PO Box 16193
Collins Street West VIC 8007

19 November 2021

Jenny Lyons
Senior Specialist – Credit & Banking
Australian Securities & Investments Commission

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

Dear Jenny

ePayments Code Review – Final round of consultation

We refer to your letter dated 29 October 2021 seeking final feedback on ASIC's revised proposals for amendments to the ePayments Code. This feedback is provided on behalf of Consumers' Federation of Australia, CHOICE, Consumer Action Law Centre, Consumer Credit Legal Service WA, Financial Counselling Australia, Financial Rights Legal Centre and Westjustice.

Consumer advocates express profound disappointment that ASIC maintains its positions in relation to the proposal to reduce consumer protection within the ePayments Code as it relates to scams, both in relation to the mistaken payments provisions (proposal C3) and those relating to unauthorised transactions (proposal E1). We consider that ASIC should not abide a reduction in consumer protection for scam victims, whether or not it was initially intended for the ePayments Code to apply to scams.

Reducing the existing albeit incidental protections, without replacing them with scam-specific protections, could inadvertently send a signal globally that Australian regulators and governments are not focused on this issue, potentially making Australian consumers more vulnerable to scams. Regulator action should be sending an important message to scammers—that as a nation we take consumer protection seriously and are utilising every method possible to detect, prevent and recover scam losses, as well as prosecute those responsible for scam losses.

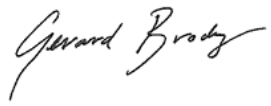
We compare the approach proposed to be taken in Australia compared to that proposed by the UK Payments System Regulator to mandate reimbursement for victims of scams who have done nothing wrong. [i]

We are also disappointed that ASIC disagrees with the position of consumer advocates in relation to mistaken internet payment complaints against receiving authorised deposit taking institutions (ADIs) (position A, table 2).

For the reasons set out in this submission, we urge ASIC to reconsider these positions.

Our response to each of the proposals in the consultation letter are attached.

Yours sincerely



Gerard Brody
Chairperson

[ii] Payment Systems Regulator, CP 21/10 Authorised Push Payment scams consultation paper, available at https://www.psr.org.uk/publications/consultations/cp21-10-app-scams/

Proposal	Response
B1 – Removing requirement for signatories to report annually to ASIC about unauthorised transactions	We oppose this proposal. ASIC's consultation letter did not respond to our June 2021 submissions. Maintaining this position also runs counter to ASIC's stated strategic priorities which states that it seeks 'expand our use of data and digital technology to inform markets and support faster, better regulatory outcomes'.[1] While we support ASIC having an ongoing power to collect a range of data from signatories, it's important that ASIC is able to obtain regular and ongoing data to inform trends. We compare this proposal to that announced by the UK Payment Systems Regulator to require banks to publish data on their performance on scams, and reimbursement levels for victims.[2]
B1 – Retain power to undertake targeted ad hoc compliance monitoring	We support this proposal.
C1 – Amend Mistaken Internet Payment (MIP) provisions of the code so that a receiving ADI, exercising reasonable discretion, can decide (in cases where there are not sufficient funds in the recipient's account) that it is appropriate in the circumstances not to pursue the total amount of the mistaken payment and instead either pursue only a partial return of funds or not pursue any return of funds	We generally support this proposal, and acknowledge that it is appropriate for the receiving ADI to balance the interests of both the sending consumer and unintended recipient. However, we seek clarity about the wording used. The standard to which the receiving ADI is to be held when making the decision to return partial funds is 'exercising reasonable discretion' (proposed clause 32.2). However, proposed clause 32.3 refers to 'reasonable endeavours', which is a different concept to a discretion. We consider that the provision should require the ADI to take action (i.e. to take reasonable endeavours), that is, to consider whether partial return is appropriate, considering the proposed factors. We do not think that the receiving ADI should able to merely elect not to consider partial return under a 'discretion'. In relation to the factors in clause 32.3, we suggest the following: • Removing 'The impact that the passage of time has had on the ADI's ability to distinguish the mistakenly paid funds from funds to which the unintended recipient is entitled'. We consider that the factors should distinguish between whether the 'passage of time' is caused by the receiving ADIs own inaction, or whether the consumer has delayed in reporting the mistaken internet payment. If it includes the former, then this may create incentives for the receiving ADI not to take the necessary inquiries and steps. Moreover, it should not be difficult for a receiving ADI to distinguish the mistakenly paid funds from other funds based on an objective reading of the transaction history. • Clarifying the meaning of 'the need to limit excessive interaction with the unintended recipient'. While we would agree that an unintended recipient should not be badgered, we are concerned that this factor could be used by a recipient ADI to not take required steps so as to avoid contacting the unintended recipient. In some cases, there will need to be appropriate engagement with an unintended recipient.

[1] ASIC corporate plan 2021-2025, available at: https://asic.gov.au/about-asic/corporate-publications/asic-corporate-plan/

[2] Payment Systems Regulator, CP 21/10 Authorised Push Payment scams consultation paper, https://www.psr.org.uk/publications/consultations/cp21-10-app-scams/

Proposal	Response
	• Noting proposal C2(d) below (i.e. that non-cooperation by a receiving ADI or unintended recipient is not a relevant consideration in considering whether an ADI has complied with its obligations), we suggest an additional factor that might oblige an ADI to engage with these parties more than once, e.g. "What actions the sending ADI took in seeking the cooperation of the receiving ADI or unintended recipient, including the number of times a sending ADI attempted to contact one or both of these parties and the different channels of communication if attempted".
C2(a) – Require the sending ADI to investigate whether there was a MIP and send the request for return of funds to the receiving ADI 'as soon as practicable' and, in any case, no later than five business days after the report of the MIP	We reiterate our previous submission that given the low-cost and speed of electronic transactions and requests, a maximum time frame of 5 business days is too long, and consider that this should be reduced to 1-2 days. We acknowledge that the request to return funds must occur 'as soon as practicable', but are concerned that 5 business days may become the default. Such a delay may mean it is less likely that funds are recoverable.
C2(b) - Require both the sending and receiving ADIs to keep reasonable records of the steps they took and what they considered in their investigations	We support the CP341 proposal and consider it should not be weakened. We understand that the information listed would assist AFCA in its dispute resolution role. We note that AFCA's powers to obtain information from firms is limited to firms to which complaints are made about (i.e. the sending ADI), so it is important for the receiving ADI to have code obligations to also provide information. This will enhance access to justice.
C2(c) – Require the sending ADI, when they tell the consumer the outcome of the investigation into the reported MIP, to include details of the consumer's right to: (i) complain to the sending ADI about how the report about the MIP was dealt with; and (ii) complain to AFCA if they are not satisfied with the result.	We support the proposal.
C2(d) – Clarify that non-cooperation by the receiving ADI or the unintended recipient is not a relevant consideration in assessing whether the sending ADI has complied with its obligations.	No comment, although note the above in relation to proposal C1.
C3 - Clarify the definition of 'MIP' to ensure that it only covers actual mistakes inputting the account identifier and does not extend to payments made as a result of scams	We strongly oppose this proposal. This change will contribute to reduced redress for scam victims, given that ASIC admits that the current drafting of the code has offered redress for consumers. ASIC should not abide by such a reduction in consumer protection. ASIC states that the general law protections against scams remain, and that AFCA will still have its ability to consider matters of fairness and reasonableness in reaching determinations in scam related disputes. As stated in our June 2021 submission, we consider that in absence of clear regulatory standards in relation to

Proposal	Response
	the level of diligence an ADI should take in detecting, preventing and recovering scam losses, consumers will continue to suffer substantial losses with little ability to obtain redress. Our June 2021 submission set out a range of existing legal principles as well as details of case law which provide some guidance about what steps an ADI should take. Despite these principles, there remains a lack of clarity about a consistent standard expected of ADIs. This lack of clarity results in AFCA making statements in determinations such as 'banks do not have a general obligation or duty of care to observe or monitor customers' transactions, or to maintain watching briefs of scams for its customers' benefit'.[3] We consider this to be wrong at law, as it ignores ADIs' contractual duty to question a valid mandate, that is, that they should exercise reasonable care and skill to ensure that transactions processed are consistent with a customer's wishes. This duty is very relevant for scam transactions. We note that the Australian Banking Association agrees that there is a lack of clarity in the relevant standard for ADIs, with its submission stating that it 'sees value in ASIC issuing guidance or similar instrument specifically about scams, which could also guide AFCA's decision making. We consider this would be an important step to maintain clarity about ADIs' obligations and regulator/AFCA expectations'. Given this, we urge ASIC to not make the change proposed until there is clarity in regulation as to the standard expected of ADIs in detecting, preventing and recovering scam losses. To proceed with this change without such a regulatory standard will reduce the expectation that ADIs take steps to identify and prevent scams where it is in their power to do so and reduce the ability of a consumer to recover scam losses from an ADI indefinitely. This change also runs counter to ASIC's commitment to reduce risk of harm to consumers associated with increased scam activity in its 2021-2025 Corporate plan.[4] We do not agree with ASIC's concern that the 'evolving' nature of scams means that it would be difficult to codify the appropriate responses expected of ADIs. Whether it is in the ePayments Code or another regulatory instrument, there is a need to adopt standards similar to that in the UK Contingent Reimbursement Code for Authorised Push Payment Scams. This code provides for a fair system of redress for consumers, and has been able to respond to the evolving nature of scams. Recent data from the UK Financial Ombudsman Service shows that 73% of determinations relating to authorised push payment fraud were upheld in favour of the consumer, showing that a clear standard can contribute to customer redress.[5] It is appropriate that

[3] E.g. AFCA Determination 783198
[4] ASIC Corporate Plan 2021-2025, https://asic.gov.au/about-asic/corporate-publications/asic-corporate-plan/
[5] See: https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/

Proposal	Response
	financial firms bear greater liability for these sorts of scams given they are in a much better position to identify fraud risk and invest in capabilities to mitigate such risk. Furthermore, codes play a critical role in the regulation of financial services in complementing other regulatory requirements – especially where more detail is required. As such they need to be living documents that adapt with fast changing, highly dynamic sectors. To stay relevant Codes need to be nimble reviewed, redrafted and updated regularly to meet changes in the financial services environment. They also need to be supported with resources to do so otherwise they become irrelevant. These expectations of Code evolution are placed on industry in their self-regulatory codes with regular three-year reviews and the ability to update these Codes between those times where appropriate. These expectations placed on industry Code administrators must be similarly applied to the administration of this Code. We note that this current review has been ongoing since 2018. In this time ASIC could have undertaken the "significant redrafting of the Code to capture the factors contributing to scams and the appropriate responses by ADIs" that ASIC suggests is a barrier. If ASIC continues to consider that the "code is not the appropriate vehicle for addressing scams and dealing with their complexity" then it must detail what the appropriate vehicle is since the ABA's position outlined above suggests ASIC being kept abreast of industry approaches and devised solutions will not be enough to fill the regulatory gap and uncertainty being created by this decision.
C4 – Provide additional important information in the on-screen warning about mistaken internet payments required by clause 25 of the Code, including a call to action to check the BSB and account number, and wording to the effect that if funds are sent somewhere other than the intended recipient, the consumer may not get their money back.	While we don't oppose this proposal, we maintain that it would be more effective for the code to require account number and name matching. In relation to the proposal to set an expectation of best practice (separately from the Code) for subscribers to test, learn and adapt their warnings according to impacts on their customers, we consider that this should be done in a transparent way with engagement from consumer advocates.
D1 & D2 – relate to small business	No comment
E1(a) – Clarify that the unauthorised transactions provisions only apply where a third party has made a transaction on a consumer's account without the consumer's consent and do not apply where the consumer has made the transaction themselves as a result of misunderstanding or falling victim to a scam)	We strongly oppose this change for the reasons set out in response to proposal C3 above.

Proposal	Response
E1(b) - Clarify that the pass code security requirements mean that consumers are unable to disclose their pass codes to anyone (subject to the exceptions in clauses 12.8 and 12.9 of the Code) and, if they do and the subscriber can prove on the balance of probability that the disclosure contributed to an unauthorised transaction, the consumer will not be able to get indemnity from the subscriber for that loss E1(c) - Provide some examples of scenarios that amount to express or implicit promotion, endorsement or authorisation o the use of a service referred to in clause 12.9 of the Code. (d) Clarify that a breach of the pass code security requirements by itself is not sufficient to find a consumer liable for an unauthorised transaction—the subscriber must, in addition, prove on the balance of probability that the consumer's breach of the pass code security requirements contributed to the loss.	We support clarification that a code signatory must prove that the consumer's breach of the pass code security requirements contributed to the loss before an institution can deny liability. However, we maintain our previous view that the ePayments Code should effectively prohibit screen scraping or data capture outside the safeguards of the Consumer Data Right regime. We also oppose the proposed clarification (in the form of a note) that a subscriber has not approved a customer's use of a particular screen scraping service merely because the subscriber has chosen to use that service provider for its own purposes or has failed to actively prevent a particular customer behaviour. We consider that if subscribers are promoting the use of screen scraping technology in their general operations, then it is manifestly unfair to then place the risk of loss associated with using that technology on the consumer. We note that in its New Proposal B, ASIC takes the view that what amounts to disclosure will turn heavily on the individual circumstances, and that it is willing to let potentially clear-cut situations (duress, financial abuse) be considered by internal investigation and/or AFCA determinations rather than codified definitions. We consider that an explanatory note that potentially provides for a wide set of circumstances in which a subscriber is not responsible for the circumstances of a disclosure runs counter to that approach.
F1 – Define and incorporate biometric authentication into the code.	We support the proposal
F2(a) – Not proceed with the proposal to revise the code's use of the term 'device' and instead refer to 'payment instrument'.	No comment
F2(b) – Include virtual debit and credit cards in the definition of 'payment instrument'	We support the proposal
F3(a) – expressly extend all relevant provision to situations in which a 'pay anyone' payment is made through the NPP.	We support the proposal
F3(b) – Add a definition of 'Pay Anyone internet banking facility' as a facility where a consumer can make a payment from the consumer's account to the account of another person by entering, selecting or using a BSB and account number or PayID or other identifier that matches the account of another person	We support the proposal, including for the terminology to also cover mobile and telephone banking.

Proposal	Response
F4 – Amend the Code to cover the provision of electronic transaction receipts as well as paper receipts, with a carve out for EFT transactions from clause 5.3	No comment
G1(a) – Replace references to Regulatory Guide 165 Licensing: Internal and external dispute resolution (RG 165) with references to Regulatory Guide 271 Internal dispute resolution (RG 271) with chapter F of the code to be adjusted to reflect new settings in RG271	We support the proposal
G1(b) – Combine Chapter F and Appendix A so that complaints handling requirements are contained in a single framework instead of two, while retaining important differences in relation to unauthorised transaction report investigations	We support this proposal.
G1(c) – Require all subscribers to have IDR procedures that are set out in RG 271, except those that are not already required to meet this standard.	We understand that ASIC will engage with subscribers that are not required to comply with RG271 but are required to comply with AS/NZ 10002:2014 on complaint handling. We support there being consistency in the standards across all subscribers.
G1(d) – Not require all subscribers to be members of AFCA	We do not support this proposal. We consider that all subscribers should be members of AFCA if they are not required to be members already.
H1 – Align the facility expiry period in the Code with the expiry period in the Australian Consumer Law, which is 36 months, via a note.	We support this proposal.
I1 – Apply 12-month transition period before the updated Code commences.	This review has been going on for more than 2 years. Given this, we consider that a 6-month transition period should suffice.
New Proposal A – Do not alter the settings in the Code or consider changing AFCA Rules to accommodate complaints against the receiving ADI but discuss with industry the possibility of developing industry best practice principles for actions/behaviour of the receiving ADI	CFA strongly opposes this proposal. The inability to make a complaint against a receiving ADI has been a long-standing issue, and this review of the code is the opportune time to remedy this to promote access to justice. As stated in our submission, there are many instances where complaints can be made to AFCA notwithstanding there being no provision of a financial service. ASIC says that this has only been included where there has been 'detailed policy consideration'. The current review—which has been ongoing since 2018—has been and remains the perfect opportunity for such policy consideration. ASIC states that it could explore including a special exception in AFCA's rules. We strongly suggest that this exploration occur through a dedicated consultation. In response to ASIC's concerns about privacy of the unintended recipient, there does not appear to be a requirement to interfere with their privacy – the complaint is against the receiving ADI, and any complaint could mask their identity. Further, in relation to

Proposal	Response
	ASIC's concern that this may result in multiple complaints against a sending and receiving ADI, we do not see why this is a barrier. In appropriate matters, the parties could be joined to one complaint. We do not consider that a special exception would require any significant change to AFCA Rule 6.2 or its Operational Guidance. ASIC states that industry has indicated that it can develop a solution outside the code. It is very difficult to comment on this without any information about what this solution looks like.
New Proposal B – Unauthorised transactions: Do not consider any changes to the Code to define what amounts to 'disclosure' (e.g. in the case of screen scraping) or 'voluntary disclosure' (e.g. in the case of financial abuse or duress, arguably affecting the voluntary nature of the disclosure). Instead, this should be left for consideration by the subscriber (and AFCA) in individual cases when considering the customer's level of contribution to the unauthorised transaction.	We generally support this proposal, noting that AFCA can use its fairness jurisdiction in a particular case to determine what amounts to disclosure. However, we consider that it could be made celar that disclosure is not voluntary where its provided pursuant to undue duress in family violence situations. As noted above, we als o consider that where a signatory promotes the use of screen scraping, it cannot then take the position that the consumer ahs 'disclosed' their pass code such that leaves them liable for losses.
New Proposal C - Amend the existing Note 1 under clause 12.4 (regarding storage of credentials on computers, etc.) to remove the reference to 'Blackberry	We support this proposal.
New Proposal D – Clarify that the definition of 'pass code' includes one-time pass codes	We support this proposal
New Proposal E – Clarify that the definition of 'identifier' includes 'tokens' (i.e. tokenisation)	We support this proposal
New Proposal F – Consider defining 'complete identifier' in clause 5.3(a)	No comment
New Proposal G – Consider replacing references in Chapter F to 'complaints' about unauthorised transactions with 'report' (or similar) of an unauthorised transaction. Also, relocate aspects of Chapter F ('Complaints') of the Code to Chapter C ('Unauthorised transactions') that deal with investigation of unauthorised transactions, so that all aspects of the UT investigation process are housed within Chapter C.	We generally support this proposal, however we seek clarity that the outcome is not to reduce the rights of consumers who make unauthorised transaction reports and/or complaints.

Proposal	Response
Leave Ch F as very basic – containing only the requirement that subscribers must comply with RG 271. Despite the above, we would retain the current 6-year limitation period for reporting unauthorised transactions	
New Proposal H – Specify that clause 4.8 (expiry dates) does not apply to credit and debit cards (but clarify that reloadable scheme cards are not subject to this carve out).	We support this proposal
New Proposal I – We do not propose to increase the threshold for the code's tailored low-value facility requirements from $500 to $1000	We support this proposal
New Proposal J – Update the privacy guidelines in clause 22 to reflect the current state of the law	We support this proposal
Other issues	We express disappointment that ASIC has not responded to the concerns about card scheme updater services and recurrent payments outlined on pages 10 and 11 of CFA's June 2021 submission.