availability and Use and, most recently, within the context of CP 341. illion supports the following assertion offered by ASIC within CP 341:

> *"It is not ideal, in our view, that the Code should give rise to this 'grey area' (comprising various interpretations) and leave consumers, their financial institutions and, indeed, screen scraping*

providers with the uncertainty as to what consumer behaviours amount to practices permitted under the Code."[1]

It is clear that ASIC appreciates the complexities associated with the transition to a Consumer Data Right regime and has acknowledged the ambiguity created within elements of the code, as it pertains to pass code security. Whilst the preservation of the "status quo" in relation to pass code security does not strictly deliver a resolution, the proposal put forward by ASIC provides a layer of certainty that has been highly sought after by service providers and consumer advocates alike. In the absence of more exhaustive consultation processes initiated by Government, illion does not believe it is incumbent upon ASIC to engineer a prescriptive policy framework beyond this clarification.

illion believes DDC is a critical mechanism to empower consumers and facilitate competition, valued by consumers, is secure and cost-effective, and is making a significant contribution to the competitive dynamics in the current market. illion also notes the inclusion of DDC in ASIC's December 2019 revision of Regulatory Guide 209 (RG 209), validating its use and confirming the efficiency it provides to verification processes.

According to ASIC:

> *"Developments in relation to open banking and digital data capture services will affect the accessibility, and cost of obtaining, transaction information and an overall view of the consumer's financial situation. These kinds of services may also help licensees to streamline their process—for example, potentially enabling licensees to complete both inquiries and verification of consumer information."*[2]

illion believes DDC technology provides an important benchmark to assess the early performance of Open Banking and advises that the technology should be recognised and facilitated under the updated version of the ePayments Code and permitted to operate in conjunction with the Consumer Data Right.

In DDC, industry has a solution in place that works, with no indication from ASIC that there is any harm caused to consumers by this technology. Appearing before the Senate Select Committee on Financial Technology and Regulatory Technology in February 2020, Commissioner Sean Hughes observed that "there's no evidence of which we're aware of any consumer loss from screen scraping."

It is important to acknowledge the circumstances whereby consumer liability applies, and the risks associated with uncertainty within the Code. In effect, however, the contents of CP 341 are an endorsement of the statement made by Commissioner Hughes in the parliamentary committee hearing, confirming that the regulator "has seen no evidence to suggest" that DDC technology has contributed to consumer loss.[3] This is a welcome affirmation of the applicability of the technology and a timely reminder — in lieu of the review — that there remains an effective operating role for DDC within an embryonic Open Banking framework.

DDC technology is a useful data transfer tool that is used consistently and safely to deliver substantial value to consumers and data holders.

---

[1] Australian Securities and Investment Commission (2021). *CONSULTATION PAPER 341: Review of the ePayments Code: Further consultation*, p. 36.
[2] Australian Securities and Investment Commission (2019). *Regulatory Guide 209 Credit licensing: Responsible lending conduct*, p. 43.
[3] Australian Securities and Investment Commission (2021). *CONSULTATION PAPER 341: Review of the ePayments Code: Further consultation*, p. 36.

illion's digital infrastructure is relied upon by over 15,000 corporate and government clients. We have been providing DDC services to over 1.3 million consumers for over seven years and are currently processes 1.3 million connections a month.

We have information security measures and processes in place to protect consumers: ISO27001, SOC2, 246-bit encryption of data. In the past seven years illion have experienced zero (0) security breaches of our service and nor are we aware of any other cases globally which have resulted in a security breach.

illion welcomes the opportunity to reinforce the need for clarity around Digital Data Capture (DDC) or 'screen scraping'. However, we are seeking a more definitive statement in the ePayments Code to ensure that there is no misunderstanding with respect the appropriateness of the use of DDC in the current financial environment.

Proposed provisions related to Section E "Clarifying the unauthorised transactions"

The section carries a strong implication that consumers will not be protected from financial loss related to use of a third-party service unless explicitly promoted, endorsed or authorised by the subscriber. This is a key concern of illion's as this implication justifies subscriber's continued proactive efforts to forbid the use of DDC technology, which itself creates substantial barriers to competition.

We do not feel these sections or implications are necessary as the matter can be better addressed through better direction around password security requirements.

E1Q3 Is it possible for a consumer to input a pass code to a screen scraping service without this amounting to 'disclosure'?

We strongly feel that use of an aggregation service, which is correctly utilising industry standard encryption methods, does not amount to 'making known' or 'making visible' the users pass code.

Credentials aren't human readable, they're digitised and encrypted and passed safely to the banks before being discarded.

Proposal E1 (b) could be modified to remove any room for ambiguity around this subject by clarifying that consumers must not *provision access to another individual*.

Clause 12.3 of the Code now implies that keeping an electronically stored record of pass codes should be permitted. This feels like a necessary amendment as technological advances have led to password managers becoming widely employed.

When considering the concept of 'extreme carelessness' introduced in clause 12.4, we feel it is more likely a user would exercise poor judgement in selection of legitimate password managers than in utilising a reputable aggregation service which has been recommended by a trusted advisor or platform. In both cases however, 'making known' or 'making visible' a pass code to *another individual* is not the result, nor the users intended action.

E1Q4 Is it possible for consumers to use screen scraping in a way that does not lead to the risk of financial loss?

While we strongly believe that the design of our aggregation service achieves very little risk, a secondary safeguard would be purposeful. We have observed the use of Multi-Factor Authentication (MFA) becoming broadly adopted within the financial sector. MFA provides protection against unauthorised access which may otherwise occur if credentials alone are compromised. Introduction of MFA is a subtle change to consumers behaviour without carrying material detriment to user experience. In effect, MFA creates 'a password required for viewing an account' and 'a password required to transact with the account'.

E1Q5 What types of examples involving express or implicit promotion, endorsement or authorisation of the use of a service would be helpful to include in the Code?

With regard to Digital Data Capture, we are not aware of a scenario where a subscriber would recommend an account aggregator service except to facilitate sharing of data held by an un-associated company (who is likely also a subscriber).

Conclusion

illion would welcome greater collaboration between industry and the regulator as technological innovations recalibrate the environment for ePayments, necessitating not only continued satisfaction of compliance obligations, but further upholding and adherence to evolving community expectations.

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

Yours sincerely,

General Manager, Consumer Bureau