FinTech Australia

SUBMISSION PAPER:

Submission to Australian Securities & Investments Commission on the Review of the ePayments Code

April 2019

This Submission Paper was prepared by FinTech Australia working with and on behalf of its Members; over 300 FinTech Startups, VCs, Accelerators and Incubators across Australia.

Table of Contents

About this Submission

This document was created by FinTech Australia in consultation with its Payments Working Group, which consists of over 172 company representatives. In particular, the submission has been compiled with the support of our Working Group lead:

- Simone Joyce, Paypa Plane

This Submission has also been endorsed by the following FinTech Australia members:

- Ezypay
- Frollo
- Paypa Plane
- Volt
- FlashFX

Submission Process

In developing this submission, our Payments Working Group held a series of consultations to discuss key issues relating to the questions raised by the Australian Securities & Investments Commission.

We also particularly acknowledge the support and contribution of our Policy Partners, DLA Piper to the topics explored in this submission.

The views expressed in this paper do not necessarily reflect the view of our Policy Partners, DLA Piper in supporting the preparation of this paper.

Issue for consultation

FinTech Australia welcomes the opportunity to put forward its position on behalf of members in relation to the ePayments Code (**Code**). Our members believe the Code offers a number of strong consumer protections, and helps promote trust in the electronic payments system. In addition, our members have identified issues and corresponding solutions that will improve the Code.

List of proposals and questions

B1 We propose to assess whether the Code, as currently worded, has successfully adapted to today's payments environment and is sufficiently adaptable to respond to emerging and future developments in financial technological innovation and changing customer behaviours.

B1Q Are you aware of any specific examples where the Code is not adequately catering for these things?

It is clear that more consultation and collaboration is required in order to create an adequate code in light of New Payments Platform (NPP) transactions. The Bulk Electronic Clearing System (BECS) procedures relate to the BECS payment rails, which are predominately used for direct entry transactions. Given the NPP does not allow for a 'direct entry' or pull style transaction, and will mirror more closely a scheduled, pre-approved 'direct credit' or 'push' transaction, it is very important that this Code considers the impact of this difference.

The BECS procedures, which contribute to the Code, are not adequate to govern a scheduled preapproved and recurring transaction on the NPP rails. It could be argued that they are no longer adequate to appropriately govern the current, growing, volume of direct entry transactions occurring in an increasingly digital and subscription-based economy, where fraud can occur more insidiously and in larger volumes.

The existing Code for BECS operation is not strident enough to protect consumers, businesses or financial institutions. Currently, any bank account and BSB can be submitted to a direct debit user with an APCA ID to have the account debited. There is no check of account holder permission or ability for a consumer to directly approve a direct entry transaction. The current standard of direct debit authority forms may have been relevant before digital payments became the accepted standard and subscription-style payments became so numerous. These forms must be held for seven years beyond the date of the last transaction and this is not widely understood by

businesses or consumers. In many cases, the consumer does not even have access to an accurate and current schedule of payments.

Not only does this create opportunities for malicious fraud, it also increases the rate of 'friendly fraud' and disputed transactions. The recourse for a mistaken debit (either by error or fraud) is a retrospective one and results in loss of consumer funds, potential loss of business funds and expense to all stakeholders (including the financial institutions who must investigate). Other countries have identified this as a problem and put in place either insurance schemes or permission layers that must be met before a transaction can take place. In Australia, we have neither of these mechanisms.

There is also little guidance on the types of fees that payment facilitators or providers should be able to charge consumers and the information that should be provided to consumers about these fees. Without any type of code of practice – either compulsory or suggested, there has been an increasing level of consumer (and business) cost associated with third party providers in the direct debit industry.

The consideration of the current Code presents an excellent opportunity to critically assess current procedures for the BECS users and allow this to formulate a relevant code for NPP preapproved or scheduled transactions.

Without more transparent and collaborative discussion between the NPP and stakeholders, formulating any code of practice that aims to direct behaviour during NPP transactions is redundant; the existing framework cannot be relied upon due to lack of relevance and the opaque roadmap from the NPP makes it challenging to identify appropriate guidelines to future proof a code of practice.

Separately, our members believe the descriptors on bank statements from card/bank debits need to be improved. Depending on the gateways used, the descriptor changes between legal name and trading name and this often confuses the end customer. Mandated consistency would result in fewer misunderstandings.

B1Q2 How could our assessment of these things be done in a simple and consumer-focused way?

Declined transaction reasons are not clearly available to consumers. The current BECS rules use return code 6 - refer to customer - which could indicate insufficient funds, or exceed daily limit, or a result of a raft of algorithms used by issuers/banks to pick up transaction behaviour anomalies. In the recurring payment space, non-payment could result in cessation of service. This leads to disputes between customers and small

business when the root cause of the decline is not clear (e.g. "I had sufficient funds, why did the transaction decline?").

Card transactions are declined for the same reasons as above with “do no honour” so it really confuses cardholders when transactions decline for this reason.

As issuers/banks introduce more transaction monitoring rules, in-app card controls to limit merchants and spend limits, it needs to be made clearer to the end customer the impacts to recurring payments. These functions give the account holder lots of freedom, but our members are finding people cancelling direct debits through these apps and setting low daily limits without knowing necessarily the impact to their recurring payments. Insurance is a classic example where non-payment will result in a loss of service/ability to claim.

B2 We propose to assess the clarity and appropriateness of the current policy positions in the Code’s complaints handling provisions.

B2Q1 Is there justification for maintaining two complaints handling regimes in the Code (i.e. Chapter F and Appendix A)?

Our members will further reflect on this question and may provide a response in the near future.

B2Q2 Would there be any benefits in more closely aligning the complaints handling provisions in the Code with RG 165?

Our members will further reflect on this question and may provide a response in the near future.

B3 We propose to consider whether the current settings in the Code for unauthorised transactions are appropriate and sufficiently clear.

B3Q1 What are the benefits and challenges of the Code’s current settings for unauthorised transactions?

There is currently a certain amount of ambiguity surrounding the inherent risk (or lack thereof) in the current environment where consumers either knowingly or unknowingly use a ‘scraper’ tool in order to verify their account, provide access to their account for transactions or for other information. There are no current ubiquitous standards and the definition of a breach of pass code security is often subject to the particular view of the

customer's ADI – meaning the use of a scraper tool may breach passcode protocol according to the rules of one ADI but not another.

Our members believe the Code should be amended to expressly permit the use of scraping, by permitting the disclosure of passcodes for the purpose of scraping as an exception to the current passcode disclosure. Banks, conversely, should also not have the ability to block scraping.

The primary benefits of scraping include:

- for consumers there is no need to fill out bulky application forms, upload documents and wait for verifications and so on, as registration and identification data can simply be supplied by the bank where you are already registered;

- the consumer is able to better manage his affairs by having a holistic view of all his banking across numerous institutions;

- for financial institution lenders they are better able to carry out responsible lending assessments by independently verifying a consumer's income and expenses with relevant, accurate, and up-to-date data from the consumer's own accounts; and

- as financial institutions are getting access to banking history, they can often supply the consumer with more attractive offers based on previous performance at other institutions. Via banking data through scraping banks are not only getting to Know-Your-Customer, better but are also able to better understand customer needs and adapt their offers to suit those needs.

Further, we believe scraping should continue to operate in conjunction with Open Banking - as acknowledged in the Farrell Report, which provided "banning [scraping] would remove an important market-based check on the design of Open Banking" [Scott Farrell, Review into Open Banking (December 2017)].

Often the consumer is not aware that they are making use of a scraping tool. This ambiguity is often the result of poor communication to the consumer (either on behalf of the ADI or the third-party system operating the scraper tool). These clauses relate very closely to the Open Banking framework and will need more consideration to protect and inform consumers whilst allowing for innovation and new product offerings. The Code may be able to better inform the consumer as to the benefits and risks of using a third

party scraper tool by perhaps coming up with some template wording institutions can use.

In summary we suggest that the ePayments Code be amended to provide clarity on scraping technology and to 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 scraping where it can coexist with Open Banking. This continued utility may relate to real-time data provision; simplicity of customer on boarding; level and quality of data availability; and provide a redundancy fail-safe, for example, in a period during which an ADIs API is offline. We believe scraping will also provide an important benchmark to assess the performance of Open Banking, at least during its establishment phase.

The Code could also address the process that complaints specifically about third-party scraper tools (or similar) (from consumers, FinTechs or other stake-holders) can be raised and managed. As these are relatively new tools, users may not have clear procedures to lodge complaints, or for providers/ADIs to respond to any complaints – it is possible for the Code to identify such procedures to the benefit of all stakeholders.

B3Q2 What role, if any, could the Code play in preventing or reducing the risk of customers falling victim to financial scams, or helping customers who have lost money through scams?

It may be that the Code provides guidance on best practices to assist customers in protecting themselves from scams, similarly to what is available from Basic's Money Smart resources. For example, the Code may provide open source information for subscribers to provide to customers relating to:

- understanding the tricks scammers use;
- protecting personal information;
- using strong passwords;
- securing computers and mobile devices;
- thinking before sending money online; and
- questioning offers of easy money.

This would also assist businesses to protect themselves and their customers from online fraud. If ASIC could develop a set of improved best practices to safeguard consumer data, that would be beneficial.

Although the potential for fraud is high for online transactions, our members should not have to concede and accept it as a business cost.

By ASIC putting the right tools and processes in place, our members can reduce their chances of an attack (especially when accepting bitcoin payments), keep both business and customers safe, and reduce the chances of losing revenue and drowning in chargeback fees.

B4 We propose to review the data reporting requirements in the Code and assess the most valuable and efficient approach.

B4Q1 Would it be helpful (for consumers or subscribers or both) for ASIC to collect and publish data about particular matters under the Code? If so, what matters, and why?

It may worthwhile gathering information not just on 'card' fraud and mistaken bank transfer payments (when a payer enters their banking environment to instigate a payment to another bank account) but also on mistaken and fraud related to direct entry payments (where a payment is 'pulled' from a bank account by an accredited with necessarily explicit permission from the account holder). Given direct entry payments account for the bulk (both volume and value) of payments in Australia. For example, in January 2019, over 251 million direct entry transactions took place (worth upwards of $3BN), even a fraction of a percentage of unauthorised transactions due to error or fraud equates to a considerable value. Given there is no formalised data collected or released, at least publicly, it is hard for a code of practice to address and attempt to mitigate loss via direct entry fraud/error by defining better protocols and guiding behaviour.

B5 We propose to consider whether the provisions in the Code for mistaken payments are simple and accessible enough, and whether ADI subscribers should have any role in mitigating or preventing such payments.

B5Q1 Is the process for seeking return of mistaken internet payments sufficiently simple for customers?

There is insufficient provision in the Code relating to subscribers' obligations in relation to its dispute resolution and operator call centres, particularly in relation to mistaken or unsuccessful electronic transactions. Where a mistaken internet payment occurs, or where a card transaction defaults, customers will typically contact their ADI for more information. Our members understand that where the operator cannot definitively determine the issue causing the unsuccessful internet payment or electronic transaction, the operator will register the unsuccessful transaction using one of the generic fraud codes. From this position, the customer does not have accurate and sufficient information to appropriately redress the mistaken payment.

Our members suggest the Code be updated to extend subscribers' obligations in relation the operation of its call centres. Subscribers should be obliged to ensure that its call centre operators, particularly those operating BECS and card schemes, receive more extensive training in relation to the error codes attributable to the underlying issues impacting unsuccessful electronic transactions. In this way, call centre operators will provide customers with more accurate information and will provide customers with a more straightforward process to seek return or redress of mistaken electronic payments. The discussion around expanding the error codes at B7Q1, will also be relevant in this respect.

In addition, the Code may be amended to address how to better manage human error in telephone banking services. Customers should feel confident in the telephone banking service and not fall victim to human error in processing transactions.

B5Q2 What other provisions could be included in the Code for ADI subscribers to reduce the risk of or prevent mistaken payments?

In terms of drafting the Code to address mistaken or fraudulent internet payments, more obligations should be created at the point in which the ADI engages with its subscriber.

Currently, there are insufficient processes to ensure the legitimacy of the ADI subscriber when it subscribes with the ADI. The Code should make provision for obligations on the ADI to verify and background check the potential subscriber. For example, there should be an obligation on the ADI to conduct an Anti-Money Laundering and Know Your Customer check on its subscribers to assess the potential risks, before the subscriber is approved to conduct its business with the ADI. From the outset, this would prevent mistaken payment, or at least reduce the risk of such, to the extent that ADIs would be undertaking more robust checks of its subscribers and potentially preventing mistaken payments occurring from the outset.

B5Q3 To what extent do you think the mistaken payments procedures in the Code will remain relevant as more customers begin using the New Payments Platform?

Though the NPP will, as the code review paper identifies, reduce the number of mistaken payments during a 'pay anyone' bank transfer, there is no guidance on how the NPP will lower the number of disputed direct entry transfers. In any case, there will be a considerable period of time between the majority of direct entry transactions migrating to NPP transactions - the system architecture needs to be designed, rules of use created, ADIs and providers must be technically prepared and then, finally, business and consumer users must all be prepared to adopt the solution, at which point, cost per payment will become a factor. The RBA published 'Payment Costs in Australia' publication identifies direct entry to be the cheapest way that a business can accept payment. If 'per payment' costs for NPP run direct entry payments is comparably higher this will become a barrier to adoption.

Given this long lead time, and the likelihood that many direct entry BECS transactions will continue to occur many years after the NPP does offer a direct-entry style payment (a precedent set by the continued use of cheques), it is appropriate that a Code review should address direct entry mistaken and payments fraud and provide recommendations on how stakeholders should operate when performing or interacting with direct entry payments.

B6 We propose to explore whether it may be appropriate to extend the Code, or at least some of its protections, to small business.

B6Q1 Do you think that all or any parts of the Code should, or could appropriately, apply to small business?

Our members believe that some of the concerns in relation to extending the Code to apply to the protection of small businesses still remain. In particular, the obligation on the Code subscriber to monitor the extent to which its customer is sufficiently a small business would be a significant one. As was raised in the 2010 consultation, this issue would create significant non-compliance exposure for the Code subscriber.

B6Q2 Are you aware of any data that shows the prevalence of electronic banking problems for small business customers?

"Friendly fraud," also known as chargeback fraud, happens when a customer disputes a legitimate charge on their payment card. Most merchant chargeback disputes are raised

where a merchant has a chargeback claimed against them or where the merchant is a victim of fraud and the dispute is lodged against the merchant's financial services provider. Most frauds against merchants occur through online and email transactions. Generally, merchant chargeback disputes rule in favour of the card/account holder even when the consent proof is provided. Sometimes the consent proof is not accepted by the issuing banks and it is therefore rejected.

BECS/card schemes need to make the consent standard clearer and to ensure that even electronically captured consent is acceptable. Small businesses need protection from friendly fraud, purposeful disputed payments. It is suggested that the chargeback reason 'fraudulent' transaction needs to be used as intended. Our members see this reason code all the time with legitimate merchants, with non-fraudulent claims, for example, do not recognise the debtor.

B6Q3 How might the Code best define 'small business'?

Our members believe the definition is sufficient.

If the Code were extended to small business, our members support the current definition used by ASIC in relation to small business: a company with two out of these three characteristics (a) an annual revenue of less than $25 million, (b) fewer than 50 employees at the end of the financial year, and (c) consolidated gross assets of less than $12.5 million at the end of the financial year. Our members believe the Code should adopt this definition for the purpose of ensuring uniformity across the regulatory standards.

B7 We propose to consider any other aspects of the Code that may need updating as part of our review.

B7Q1 Are there any other aspects of the Code that should be updated?

Our members suggest that the Government has not provided clear direction on whether the Code will be made mandatory or how they intend to regulate consumer protection in this area. Once the Code has been reviewed and updated, the Code may be made mandatory for any entity that intends to send or receive electronic payments. Communication regarding whether the Code will remain voluntary needs to be improved.

In addition, we suggest amending the Code to clarify that consumers can share their information with an ASIC-accredited list of secure third-party services without losing any protections provided by the Code.

Furthermore, currently a number of different transaction response codes exist, for example, an error due to the customer's card issuer has declined the transaction as there is a problem with the card number. The Code should be amended to ensure bank response codes provide an appropriate level of detail. Currently, the amount of detail is inadequate. The error may indicate that the customer should use an alternate credit card, or contact their bank, however it does not specify the particular problem producing the error. We recommend that the Code be updated to oblige subscribers to specify error codes in more detail. This would have a number of positive consequences. Firstly, it will improve the customer's experience by enabling the customer to have a more comprehensive understanding of their banking and the issues disenabling their payments. This update may also be beneficial from a dispute resolution perspective, as it may prevent the circumstances where a dispute is escalated involving a customer misunderstanding regarding what the issue was and who was at fault.

While the consultation paper has identified account aggregation as one of many reasons for why the code needs to be updated, we believe that this subject needs to be addressed specifically in the revised Code. The current Code has allowed different ADIs to interpret clauses how they want and this has arguably been to the detriment of innovation in the sector. One may ask, what relevance will account aggregation have when Open Banking is in full flight? As can be seen in other markets, if we want to deliver on the promise of Open Banking and the potential of open data, then these two will run in parallel with aggregated data filling the many gaps that Open Banking cannot/ does not fill. This will be a long journey and the industry needs to be consistent with both its rules and how it educates the market if it is to be successful.

Further, it makes sense for the Code to draw broad parallels with Open Banking and what it is trying to deliver. As part of this, it should be specific about 'aggregation', removing any opportunity for misinterpretation, ensuring that the customer is informed, suitably protected and allows the customer to choose to share their data (via aggregation methods) without penalty or recrimination.

Conclusion

Our members are pleased that ASIC is proposing better protection for small business and a streamlined complaints handling system as part of a major review of Australia's ePayments Code. The Code must have the ability to respond to the rapidly changing payments landscape, both from a perspective of delivery mode and service provider. ASIC must find the balance between consumer empowerment and consumer protection. Our members support the Code protections being consistently applied.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian FinTech Industry, representing over 120 FinTech Startups, Hubs, Accelerators and Venture Capital Funds across the nation.

Our vision is to make Australia one of the world's leading markets for FinTech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to drive cultural, policy and regulatory change toward realising this vision.

FinTech Australia would like to recognise the support of our Policy Partners, who provide guidance and advice to the association and its members in the development of our submissions:

- DLA Piper
- Baker & McKenzie
- Hall & Wilcox
- King & Wood Mallesons
- K&L Gates
- The Fold Legal