9 July 2021

Ms Jennifer Lyons
Senior Specialist – Credit, Retail Banking and Payments
Financial Services Group
Australian Securities and Investments Commission

By email: Jennifer.Lyons@asic.gov.au

Dear Ms Lyons

COBA Response to ASIC's Review of the ePayments Code: Further Consultation

COBA welcomes the opportunity to respond to ASIC's second consultation on the ePayments Code (CP 341) and appreciates the continued engagement with ASIC on this key policy area. As outlined in our previous submissions to ASIC, it is our view that the Code should be clear and explicit in outlining the responsibilities of the subscriber and the consumer, in a way that is fair, promotes consumer confidence and promotes efficiency in the market. This response outlines COBA member feedback on ASIC's proposed changes to the Code. We do not have member feedback or a common sector view on all of the proposed changes.

Feedback on specific positions is below:

Compliance monitoring and data collection

COBA members support the proposal by ASIC to remove the requirement in the Code for subscribers to report annually to ASIC on the incidence of unauthorised transactions because of the resources required to collate this information in a format specific to reporting requirements under the Code. However, members would like ASIC to consider member resources and operational capacity when requesting ad hoc reports on compliance with the Code and to allow for sufficient time to respond to ASIC's requests. Additionally, members have outlined that there does not seem to be a tangible benefit to the public from the data provided to ASIC for the calendar years 2015 to 2017 and therefore ASIC should communicate to subscribers the expected benefits from this decision to collect information.

Clarifying and enhancing the mistaken internet payments (MIP) framework

COBA members have questioned the value of ASIC's proposal to require sending ADIs to advise the consumer of their dispute resolution rights under proposal C2. Members noted that this proposal would lead to an increase in complaints which have no basis other than the fact that the consumer is not satisfied because the sending ADI was unable to recover a payment that was carried out in accordance with the consumer's instructions and was unable to be recovered as a result of the action or inaction by the receiving ADI or its customer.

Another COBA member has stated that there is a gap in the Code where a receiving ADI may be aware of a mistaken payment but has not received a recall request from the sending ADI. COBA welcomes protocols around this, as customers who hold mistaken payments in their accounts can face issues when lodging their annual tax returns and other administrative inconveniences.

COBA members support ASIC's proposal to require ADIs to provide additional important information in the on-screen warning about mistaken internet payments. The use of prescribed wording is preferred as this would remove any ambiguity about what information must be disclosed and would also ensure all subscribers are providing the same information to consumers.

COBA members are supportive of ASIC's proposal under the 'Partial return of funds' and welcome a non-exhaustive list of examples of what would constitute as 'reasonable endeavours'. This is particularly useful in the case where the ADI does not have updated contact details for the customer, or the customer is otherwise unable to be contacted and would help in outlining the steps the ADI would have to take to achieve the 'reasonable endeavours' threshold in these circumstances.

COBA members agree with ASIC's proposal to clarify the definition of MIPs as they believe it should apply to all forms of mistaken payments using the New Payments Platform. The current definition specifically excludes payments on the New Payments Platform. Due to customers not being able to select which channel is used to conduct transactions other than those using a PayID, COBA members agree that customers should be afforded the MIP protections where the payment is sent using BSB and Account Number to ensure customers are not disadvantaged by decisions outside their control.

Clarifying the unauthorised transactions provisions

COBA members support ASIC's proposal to clarify that the unauthorised transaction provisions do not apply where the consumer has made the transaction as a result of a misunderstanding or falling victim to a scam. COBA members are concerned about the rising incidence of scams and the impact on consumers. We agree with ASIC's view that the industry response for protecting consumers from scams is most appropriately managed in a coordinated manner outside the Code. However, COBA members have reiterated the concerns raised in our previous submissions to ASIC about providing clear and fair rules for allocating liability for unauthorised transactions.

ASIC has noted that in linking a breach of pass code security requirements (PSRs) to unauthorised transactions, the subscriber "must prove on the balance of probability that the breach of the pass code security requirements has contributed to the unauthorised transaction in question". As highlighted in our previous submissions, COBA members have raised questions about the application of the 'balance of probabilities', the relationship between PSRs and terms & conditions, and the distinction between causing a loss and contributing to a loss.

Further, COBA members have noted that AFCA's application of clause 11 of the Code as demonstrated in its determinations, makes it impossible to discharge the burden of proof, especially in scenarios where consumers have provided remote access to a device. This is because clause 11.3 of the Code currently requires subscribers to prove, on the balance of probability, that any breach of PSRs involving more than one pass code was more than 50% responsible for the losses. Due to payments requiring either one or two pass codes (e.g., login password and a one-time code generated by a security token) AFCA have determined that the breach of the PSR for only one of these pass codes does not meet the 'more than 50%' threshold and therefore subscribers are always liable for the loss in these circumstances.

COBA members consider that the current requirement for the breach of PSRs to be 'more than 50%' responsible for the losses should be removed. COBA also requests more clarity from ASIC on what constitutes a "contributory link" in this situation.

A COBA member has noted that the ability to dispute payments for up to 7 years is too long, particularly when there is no onus on the customer to demonstrate a reasonable excuse for any delay beyond the 3-year timeframe provided for, under various scheme rules and that there are other more appropriate avenues for recourse. The COBA member noted an example of a customer raising a complaint in relation to direct debit payments collected by a service provider which had been going on since the 1990s. In that scenario, the customer had a more appropriate avenue directly with the service provider, but the customer nevertheless chose to use the ePayments Code due to its provision to dispute payments.

Detailed comments by an individual COBA member have been attached in **Appendix A**.

Thank you for the opportunity to provide these comments. If you wish to discuss any aspect of this response, please contact [redacted] at ([redacted]) or [redacted] ([redacted]).

Yours sincerely,

[redacted]

[redacted]
Chief Executive Officer

Appendix A – An individual COBA member's feedback

COMPLIANCE MONITORING AND DATA COLLECTIN

B1Q1 Do you support removal of the requirement in clause 44.1? If not, why not?

Support the removal of the annual reporting requirement. We note that while this is a welcome relief, it is hoped that requests for ad hoc reports that replace the compulsory annual reporting will not be too numerous or onerous, particularly for smaller ADIs with limited resources.

B1Q5 What are the expected costs to subscribers of the additional monitoring or surveying function mentioned in proposal B1(b)(ii)?

Too difficult to quantify without details of information requested and frequency. ASIC have the authority to review regulated entities in any case.

CLARIFYING AND ENHANCING THE MISTAKEN INTERNET PAYMENTS FRAMEWORK

C1Q2 Are there benefits in applying the MIP framework to situations where only partial funds are available for return? Please describe these benefits.

Yes. Minimising loss to the customer. Smaller loss preferable to a larger one if full amount is not retrievable.

C1Q3 Do you think it would be useful for the Code to provide non-exhaustive examples of what might amount to 'reasonable endeavours'? If not, why not?

Yes. Would provide better guidance and more certainty so a consistent approach across the industry is more likely to be adopted. In reality, typically once the funds have gone there is minimal chance of retrieval.

C1Q4 What types of examples would be helpful in a non-exhaustive list of examples of what might amount to 'reasonable endeavours'?

Receiving bank: Number of attempts to contact receiving customer through known communication channels (phone / email) within a given timeframe.

C1Q5 What types of factors might affect whether a particular action is necessary to satisfy 'reasonable endeavours' in individual cases?

Completeness and timing of information provided to receiving institution.

C1Q6 Are there any practical impediments to implementation of the proposals at C2?

No, but sufficient compliance lead-time requested for ADIs to put reporting processes in place to cater for the new requirements, bearing in mind the significant compliance project workload. Details already kept to a certain degree as a record in case of customer dispute, and potential escalation to AFCA.

C1Q7 What are the costs to subscribers of extending the MIP framework to cover the partial return of funds reasonable endeavours to retrieve the remainder of the funds?

Difficult to quantify. In theory should not be no real difference in process than current practice for chasing the full amount.

C2Q2 What are the costs associated with compliance with the proposed timeframe?

Should be no greater than current.

C2Q3 Do you agree with the proposed recording keeping requirements? Why or why not? What are the costs of the proposed record keeping requirements?

Records kept at present in case of escalation to dispute. Should not be a significant change.

C2Q4 What do you consider are the costs of requiring ADIs to inform consumers of their dispute resolution rights?

Difficult to quantify but not expected to be significant as wording to be added to response templates where required.

C2Q5 What are the benefits and/or burdens of C2(d)? How do they compare to benefits and/or burdens of the current requirements in the Code?

No real change as receiving bank not currently at fault in current situation. Agree this should be the case given receiving bank has no visibility of error or choice in accepting the funds.

C3Q1 Do you support our proposed clarification of the definition of 'mistaken internet payment'? If not, why not?

As proposed, this excludes push payment frauds. This is problematic given it is not addressed anywhere else and is a vexed area for ADIs with inconsistent approaches to AFCA determinations. Clear guidelines are required to address this area, and regulatory messaging to date has not given any indication of where, when or how it will be addressed. There has been talk of a broader scam strategy from the regulators but no clear map. In the absence of such a plan, the preference is for clear guidelines on accountabilities of customers and banks within the ePayments code that include definitive statements on same.

C3Q2 Please compare the costs and regulatory benefit of the following alternative scenarios:

(a) 'Mistaken internet payment' is defined to refer only to actual mistakes inputting the account identifier.

See above. Would be acceptable if push payment responsibilities / liability were adequately addressed elsewhere in black and white which is not currently the case.

(b) 'Mistaken internet payment' is defined to include situations where a consumer inputs the incorrect account identifier as a result of falling victim to a scam (also known as 'authorised push payment fraud').

Benefits would be clarity around responsibility of customers to understand the transaction they are entering into, who they are dealing with, and requirement to check all details before executing a transaction.

ADIs are facing increasing costs paying out claims in instances where they have done everything right and a third-party scammer has successfully defrauded a customer. The costs of doing so are becoming increasingly more prohibitive, especially for smaller mutual ADIs.

The prevailing attitude of AFCA is to find for the customer because the banks have money to pay, even though the process of the banks cannot be faulted.

ePayments code should by definition cover all electronic payments. It can then be used as a single reference point on transactions for both consumers and banks, without the need to refer to multiple sources.

C4Q2 Should precise wording for the on-screen warning be prescribed, or should flexibility as to the precise wording be allowed? If precise wording is prescribed, what should that wording be? If the Code allows flexibility, what wording would serve as a useful benchmark for compliance with the on-screen warning requirement?

Yes, prescribed wording is highly recommended. Would result in consistency across all banks and remove one major item of contention where AFCA interprets each case differently according to wording and position of warnings. Given AFCA's inconsistencies, we would go further and prescribe positioning and bolding / otherwise of warning.

C4Q3 What costs and regulatory burdens would be involved in implementing the proposed change?

Minimal. One time amendment of key documents and existing wording on IB and App, etc. Provided sufficient lead time for compliance to implement the wording changes, then little impact anticipated.

EXTENDING THE CODE TO SMALL BUSINESS

D1Q1 Do you support our proposal to provide for an 'opt-out' arrangement for individual subscribers in relation to small business Code coverage? Why or why not?

We are still unclear as to the case for including small business. If it is to be included, we prefer opt-out to mandated, and agree with the position of this not being retrospective.

D1Q2 How likely do you think it is that your organisation (if you are a Code subscriber) and other subscribers will opt out? On what grounds might you or other subscribers opt out?

Our position is that consumer and small business have very different operational parameters and needs, and small business should be subject to their own regulations including payments. There is also a compliance burden in determining eligibility, plus the fact size of businesses can change.

D1Q4 What are the costs and benefits for industry of our proposal?

Significant costs in tie and resource to develop and monitor. Added compliance burden when a case has not been made for small business inclusion.

D1Q5 Do you agree with our proposal D1(b), that the Code should not apply retrospectively to small business facilities already acquired at the time of commencement of the updated Code? If not, why not? What are the costs and complexities versus benefits of our proposal and alternative approaches?

Agree that if applied to small business, it should not be retrospective as it changes the playing field after business membership first struck. No business case has been made to apply retrospectively.

D1Q6 What are the key parts of the Code that may present difficulties for subscribers in extending the Code's protections to small businesses? Please provide reasons.

Difficult to determine existing knowledge / facts in cases where multiple individuals within a business have access to or responsibility for payments. Muddies the waters around liability.

D1Q7 Does our proposed change to the definition of 'user' (by including employees, contractors or agents of a small business) address any concerns about any increased risks to subscribers as a result of extending the Code's protections to small businesses? If not, why not? Do you think this could have any unintended impacts? If so, what are they?

No. The risks remain as they are more around the nature of business transactions and multiple person access than to do with the definition of user. This increases an ADIs risk in that businesses conduct significantly more transactions than an individual and for considerably larger dollar amounts.

By nature, most businesses are also more heavily involved in foreign transactions which means the risk of fraud may be greater than someone who uses an account for personal reasons domestically.
The other risk to consider from an ADIs perspective is the increased onus of how an ADI will manage/monitor when a "small business" no longer exists as a small business.

D1Q8 Do you agree that we should review the extension of the Code to small business on an opt-out basis after 12 months? If not, why not?

Yes. Given concerns and industry preference not to include small business for reasons previously stated, a review after 12 months is better than no review if small business has ultimately been included.

D2Q1 Do you agree with the proposed definition? If not, why not?

The actual number is less relevant than the argument that small business should be excluded. The compliance burden would not vary greatly with any nominated number under 100.

D2Q3 What alternative definition(s) would you suggest? Why? How do you think the costs and benefits compare to those relevant to our proposed definition?

Sole trader only as most relevant and applicable to individual consumer protection, but even then, the nature and volume of business transactions is just not comparable to an individual consumer.

D2Q4 Given the discrepancy between our proposed definition and AFCA's definition of small business (see paragraph 104), which approach do you think is preferable for the Code? Is there an issue in having slightly different definitions?

Strong preference for using same definition for reasons of certainty and smoother compliance.

CLARIFYING THE UNAUTHORISED TRANSACTIONS PROVISIONS

E1Q1 Do you agree with our proposals? If not, why not?

No. ADIs are already struggling due to the current form of the code when regulators are interpreting what an unauthorised transaction is and when an account holder has/has not breached their obligations in regards to passcode security requirements. Our concerns as follows:

a) Watering down of the PSR Framework may work to the detriment of ADIs. This is because it explicitly holds an account holder liable for one or more actions proving that they have breached their obligations under the code.
b) By removing the explicit references to what an account holder's obligations are, this could have the reverse effect and encourage risk taking of transactions by account holders. This is because both the account holder and regulators such as AFCA will use this as the basis for an argument in favour of the account holder. This has definitely been our experience with AFCA to date.

c) Removal of these obligations may mean that both the account holder and regulators such as AFCA have more room to hold an ADI responsible for transactions. Especially if the threshold is replaced with "on the balance of probabilities." This definitely leaves the code open for interpretation.
d) To date, despite having these provisions in place, ADIs have found it extremely difficult to prove that an account holder has breached one or more of those obligations, purely on the basis that it is physically impossible for an ADI to show physical evidence of that breach. For example, despite having secondary authentication via SMS code, where it is apparent to an ADI that the account holder likely "disclosed" one or more of those passcodes, say by giving access to a scammer by logging them onto their computer and subsequently their internet banking, we have no records that could prove this.
e) The code further states the following: *"the fact that a facility has been accessed with the correct device and/or pass code, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in clause 12."*
Which also plays a significant role as it would be almost impossible for a scammer to get two passcodes correct (including the SMS Verification) without the assistance of the account holder. Despite this, whilst it is obvious to the ADI and regulators such as AFCA, AFCA has continued to use this provision as the basis of all complaints to hold an ADI liable.

It is our view that the PSR requirements should be expanded to include 'providing access to' a third party by way of entering one or more passwords on a device or platform which gives access to a third party to be captured by the term "disclosed." The code should increase an account holder's responsibility so that it encourages account holders to act with more caution and to protect themselves as much as possible from foreseeable fraudulent activity.

We do not agree that changing the threshold to "on the balance of probabilities" does not change the liability provisions. As mentioned above, we have had very negative experiences in our dealings with regulators such as AFCA who we feel find any loophole in the code to shift the onus on ADIs. In some cases, we have been told by AFCA that "*the claim is only for x amount and to just pay it to close the case off."* When we have to deal with one or more of those types of claims monthly or annually, the claim then becomes an issue that is greater than just x amount.

As noted in previous submissions regarding the ePayments Code and AFCA review, there is real potential for a spate of claims targeting a single ADI or our sector that could have significant severe and long-term financial damage. We are simply not in a position to write these claims off and still compete on an even playing field with major banks who have the scope to cover these escalating costs. This poses a growing risk to our sector and should not continue to be ignored.

E1Q2 What are the costs or regulatory burden implications flowing from our proposals? Do the benefits outweigh the costs or regulatory burdens?

Refer previous answer. The benefits do not outweigh the costs, and in fact tilt the risk further on to ADIs than is currently already the case by placing a greater burden of responsibility on them to prove customer liability when the customer has clearly breached the passcode security requirements. The concept of "balance of probability" further erodes the responsibility of the customer with AFCA already prone to a loose interpretation in favour of the complainant.

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

Not to our knowledge.

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

There is always a heightened risk of loss, and it is unfair for the ADI to bear the added risk when the consumer has elected to disclose a password.

MODERNISING THE CODE

F1Q1 Do you agree with the proposal to define biometric authentication in the Code? If not, why not?

We believe that the code should be technology neutral, i.e. allow for all forms of access & authentication without specifically mentioning them.

F1Q2 How would you suggest biometric authentication be defined in the Code?

Broad definition noting it is treated the same way as other means of authentication.

F1Q3 Which particular clauses in the Code do you think need to include a reference to biometrics in order for the clauses to continue to have their intended effect?

Include within the overall up-front definition of authentication, "all types, including password, biometrics, etc." then refer to definition within the Code where necessary.

F1Q4 Do you agree that we should not include biometrics in the general definition of 'pass code'? What might be the impacts of taking this approach? In particular, how would using the concepts of biometric authentication and pass codes interchangeably within the pass code security requirements work in practice? What are the costs or regulatory burden implications of our proposals?

No. See above. We view a customer choosing to disclose their password, unwittingly or otherwise, in the same light as authorising access via biometrics. The thought process is the same, just a different mechanic.

F3Q1 Do you agree that the Code's protections should apply to transactions made through the NPP? If not, why not?

Yes, but noting immediate nature of the NPP transactions and implications for recovery.

F3Q2 Are there any particular provisions in the Code that, while workable in the BECS context, would not be workable in the NPP context? What are these and what are your reasons?

Note that same rule could apply but recovery potential is lower given instant availability of funds in receiver's account.

F3Q4 Do you support the Code's provisions, as relevant, expressly relating only to BECS and the NPP? Or would your preference be that the Code is payment platform agnostic? What are your reasons?

Comfortable with reference to BECS and NPP and suggest all-encompassing term to cover other future payment avenues given technology likely to advance prior to next review of the code if history is any guide.

TRANSITION AND COMMENCEMENT

I1Q1 If each of ASIC's proposals in this consultation paper were to be implemented in an updated Code, what do you think an appropriate transition period would be for commencement of the updated Code? What are your reasons?

Longer lead times preferred given workload and demand on limited resources of smaller ADIs in particular. Preference is for 12 months from the release of the new Code in late 2021 as a minimum. ADI's are working to an overloaded compliance project schedule with a number of projects including Open Banking, Internal Dispute Resolution and Design & Distribution requiring the same skilled resources, in particular within the IT space.