PO Box 16193
Collins Street West VIC 8007

12 February 2021

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

Jenny Lyons
Senior Specialist
Credit, Retail Banking & Payments
Australian Securities & Investments Commission
Level 7, 120 Collins Street
MELBOURNE VIC 3000

Dear Jenny

ePayments Code Review

Thank you for the opportunity to provide feedback to the two letters of December 2020 that ASIC has circulated relating to the ePayments Code Review. This letter has been endorsed by Financial Counselling Australia, the Financial Rights Legal Centre, Consumer Action Law Centre and the Australian Privacy Foundation.

We support the submission authored by Financial Rights Legal Centre, dated 18 January 2021, as it pertains to the code's pass code security requirements and ASIC's approach to screen scraping. We note a view that 'screen scraping'—which has inherent risks associated with providing a third-party access to an individual's financial data by giving them secret pass codes—should only be banned when Open Banking is mature as a replacement. The Government's framework for supporting innovation in financial services relies on Open Banking and the Consumer Data Right, so we consider that the sharing of transactions should be within that framework, with its safeguards and protections, rather than outside of it. On this basis, we consider that ASIC needs to reconsider its approach to screen scraping.

CFA offers the following responses in key other areas that ASIC is consulting upon:

- Frauds and scams – CFA is disappointed by ASIC's view that the ePayments Code should not address scams. Payment scams and fraud are increasing, and are a significant area of consumer harm in the area of ePayments. It is unsatisfactory, and a step backwards in consumer protection, for ASIC to take this view. In particular, we oppose the proposed change to the code that the unauthorised transaction provisions apply only to where a person other than the customer has made a transaction without the customer's consent— we consider that where the customer makes the transaction but does so under the control of a fraudster, protection should be provided. This will provide incentives to ADIs and others in the payments sector to better protect against scams and frauds.

- Unauthorised transactions – we support the proposal to clarify that the reporting of an unauthorised transaction is different from a complaint about the unauthorised transaction process or outcome. However, effort must be taken to ensure any changes do not result in customer confusion, fatigue or barriers in accessing the complaints process.

- Mistaken internet payments

    - CFA strongly supports the ePayments Code facilitating a consumer complaint, including via the Australian Financial Complaints Authority (AFCA), against a receiving authorised deposit taking institution (ADI). This is currently a large gap in access to justice. Commonly, a consumer who has made a mistaken payment advances a complaint against their ADI, but the ADI may have done all that is required. They are unable to advance a complaint against the ADI that received the funds, due to limitations in AFCA's rules. We recommend that AFCA's rules be amended to address this gap.

    - CFA considers that the ePayments Code could provide greater guidance about what is required of ADIs when investigating mistaken payment transactions. This could include timeframes and/or factors about the steps that ADIs should take (i.e. greater steps when the funds amount is large, or the customer is experiencing vulnerability). ADIs should also be providing clear and understandable information about what steps that have been taken by ADIs to recover funds, and information about avenues for complaints if funds are not returned.

    - CFA remains dissatisfied with the inability of ADIs to undertake account name and number matching to limit the likelihood of mistaken payments. We consider that while existing warnings are reasonably clear, there remains a reasonable consumer expectation that banks are ensuring transactions are directed to the correct account. We are not convinced that enhanced warnings will address the issue.

    - CFA supports the proposal to make the code payments platform neutral, not linking it to the BECS system but broadening coverage to other forms of payment such as 'pay anyone' functions through the New Payments Platform.

- Pass code requirements — CFA understands the proposal to extend the responsibility of customers to protect their pass code to protection of their own devices. This should only occur if there is adequate default protection at the device level, i.e. the obligation should be

on manufacturers of devices to ensure that devices like phones, fitbits, watches, rings etc cannot be easily accessed fraudulently.

- Compliance and monitoring – CFA considers that the ePayments Code should empower ASIC to collect a range of industry data to inform compliance and its regulatory objectives. This should include an ability to collect data on an ongoing basis, not just one-off. We understand that ASIC has undertaken consumer research about payments issues including unauthorised transactions during 2020. We encourage ASIC to publish this research to inform community understanding and policy dialogue.

- Listing and switching rules – CFA is not convinced that the listing and switching rules have facilitated switching effectively, or there is wide uptake of these services. There are a number of limitations, including that the rules only apply to transaction accounts rather than, for example, credit cards—many customers have recurrent payments attached to credit cards, and can experience similar barriers in switching. Further, the listing of recurrent transactions relates only to those established through the BECS system rather than those established through scheme arrangements (i.e. VISA and Mastercard debit card numbers). Given more and more merchants establish recurrent payments using scheme arrangements rather than using BSB and account numbers, this is inherently limited.

While ASIC's consultation letters did not cover the provision of the ePayments Code that regulate minimum expiry dates for certain non-cash payment facilities, we consider that this provision should be updated in light of the *Treasury Laws Amendment (Gift Cards) Act 2018* (Cth) (**Gift Card Act**).

The Gift Card Act amended the Australian Consumer Law so that a minimum expiry period of three years is required for gift cards. While in general the Australian Consumer Law (**ACL**) does not apply to financial products (including gift cards issued by ADIs, which are instead regulated by ASIC and the ePayments Code), the Gift Card Act also amended the *Competition and Consumer Act 2010* (Cth) (**CCA**) so that even if certain gift cards are a financial product, they are also regulated by the ACL for the purposes of the gift card minimum expiry period reforms (see section 131A(1) of the CCA). As such, it would appear that the ePayments Code is out-of-step with the requirements of the law.

We also suggest that issuers of facilities with stored value (such as gift cards) be required to retain the contact details of customers. These cards usually have to be activated with the issuer, which is a convenient time to do so. We have received reports of cards being cancelled due to suspicious transactions but the issuer not contacting the customer.

Should you have any questions about this submission, please contact me at chair@consumersfederation.org.au.

Yours sincerely

Gerard Brody
Chairperson