CUSTOMER OWNED BANKING ASSOCIATION

5 April 2019

Jennifer Lyons
Deposit Takers, Credit and Insurers
Australian Securities and Investments Commission
Level 7, 120 Collins Street
Melbourne VIC 3000

Email: ePaymentsCode@asic.gov.au

Dear Ms Lyons

CP 310 Review of the ePayments Code: Scope of the review

COBA welcomes the opportunity to provide a submission to ASIC for its Review of the ePayments Code (the Code). COBA is grateful for the opportunity last year to provide ASIC preliminary views regarding the potential scope of the Review and we appreciate ASIC's transparent approach to consultation.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has $118 billion in assets, 10 per cent of the household deposits market and 4 million customers. Customer owned banking institutions account for around three quarters of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market.

COBA understands that ASIC's Consultation Paper 310 (CP 310) seeks feedback on the topics that ASIC proposes to include in the scope of the Review, and that a second, more substantive consultation paper will be issued later this year, setting out ASIC's proposed modifications to the Code.

COBA considers that regular review of the Code is an important process, particularly given the significant ongoing developments in financial technological payments innovation and the need to ensure that the Code is simple to apply and easy to understand because of its broad application to a diverse range of industry participants.

COBA recognises that the Code is a voluntary code of practice that regulates electronic payments, including automatic teller machine transactions, online payments, BPAY, EFTPOS transactions, credit/debit card transactions and internet and mobile banking. COBA notes that most ADIs in Australia, as well as a small number of other providers of electronic payment services, subscribe to the Code.

COBA notes that Code's requirements apply to any subscribing entity, including entities not subject to the financial services and consumer credit regulatory regimes. We note that these requirements form part of the terms and conditions between a customer and their subscribing financial institution. In this respect, we recognise that any breach of the Code is a breach of the subscriber's contract with their customer and, in some cases, potentially a breach of ASIC-administered law.

This submission elaborates on the preliminary views we provided ASIC last year and also provides our comments on a number of proposals in CP310, with specific focus on the following areas:

- future proofing the Code – Proposal B1
- complaints handling – Proposal B2
- data reporting – Proposal B4

- mistaken internet payments – Proposal B5
- small business access to Code provisions – Proposal B6
- mandatory consumer warning on pass code security requirements, and
- use of third-party aggregation services.

Future Proofing the Code

COBA supports **Proposal B1** 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.

We note, in particular, ASIC's observation in CP 310 that "the current version of the Code has not been able to adapt to the New Payments Platform and consider that it **will not be adaptable, as currently worded**, to any other future payment platforms that may emerge". [Emphasis Added].

COBA would like to offer the following suggestions to support alignment with existing payment platforms and adaptability with emerging developments over the next 5 years before ASIC is required to review the Code again.

- At a broad level, we suggest that the alignment of the Code would be improved if the rules being applied match the payment type being used – that is, VISA, MasterCard, BPAY, NPP, AusPayNet (CS1, CS2, CS3) rules would be the guiding procedures rather than the Code.
- We suggest that the Code capture sending outbound payments using a PayID. While NPP payments can be sent with a BSB and account number, we would still expect similar rules to apply as for payments with direct entry.
- In relation to the NPP, we suggest that the definition of e-payments within the Code be updated to define electronic payments as any payment method other than paper (e.g. cheques, warrant, etc.). We believe that this would help cater for the NPP and contribute to future proofing.

Furthermore, we would encourage ASIC to examine as part of the Review how the Code can be modified to adequately address liability in relation to transactions facilitated through 'payment gateways' (i.e. third-party providers of payment services such as PayPal and Afterpay). Our view is that the Code presently does not adequately address this issue.

Under the Code, card issuers are responsible for investigating unauthorised transactions on behalf of their customers. The investigation must be completed within a set time period and the burden of proof falls upon the card issuer. Generally, where it cannot be reasonably demonstrated that the customer has themselves authorised or otherwise facilitated the transaction, the liability for that transaction falls upon the card issuer.

Where a transaction is made at a merchant using a card, the means of investigating the transaction is typically available to card issuers through the card scheme.

However, where a transaction is made through a payment gateway, the means of investigation are limited to that part of the transaction that occurs through the card network (i.e. payment from the card to the payment gateway). Therefore, the card issuer is essentially responsible under the Code for completing an investigation that it is not able to complete.

While our members have had good experiences with referring customers back to payment gateways, if a customer does not wish to contact the payment gateway and/or their response does not yield either a refund or confirmation that the customer authorised a transaction, the liability returns to the card issuer.

In this context, where a transaction is completed via a payment gateway, our view is that the Code does not recognise:

- the existence of third-party payment providers or payment gateways

- that the transaction is facilitated between the merchant and the payment gateway
- that a clear line of sight on a transaction between a card issuer and merchant extends only from the card issuer as far as the payment gateway, and
- that a payment gateway will not generally provide access to customer accounts or end-to-end transaction details to a card issuer.

Complaints Handling

COBA supports **Proposal B2** to assess the clarity and appropriateness of the current policy positions in the Code's complaints handling provisions.

COBA considers that it would be beneficial to more closely align the complaints handling provisions in the Code with ASIC's RG 165 Licensing: Internal and external dispute resolution. COBA supports AFCA as the external dispute resolution (EDR) mechanism for Code subscribers and consumers.

It is important for consumers to have access to free, impartial and independent EDR, and we believe that Australian consumers benefit from AFCA's legislated approach that is based on procedural fairness, rather than litigation.

With that being said however, COBA members are very concerned about rising costs associated with defending disputes, particularly low-value disputes where members have complied with the Code.

There appears to be a growing trend of baseless complaints being taken to AFCA.

It appears that some consumers may be anticipating that the Code subscriber will settle their claim, without question, solely because the Code subscriber's EDR effort and cost associated with defending the claim far exceeds the disputed value of the complaint.

This unfairly burdens Code subscribers and creates costs that ultimately need to be borne by other customers in the long run. For large financial institutions, this type of situation is more easily absorbed. For smaller institutions however, this only operates as a significant operational burden that diverts limited resources that could otherwise be focussed on product and service innovation.

An AFCA member is required to pay an individual complaint fee if AFCA receives a complaint against that AFCA member. The AFCA fee would then increase if the AFCA member 'pushes back' even if it is to respond to confirm that it has acted in accordance with the Code.

Given the potentially significant financial impact that this process can have on a Code subscriber, we would encourage ASIC to examine this issue in detail as part of the Review.

On a related matter, COBA considers the Code's 6-year complaints procedure limitations period to be too long. In practice, this means that COBA members would be responsible for the resolution of a claim at 5 years and 9 months, for example, where the originator of the transaction is no longer is in operation.

Indeed, given the capabilities of digital banking channels today, it would appear increasingly unlikely that a consumer would not be aware of unauthorised payments on their account 6 years later. On this basis, we suggest that a 3-year complaints procedure limitations period is more appropriate.

Data Reporting

COBA supports **Proposal B4** to review the data reporting requirements in the Code and assess the most valuable and efficient approach.

COBA notes that the Code requires a subscriber to report to ASIC or its agent annually information about unauthorised transactions as specified in a notice published on ASIC's website for the purposes of this clause, and that ASIC must consult with subscribers to determine the specific requirements.

COBA encourages ASIC to report annually, at an aggregated level, on analysis of the data that it is required to collect from Code subscribers. COBA appreciates the aggregate analysis provided in ASIC's CP 310 on unauthorised transactions and mistaken payments, recognising that ASIC's analysis on mistaken payments is based on data from a one-off data collection in 2015 on the causes of mistaken payments.

However, COBA would strongly object to the publication of data at an entity level, as this would likely create confusion. For example, we note from CP 310 that ASIC has "observed a lack of consistency in how subscribers categorise individual types of unauthorised transactions in their information systems"[1].

Going forward, ASIC may wish to consider the merits associated with annually reporting on matters such as mistaken payments, average return time for mistaken payments, amount returned to customers and a breakdown of cause, for example. We believe that annual reporting from ASIC would provide long term benefits to consumers and subscribers, particularly as this would help identify and address potential problems faced by customers and subscribers.

With that being said, COBA considers that it is critical for ASIC to continue its practice of consulting with subscribers to determine the specific requirements of any future data collection. We greatly appreciate ASIC's clear recognition that for many subscribers, particularly smaller ADIs, completing and lodging the data reporting questionnaire is resource intensive and time consuming.

COBA notes from CP 310 that the Australian Payments Network publishes aggregated payments fraud statistics twice a year. We note that there is some overlap between ASIC's data collection and that of the Australian Payments Network. We agree with ASIC that there may not be any benefit in ASIC collecting data that is routinely collected by industry associations and encourage ASIC to continue to work closely with industry to minimise the risk of inadvertently duplicating efforts.

Mistaken Internet Payments

COBA supports ASIC's **Proposal B5** 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.

Our view is that the process for dealing with mistaken internet payments is sufficiently simple for customers to access and understand.

However, COBA considers that the Code can be strengthened to reduce the risk of or prevent mistaken payments and would like to suggest the following warnings for inclusion in the Code:

- We suggest an express requirement in the Code to warn customers that correctly entering the account name will not fix an incorrect BSB or account number and that account name checking is *not conducted* either by the sending ADI or receiving ADI.
- We suggest that NPP outgoing payments paid to a BSB and account number should carry appropriate warnings similar to that of direct entry payments.

COBA notes from the Code that the receiving ADI must use reasonable endeavours to retrieve the funds from the unintended recipient for return to the holder, where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are insufficient funds in the account of the unintended recipient. We would encourage ASIC to provide further guidance in the Code around what constitutes as "reasonable endeavours".

Where a receiving ADI is not satisfied that a mistaken internet payment has occurred, we suggest that the receiving ADI be required to explain why it is not satisfied that a mistaken internet payment has occurred.

[1] ASIC CONSULTATION PAPER 310: Review of the ePayments Code: Scope of the review. Paragraph 84.

Finally, COBA notes that the Code imposes time limits on completing the investigation of a customer claim of a mistaken internet payment. We suggest that ASIC consider prescribing time limits in the Code for the exchange of a customer's information between ADIs, to help expedite resolution of a claim.

Small Business Access to Code Provisions

COBA notes **Proposal B6** to explore whether it may be appropriate to extend the Code, or at least some of its protections, to small business.

We note that similar proposals were explored by ASIC in previous reviews of the Code, and that those review processes concluded that a case had not been made to extend the Code to small business.

To elaborate, it would be prohibitively difficult for subscribing institutions to monitor and confirm when a small business is no longer a small business. This would require inclusion in the Code of a definition/threshold test of what constituted a small business, which would not be practicable and only operate to significantly expand a Code subscribers' compliance risks.

Agreeing to an appropriate definition of small business would also be problematic, particularly given the vast array of different definitions that already exist which Code subscribers need to comply with under different regulatory and reporting frameworks.

COBA notes from CP 310 that supporters of extending the provisions in the Code to small business have previously claimed that "there is little distinction in practice between the banking needs and activities of small business owners and individual customers"[2].

COBA strongly disagree with those claims. In a small business environment, user names and passwords may be assigned to staff other than the principle account holder. Also, small businesses would typically have a significantly higher level of transactions, as they may need to transact with goods and services providers, employees, retail and wholesale clients and different governments on a daily basis. In this respect, they would typically be more experienced and familiar with electronic payments.

Indeed, it would be important for any proposed extension to target a clearly defined problem facing the small business sector. COBA is not aware of any evidence demonstrating a prevalence of electronic banking problems for small business.

COBA's view is that a clear case has not been made to extend the Code to small business. On this basis, the focus of the Code should remain on consumer transactions.

COBA notes ASIC's views in CP 310 that some provisions in the Code (such as the process for retrieving mistaken payments and provisions for allocating liability for unauthorised transactions "could potentially be extended to customers that are small businesses, without any apparent significant additional cost to subscribers"[3].

We strongly encourage ASIC to carefully explore the full potential implications of extending any provisions of the Code to small business to ensure there are no unintended consequences.

Mandatory Consumer Warning on Pass Code Security Requirements

COBA recognises from the Code that subscribers are required to provide a clear, prominent and self-contained notice to customers summarising the pass code security requirements, and that this notice must be included with transaction statements at least annually.

COBA supports the Code's present pass code security requirements. Although we note ASIC's research in CP 310 that findings in other jurisdictions about risk warnings in influencing consumer behaviour in other contexts raise questions about whether the Code's requirements achieve their intended purpose. While we recognise the need to provide clear and appropriate warnings to

[2] ASIC CONSULTATION PAPER 310: Review of the ePayments Code: Scope of the review. Paragraph 107.

[3] ASIC CONSULTATION PAPER 310: Review of the ePayments Code: Scope of the review. Paragraph 106.

customers about the importance of pass code security, this must also be balanced against the importance of optimising a customer's user experience on a computer interface, for example.

Indeed, it is also important to recognise that consumers need to take responsibility for the consequences of their own actions that increase risk (e.g. voluntarily disclosing their pass code to a family member or friend). In this respect, COBA encourages the Review to also examine the whether the Code makes sufficiently clear the responsibility of a customer to protect their own pass code(s).

Use of Third-party Aggregation Services

COBA agrees with ASIC's views in CP 310 that the requirement for customers not to record or disclose their pass code may present practical difficulties or limit their ability to access potentially useful third-party services.

In this respect, we also agree with ASIC that that there is a need to strike an appropriate balance in the Code between providing useful outcomes that take into account customer behaviours and allowing ADIs to expect reasonable protective behaviours by their customers to guard against financial losses.

Our view is that if customers freely disclose their pass code to third party sources for any purpose, and where that disclosure results in financial loss or potential financial loss to the customer (e.g. an unauthorised transaction), liability for that loss should rest with the customer.

However, if that customer's ADI has requested that their pass code be disclosed to a third party, liability for any loss through that third party should rest with their ADI.

On this basis, we suggest ASIC consider incorporating rules in the Code regarding pass code disclosure that are based on whether disclosure of a pass code was sanctioned by a customer's ADI, rather than being based around particular third-party services or service providers.

COBA looks forward to continuing to work with ASIC on progressing the Review. We would welcome an opportunity to participate at the planned ASIC stakeholder discussions in July this year. If you have any questions or comments in relation to any aspect of our submission, please contact Tommy Kiang, Senior Policy Manager...

Yours sincerely

LUKE LAWLER

Director - Policy