Australian Banking Association

02 July 2021

Jennifer Lyons
Senior Specialist - Credit and Banking
Financial Services and Wealth
Australian Securities and Investments Commission

Dear Jenny

Review of the ePayments Code: Further consultation

The Australian Banking Association (**ABA**) welcomes the opportunity to provide feedback on Consultation Paper 341, Review of the ePayments Code: Further consultation (**CP 341**). The ABA advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

The ABA's key responses are:

- ABA supports proposals to clarify the definition of a mistaken internet payment (**MIP**), and broadly supports the proposal to clarify the definition of unauthorised transactions. ABA has discussed with regulators there will be a need for a more responsive instrument, such as regulatory guidance, that is more appropriate to deal with scams and ensure that any rights or protections afforded to victims of scams are available in an equitable manner. ABA also asks ASIC to further consider:
  - Excluding all scams from the term unauthorised transactions, or ensure the drafting of the definition provides maximum clarity about what is within scope of the ePayments Code (**ePC**).
  - Further clarifying a number of matters such as the contribution rule, the concept of voluntary disclosure and extreme carelessness.
- Further work is needed to assess the case and benefits of the proposal to extend the ePC to small business. This includes a clearer articulation of the problem ASIC is seeking to address and how these can be addressed by extending the consumer-oriented protections in the ePC. The current proposal will create uncertainty for both banks and their small business customers about rights and obligations in relation to MIP and unauthorised transactions. It would also be unnecessarily complex to administer. ABA asks ASIC to consult further with the payments industry and stakeholders.
- While ABA supports modernising the Code, we consider the proposals about biometrics and virtual cards need further work. ABA also asks ASIC to consider a more fulsome modernisation of the Code.
- Given the further questions identified, ABA asks ASIC to consider a two-stage approach to amending the Code:
  - First, clarifying the definitions of MIP and unauthorised transactions, potentially in conjunction with the proposed guidance on scams. This would ensure industry, AFCA and consumers have a clear frame of reference for dealing with scams and avoid delaying AFCA's work on the scams fact sheet.
  - Second, refine potential amendments to modernise the Code and considering further the details of any extension to small businesses.

Australian Banking Association

ABA's detailed responses to CP 341 are in the Attachment.

ABA would appreciate the opportunity to discuss these responses with ASIC, prior to the next stage of consultation. If you have any questions, please contact me on rhonda.luo@ausbanking.org.au or 0430 724 852.

Yours sincerely

Rhonda Luo
Policy Director

Australian Banking Association

Attachment: ABA response to CP 341

Introductory comments: sequencing and modernising the ePC

Issue	ABA comments
Modernising the ePC	ABA welcomes ASIC's proposal to modernise the ePC. The ePC was issued in 2011. Since that time, we have seen significant changes in how consumers access, make and receive electronic payments. Further changes in the nature of services and service providers are expected. ABA has provided comments on the specific proposals. Modernising the ePC also goes to the role of the ePC in protecting consumers in online and digital payments. The safety of online and digital payments are increasingly dependent on access/security of phone/tablet, apps; banks and other institutions have dedicated considerable resources to provide information and support to their customers when accessing online services; on the whole, consumers have become much more sophisticated in their knowledge and understanding of electronic and online payments and have shown ability to adopt online services. In this environment, the ABA believes the ePC can be reviewed to reflect these additional matters. • The ePC includes specific references to things like Blackberries, and whether a user has recorded passcodes on a computer that is not password protected. • While these references are outdated, they suggest the ePC is intended to be comprehensive about how consumers can protect themselves when using electronic payments (including their use of electronic devices whose manufacturers were not ePC subscribers), and what subscribers' obligations are on matters affecting access to/use of electronic payments. • By analogy, the ePC should address how consumers are using electronic devices to access online and digital payments, including phones/tablets, PCs and apps. For example, instead of an example on 'extreme carelessness' about keeping passcode on a computer that's not password protected, and in a file called 'internet banking codes', the current equivalent might be a customer allowing another person remote access to their computer/phone and giving away passwords/one time password (OTP), or allowing remote access to their

	computer or phone while logging into internet banking. Also refer ABA comments relating to unauthorised transactions. • Existing proposals to modernise the ePC also require ASIC to consider how consumers use phones or other electronic devices. Refer ABA comments on biometric and device security, and 'loss' of virtual cards. ABA also asks ASIC to consider whether the ePC will need to deal with new payments innovation and features. For example, how does the concept of unauthorised transactions apply when consumers consent to third party payment initiation under Consumer Data Right (CDR).
Sequencing of reforms	ABA asks ASIC to make the more limited amendments re MIP and unauthorised transactions as a first tranche; followed by a second tranche that looks at small business extension and a more fulsome effort to modernise the ePC. With this sequencing, industry would have time to provide further proposals on modernising the ePC and the issues affecting small businesses and payments.

B. Compliance monitoring and data collection

Proposal	Questions	ABA response
We propose to do the following: (a) remove the requirement in clause 44.1 of the Code that subscribers must report annually to ASIC or its agent information about unauthorised transactions; and (b) retain ASIC's power to undertake ad hoc targeted compliance monitoring	B1Q1 Do you support removal of the requirement in clause 44.1? If not, why not? B1Q2 What are the costs to subscribers of ASIC continuing an annual collection of data on unauthorised transactions? How does this compare to the potential costs and benefits or savings of ASIC instead relying on its ad hoc monitoring power in the Code?	ABA supports the removal of the requirement in clause 44.1 Recommencing recurring annual data collection after an extended pause would require subscribers to incur costs to re-establish data collection and reporting programs. In principle, ABA supports the proposal for ASIC to rely on its ad hoc monitoring power in the Code, instead of requiring annual data reporting. This is subject to ASIC: • Consulting industry to minimise the manual work required to respond to a data request while still giving ASIC the information it requires; • Giving relevant subscribers prior notice of the proposed data collection (such as through consultation);

(presently in clause 44.2), but specify two distinct functions: (i) monitoring subscribers' compliance with Code obligations (which already exists in clause 44.2); and (ii) monitoring or surveying matters relevant to subscribers' activities relating to electronic payments.	B1Q3 Do you see any possibility for industry-led recurrent data collection and reporting in relation to unauthorised transactions? What would be the costs of setting up and maintaining such an initiative, and who would be well placed to conduct it?	• Consider other ways to streamline the request, for example obtaining data from third parties where banks have provided similar data to those third parties. The feasibility and cost of industry-led recurring data collection would depend on the scope of proposed data collection. AusPayNet has described the role that the AFCX could play, noting however the AFCX's membership does not include all subscribers to the ePC. Requiring industry to establish a new, recurring data collection program that includes all subscribers can be a costly exercise for some subscribers. The relative merits of an industry-led data collection program may also be diminished if ASIC will also use its ad hoc data collection powers under the ePC, as subscribers would be required to comply with a recurring data collection program as well as respond to ad hoc data requests.
	B1Q4 Do you support the additional monitoring or surveying function in proposal B1(b)(ii)? If not, why not? B1Q5 What are the expected costs to subscribers of the additional monitoring or surveying function mentioned in proposal B1(b)(ii)?	ABA seeks further clarity on the proposed monitoring power in Proposal B1(b)(ii), in particular whether the proposal to cover 'activities relating to electronic payments' would go beyond 'compliance monitoring of specific obligations under the Code' (the current clause 44.2). If the proposal can extend beyond monitoring compliance with matters specified in the Code, and extend to other electronic payments activities, then proposal B1(b)(ii) could increase the cost of complying with ASIC's monitoring requests. However, this may not be the case if ASIC takes into account the issues set out above on ways to minimise the cost of data requests while maintaining the effectiveness of ASIC monitoring.

C. Clarifying and enhancing the MIP framework

Proposal	Questions	ABA response
We propose to amend the Code so that: (a) the processes in clauses 28, 29 and 30 apply not only where there	C1Q1 Are there any special considerations to justify not applying the processes in clauses 28, 29 and 30 to situations in which only partial funds are available in	ABA has considered this proposal in context of the ePC's current application to retail consumer payments. The following comments do not necessarily apply if the ePC is extended to small businesses. Refer to ABA comments about the questions that need to be resolved including how the concept of mistaken internet payment could apply to business payments.

are sufficient credit funds available in the recipient's account to cover the mistaken internet payment (current application) but also where only a portion of the funds is available in the recipient's account (so that the consumer has an opportunity to retrieve at least a portion of the mistaken internet payment);

(b) it includes non-exhaustive examples of what a receiving ADI can do to meet the requirement to make 'reasonable endeavours' to retrieve the consumer's funds, while clarifying that these examples are guidance only and are neither a 'safe harbour' nor prescribed actions that the receiving ADI must in every case take; and

(c) proposals C2(a) and (b) operate together—that is, the receiving ADI must seek return of the partial (if any) funds and make reasonable endeavours to the unintended recipient's account?

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

ABA agrees with proposal C1 subject to the following requests for clarification and issues for resolution. This extension would improve trust with our customers that we have done all that we can for them. It can improve co-operation, collaboration and trust across subscribers.

However, the circumstances where it may be appropriate to provide a partial refund from a customer's account, and the factors that may mean this is not appropriate, can be more complex and require more nuanced decisions from the receiving ADI. As such, the receiving ADI should have an obligation to consider whether a partial refund is possible and appropriate but should not have an absolute obligation to provide a partial refund.

Some of the factors, including operational issues, that a receiving ADI may need to consider before providing a partial refund for a MIP are set out here:

- Is there a minimum amount that needs to left in the customer account when retrieving a partial MIP, i.e, an account cannot be drawn below x dollars.
- Is there a threshold/minimum amount that can be retrieved as part of the partial MIP, i.e, what is the minimum that can be recovered ($1 or another amount).
- Are there protections in place to ensure here would be no return of funds if customer has received payments of CentreLink benefits in the account that has received the mistaken payment. For these payments, a bank must leave 90% of their benefit in the customer's account. Also consider circumstances where a customer receives these benefits into another account held with the receiving ADI.
- Similarly allow subscribers some discretion to respond to customer's circumstances, i.e, not to put the customer in hardship or where the receiving ADI is aware of particular vulnerabilities.
- Consider implications for an unintended recipient that is a small businesses, e.g, ability of a small business to process payroll. Note small business accounts can be the uninintended recipient when payment is made from a consumer account, irrespective of whether the ePC is extended to small business customers.

retrieve the remainder of the funds.

- Is there a limit to the number of partial MIP returns that can occur or the period of time during which recovery can be attempted. Who would own responsibility for these decisions.
- If a customer has recovered partial funds are they able to request additional attempts in an effort to recover additional funds.

If ASIC proceeds with this proposal, ABA asks ASIC to clarify these questions. Some matters could be done in the ePC and via guidance; industry also seeks discussions with AFCA and ASIC to clarify how complaints about partial refunds would be considered by AFCA.

The ePC should also:

- Clarify that while the ability for the receiving ADI to consider the particular circumstances of the customer should exist, it does not impose an additional obligation for the receiving ADI to make specific inquiries about the customer's circumstances. Instead the receiving ADI should be able to rely on the information it holds about a customer at the time the refund is requested in determining whether a partial refund is appropriate.
- Specify the timeframes for requesting, initiating, responding and attempting a partial refund, and whether this would be from the time of a customer request or the sending ADI's determination there was a MIP, taking into account the questions raised.

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?

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

ABA generally supports the industry having guidance around 'reasonable endeavours'. ABA sees value in having non-exhaustive examples but asks ASIC to work with industry to identify the examples that help to provide clarity and consider where such guidance is appropriate to be included.

The term 'reasonable endeavours' is very broad and can be open for interpretation by subscribers and by AFCA. Having examples will clarify the expectations for banks and AFCA, but it could raise expectations in some customers about their ability to obtain a full or partial refund, which may not be the appropriate outcome in a particular case (note some customers also have expectations about being given information about the recipient of the mistaken payment). As such any examples would need to be carefully considered to weigh these competing considerations and clearly express the need for the appropriate

	C1Q5 What types of factors might affect whether a particular action is necessary to satisfy 'reasonable endeavours' in individual cases?	amount of discretion for the sending and receiving ADIs to consider the factors set out above. Subject to the balancing of competing considerations, it would be useful for the ePC or other guidance to clarify expectations on the receiving ADI including: • Where the unintended recipient is non-responsive to receiving ADI requests, including how many repeated attempts to make contact, and by what channels, constitutes 'reasonable'. • Length of hold. • Where the unintended recipient is not agreeable to repayment by instalment. • Where the unintended recipient proposes an impractical repayment plan, e.g, over 20 years. • Activity or potential to hold or recover funds from linked account/s, ie, where the customer closes the account to which the funds were sent, but still has other accounts with the bank. • Status of the account into which the funds were deposited, e.g, if the account is closed.
	C1Q6 Are there any practical impediments to implementation of the proposals at C2? C1Q7 What are the costs to subscribers of extending the MIP framework to cover the partial return of funds?	The practicality of implementation of the proposals at C1 would depend on the details of any absolute obligations created by the ePC and the sending and receiving ADIs' discretion to consider the factors set out above. For example, if the ePC is drafted so as to require the receiving ADIs to consider whether it is appropriate to provide a partial return of funds and making reasonable endeavours to retrieve the remainder, this should not present significant practical impediments.
We propose to amend the Code to: (a) require the sending ADI to investigate whether there was a mistaken internet payment and	C2Q1 Do you agree with the proposed timeframe in proposal C2(a)? If not, why not? C2Q2 What are the costs associated with compliance	ABA agrees with the proposed timeline. In addition we ask ASIC to discuss with AFCA to ensure expectations for subscribers are aligned. ABA considers this change should not impose significant implementation and compliance cost if:

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 mistaken internet payment;

(b) require both the sending and receiving ADIs to keep reasonable records of the steps they took and what they considered in their investigations;

(c) require the sending ADI, when they tell the consumer the outcome of the investigation into the reported mistaken internet payment, to include details of the consumer's right to: (i) complain to the sending ADI about how the report about the mistaken internet payment was dealt with; and (ii) complain to AFCA if they are not satisfied with the result; and

(d) clarify that non-cooperation by the receiving ADI or the unintended recipient is, by itself, not a relevant

with the proposed timeframe?

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

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

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?

- The ePC is drafted so as to address the issues raised in C1 about the details of any obligations and degree of discretion.
- ASIC works with industry and AFCA to clarify further points of detail relating to timeframes, such as whether an investigation as to whether a MIP has occurred needs to be completed by the sending or receiving ADI before a request can be sent.
- Having a reasonable period to implement changes to process and/or policy.

Subject to the above, subscribers will expect to incur the following costs:

- Updating business process to ensure partial refund requests are done in compliance with ePC requirements.
- Updating record keeping and management.
- Material to advice consumers of updated changes.

ABA also seeks clarity about the proposal to require a receiving ADI to comply with an AFCA decision about whether a MIP has occurred: would AFCA have the ability to determine a MIP has occurred when the ADI(s) have determined a transaction was not a MIP; and if so on when AFCA would be able to do so. The drafting in the ePC should be clear that AFCA should only be able determine a MIP has occurred if AFCA has evidence that clearly contradicts the investigation and outcome decision of the ADI(s).

consideration in assessing whether the sending ADI has complied with its obligations.

We propose to amend the Code to clarify the definition of 'mistaken internet payment' to ensure that it only covers actual mistakes inputting the account identifier and does not extend to payments made as a result of scams.

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

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.

(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').

ABA supports the proposed clarification if ASIC adopts the definition set out in C3Q2.

The MIPs regime is designed for genuine mistakes made by customers where the customer has inputted or selected intended account details incorrectly, that is, genuine typographical or fat finger errors. These are generally able to follow the MIP process where both sending and receiving ADIs are satisfied that a mistake has occurred and funds are able to be recovered.

However, where the receiving ADI is unable to be satisfied on the face of it that a mistake has occurred, the protocol for MIPs can take many days, requiring the receiving party to agree for the funds to be returned. These issues would make MIP processes inappropriate for attempting to retrieve scam funds (i.e, the speed with which funds can be withdrawn from scam accounts, accounts cannot be frozen in MIP cases).

Adopting the proposed definition in C3Q2(a) would mean scams can be dealt with more quickly and increase the chances of at least some funds being recovered, rather than go through the MIP process. As such ABA believes this change can help some customers who become involved in a scam.

The definition should exclude (in the Code provision or by examples):

- Email Hack/scams where a customer is instructed to make payment where the details have been changed purposely by a scammer.
- Cases where the compromise of the account identifiers occurs outside banking systems.
- Other authorised push payments scams, most notably Business Email Compromises. These are not mistakes as a purely typographical error.
- Cases where evidence shows a customer changed their mind after making the payment, i.e, in a buy/sell scam.

ABA reiterates we see 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.

We propose to require ADIs to provide additional important information in the on-screen warning about mistaken internet payments required by clause 25 of the Code. The messaging must:

(a) contain a 'call to action' for the consumer to check that the BSB and account number are correct; and

(b) in plain English, include wording to the effect that:

(i) the consumer's money will be sent to somewhere other than to the intended account; and

(ii) the consumer may not get their money back, if the BSB or account number they provide is wrong (even if the consumer has given the correct account name).

C4Q1 Do you support our proposals? If not, why not?

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?

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

ABA agrees with this proposal and notes some subscribers have implemented such consumer warnings.

The warning should clearly state consumers should check they have given the correct BSB and account numbers. It should state the banks do not check whether the BSB/account number matches the account name (this includes the sending and receiving bank). It should alert consumers to the implications if they do not take adequate care about payment processes (i.e, their money goes where they did not intend).

ABA asks ASIC to consider when this warning should be displayed, i.e, only when a new payee is set up, or also where a customer is paying an existing payee or where internet banking details are updated. Guidance informed by consumer research may be useful, noting too many pop up warnings can introduce unnecessary friction and may reduce the effectiveness of the warnings.

ABA considers the ePC provision should provide an example or benchmark of what the warning should contain. It should not prescribe the form of words that subscribers must use. This would allow flexibility for subscribers to adapt this warning to the style or tone of their customer communications.

ABA also notes there are technical solutions currently available for a majority of consumers to mitigate the risk of a mistaken payment, namely using PayID. Where PayID is available, using PayID is a decision for each consumer (noting not all subscribers have the capability to initiate a PayID transaction). ABA believes this matter does not require a policy decision from government, instead it requires industry, regulators and stakeholders to explain existing solutions to consumers.

Australian Banking Association

D. Extending the Code to small business

Proposal	Detailed questions	ABA response
We propose that: (a) The Code will apply to protect small businesses in relation to a subscriber unless the subscriber opts out by notifying ASIC, we publish the subscriber's opted-out status on our website and the subscriber includes notification of its opted-out status in its terms and conditions with small business customers; (b) the Code will apply to small businesses who acquire their facilities in question on or after the date on which the new Code commences (i.e. the extension to small businesses will not operate retrospectively); (c) the term 'user' (referred to in clause 2.1) will be modified to include 'small businesses' and their employees, contractors or agents; and (d) after the first 12 months, ASIC will review the number of subscribers	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? 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? D1Q3 Please provide any information you have about the nature and extent of problems for small businesses in relation to electronic payments and about how small businesses would benefit (or not) from having the same protections as individual consumers under the Code?	ABA does not support an opt-out arrangement for individual subscribers in relation to small business coverage under the ePC. • Having the opt-out mechanism solely in relation to small business coverage (but not for the rest of the ePC) would make the scope and application of the Code unclear, particularly for business customers. • It is currently voluntary to subscribe to the ePC. Query why ASIC proposes to include a voluntary regime within a voluntary regime. • To the extent there are doubts about the benefits and costs of an extension to small business, and / or questions about whether extending the ePC is the preferred way to achieve a policy outcome, ASIC should do further analysis about this question – potentially as part of the work to make the ePC mandatory – rather than leaving a significant regulatory policy question for individual industry participants to decide. ABA considers further work needs to be done to identify a regulatory policy rationale for the proposed extension to small business, and to consider how it can be done. ABA understands the intention of the ePC is to provide retail consumers confidence to use online banking services. Given this policy context, questions that have yet to be fully considered by ASIC include: The nature of payments issues that small business (and other business) owners face can be different from consumer payments, ie, businesses are more likely to have payment disputes rather than 'mistaken' payments. The ePC currently defines which consumer transactions are protected (cl 2.4 and 2.5). If this proposal proceeds, ASIC would need to undertake a similar assessment. The types of payment facilities used by a business can also be different, ie: file-based direct entry payments, HICAP, Commercial Cards, Merchant Acquiring. Extending the ePC to all small business payment transactions as proposed would apply the ePC to some complex products that

who have opted out and will consider options for any enhancements to the experience under the Code for both subscribers and small businesses	are not compatible with the ePC. Some banks may offer small business customers the use of a payment platform that is subject to its own set of security and authentication requirements and procedures, which are tailored to the needs of small businesses (as compared to individuals). These authentication requirements and procedures are unlikely to align with the liability framework in the ePC. We also query whether AFCA is the appropriate body to hear and resolve business payment disputes. Prior to a decision to extend the ePC, further work would need to be undertaken on questions such as how to determine whether a payment was an error; the liability for a small business whose staff, contractors or agents breaches the PSR requirements. For example, • The question of unauthorised transactions will be more complex because rather than just the account holder/s accessing the account, it will be a number of other people authorised to do so. It may be more difficult for both the business and the subscriber to determine and prove whether or not a transaction was authorised. • The proposal to modify the definition of "user" so an employee, contractor or agent of the business will be considered to be authorised to make the payment, does not give any regard to the mandate between the customer and the bank, and who has been authorised to transact on behalf of the customer. For example, if a contractor to a small business conducts a transaction outside the permission granted to that individual, it is not clear how AFCA would assess a dispute lodged by the small business. By comparison, Part 6 of the Banking Code is a stand-alone part that specifically addresses lending to small businesses, it does not purport to extend other Parts of the Code to small businesses. Further, some of the complexities highlighted above also do not necessarily arise in context of credit and lending decisions.
D1Q4 What are the costs and benefits for industry of our proposal?	Refer D1Q3 and D2.
D1Q5 Do you agree with our proposal D1(b), that the Code should not apply	ABA opposes the proposal to establish a voluntary opt-out mechanism within the ePC.

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?	If this proposal proceeds, ABA does not support the proposal to only apply the Code to payment facilities acquired on or after the date of commencement of the updated ePC. Small businesses may be uncertain about the protections they can receive, if some of their payment facilities are eligible for protection and others are not because of changes in their number of employees over time. Instead, if this proposal proceeds, ABA proposes an alternative approach based on the eligibility of the entity and transaction, at the date of the transaction. This would provide maximum clarity for all parties because: • If a business is eligible, all transactions made under eligible facilities would be protected by the ePC. • If a business ceases to be eligible, none of their transactions would be protected by the ePC. ABA notes this approach would require subscribers to maintain records about the number of employees over time, as such, further discussions with the payments industry and stakeholders about the pros and cons would be necessary.
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.	Refer D1Q3. ABA also highlights that the proposed definition is not consistent with limits to AFCA's jurisdiction.
D1Q7 Does our proposed change to the definition of 'user' (by including employees, contractors or agents of a small) 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?	
	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?	ABA opposes the proposal to establish a voluntary opt-out mechanism within the ePC. Refer D1Q1.
We propose to: (a) define 'small business' as a business employing fewer than 100 people or, if the business is part of a group of related bodies corporate (as defined in the Corporations Act), fewer than 100 employees across the group, and (b) apply the definition as at the time the business acquires the facility in question (i.e. a point-in-time approach to defining small business).	D2Q1 Do you agree with the proposed definition? If not, why not?	ABA does not agree with the proposed definition of small business and provides the following explanation. The proposed definition is based on a single, blunt metric. It would capture a large number of businesses, some of whom would be sophisticated users of business payment facilities. Extending the ePC in this way may have low value for these businesses. For example, fund managers can manage regionally or nationally significant assets and have significant funds under management while having fewer than 100 employees. By comparison, the Banking Code definition includes additional metrics relating to turnover and credit outstanding, which provide further indications of the size and potential level of sophistication of the business. AFCA has separate jurisdictional limits which are based on loan facility amount and claim amount. AFCA also applies the definition of 'small business' at the time of the act or omission that gave rise to the complaint. ASICs' current proposal means where a business grows significantly to a large corporation, some of its payment facilities may be still protected under the ePC but would not be able to access AFCA to enforce these protections.
	D2Q2 What are the costs and regulatory burden implications versus benefits in setting this particular definition (for example, from a subscriber's system capabilities perspective)? D2Q3 What alternative definition(s) would you suggest? Why? How do you	Implementing the proposed definition would have significant cost, system and resourcing implications for subscribers, when the benefits of the proposal are yet to be determined (see D1). • Other than due diligence that is conducted to ensure lending to eligible small businesses comply with the Banking Code, banks do not routinely collect information about the number of employees of a business customer, and this number will change over time and/or on a seasonal basis.

	think the costs and benefits compare to those relevant to our proposed definition? 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?	• Banks segment business customers differently. As such the proposal is likely to affect multiple parts of the business, each with their policies, customer documents, and systems, as well as specific communications and staff training material. • Banks would need to implement new process and system changes to capture the number of employees. Depending on the definition of small business and when the definition applies, this metric would need to be captured at time of payment facility origination or be tracked and recorded more frequently. This is because when a dispute arises, a subscriber would need to determine customer eligibility and confirm a facility was acquired or a transaction conducted during an eligible period. The actual cost of implementation and the regulatory burden implications would depend on clarification of key questions including: • Which parts of the ePC would apply to small businesses and whether the ePC would be modified to address the issues raised. • Whether the ePC would only extend to consumer- or consumer-like payments products. • Alignment with existing definitions and alignment with how banks currently segment customers. • Whether the intention is that a business that no longer qualifies as a small business would cease to be eligible for Code protection, since almost all businesses will be 'small' on day 1.

E. Clarifying the unauthorised transactions provisions

Proposal	Questions	ABA response
We propose to adjust the wording of the Code to: (a) clarify that the unauthorised transactions	E1Q1 Do you agree with our proposals? If not, why not? E1Q2 What are the costs or regulatory burden	ABA has considered this proposal in context of the ePC's current application to retail consumer payments. The following comments do not necessarily apply if the ePC is extended to small businesses. Refer to ABA comments about the

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);

(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;

(c) provide some examples of scenarios that amount to express or implicit promotion, endorsement or authorisation of the use of

implications flowing from our proposals? Do the benefits outweigh the costs or regulatory burdens?

questions that need to be resolved including how the concept of unauthorised transactions could apply to business payments.

ABA supports the intention to clarify the definition of unauthorised transactions, so it does not include scams in general.

ABA is concerned the proposed clarification would still apply the ePC to some types of remote access scams. The fact that there would not be a clear delineation that excludes all types of scams from the ePC can be a source of significant confusion. Over time, as scam methodology changes and become more sophisticated, new variations of scams may end up being inadvertently covered by the ePC.

This outcome can create unequitable outcomes between customers who become victim of very similar scams, if some cases will be dealt with under the ePC as unauthorised transactions while others will not. A subscriber's response and a customer's eligibility for a refund should not be solely determined by a small part of the transaction (i.e, who took the final action that initiated payment). This can create discrepancies in subscribers' and/or AFCA's assessment of cases that may have similar facts, and lead to criticism of some customers being treated unfairly or others not being held liable for their actions.

As such, ABA provides the following comments for ASIC's consideration and would appreciate further discussions with ASIC on these issues.

- ABA asks ASIC to consider whether the term unauthorised transactions can be clarified in such a way that it excludes all types of scams, including all types of remote access scams or any other/future types of scams.
- ABA acknowledges there are many ways for remote access scams to be committed, and it can be difficult to distinguish scams from fraud. Nonetheless the drafting should be as clear as possible that most or all remote access scams are not 'unauthorised transactions' within the meaning of the ePC.
- If the definition cannot be amended so as to clearly exclude all scams, it will be critical for the definition, together with examples and/or guidance, to provide the maximum degree of clarity about which types of scams are covered by the ePC and which are not

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; and

(e) clarify that the provisions concerning liability for an unauthorised transaction are separate to any additional arrangements available under card scheme arrangements (e.g. chargebacks).

covered by the ePC. Clarity is needed on what conduct by the user would constitute 'authorisation' of a transaction, for example: cases where the user does not authorise the specific payment but has permitted access to a phone, banking app, provided banking passcodes including OTPs to the scammer or inputted these codes themselves, downloaded remote access software, or inputted payment details that were then amended by the scammer (while the screen is masked by remote access software).

- Failing to provide this clarity may result in subscribers (and by extension, their customers) spending a significant amount of time seeking evidence to determine how a transaction occurred and whether it meets the definition of unauthorised transaction or not. At the first instance this takes resources and focus away from the speedy resolution of complaints. This can also result in more complaints being made to internal and external dispute resolution, and taking longer to establish the facts necessary to make a determination at each stage.

Further, ABA asks ASIC to review the following issues which would also help to clarify the application of the ePC for industry and for AFCA.

- Review and clarify the concept of contribution to loss. This includes when giving access to a device (such as a phone/tablet), computer or app, downloaded a remote access software, logging into internet banking on another person's instructions should be considered to have been a factor that contributed to the loss. This should also consider whether a combination of actions, taken together, contributed to loss (for example, logging into internet banking while another person has remote access, then providing or inputting an OTP).
- Review the '51%' rule.
  - This rule should clearly allow a subscriber to consider whether a consumer has given access to a device and/or app, or downloaded software, and these actions helped to enable a scam or unauthorised payment to occur. Instead, this provision could refer to steps taken/initiated by the

customer (i.e, providing remote access while login occurs, saving pass codes in a browser) and whether those steps allowed the transaction to occur.

- As currently applied to two-factor authentication, a consumer who has given away one passcode (and may have taken other steps that contributed to a loss) has no liability. ABA proposes this rule be reviewed to consider actions beyond the voluntary sharing of pass codes and allow for partial allocation of liability.

- Clarify the concept of 'voluntary' disclosure (cl 12.2). AFCA has previously taken the view that disclosure to a scammer that the customer believes to be the police or the bank is not 'voluntary' disclosure. This is not consistent with the expressed policy intent of Proposal E1. Also consider whether a person giving away an OTP, knowing the code is only used or generated to authorise a payment, is 'voluntarily' disclosing a pass code. Allowing remote access raises further questions, as (for example) keystroke technology can result in the disclosure of pass codes that the customer enters, even if the pass codes appear to be masked.
- Provide guidance on the meaning of 'extreme carelessness' (cl 12.4), for example, providing remote access while logging in, failure to password-protect a phone that is used to access electronic payments, creating or inputting a payment code while someone else has remote access.

E1Q3 Is it possible for a consumer to input a pass code to a screen scraping service without this amounting to 'disclosure'? E1Q4 Is it possible for consumers to use screen scraping in a way that does not lead to the risk of financial loss? E1Q3 Is it	While it is possible for customers to use screen scraping without this amounting to 'disclosure', this is subject to the security of the website or application using this technology, and may depend on the terms of the contract between the customer and entity. ABA considers it is preferable for the ePC to provide clarity that screen scraping can result in unintended disclosure of passcodes, and to clarify that use of screen scraping could be one factor that 'contributes' to a loss. This means the subscriber would still need to establish a contributory link between screen scraping and the specific loss that occurred.

	possible for a consumer to input a pass code to a screen scraping service without this amounting to 'disclosure'? E1Q4 Is it possible for consumers to use screen scraping in a way that does not lead to the risk of financial loss?	As the ABA has previously advocated, the ePC's position on screen scraping should be kept under review in light of Open Banking implementation, including as to liability for using screen scraping and whether this practice is permitted. Open Banking provides a true alternative to screen scraping, rather than seeking to define 'a use of screen scraping that does not lead to the risk of financial loss'. Under Open Banking, customers share their data through secure APIs.
	E1Q5 What types of examples involving express or implicit promotion, endorsement or authorisation of the use of a service would be helpful to include in the Code?	It may be helpful to clarify whether anything not expressly prohibited by a subscriber would be implicit endorsement, and what would amount to an implicit prohibition.

F. Modernising the Code

Proposal	Questions	ABA response
We propose to: (a) define biometric authentication in the Code; and (b) incorporate biometric authentication into the Code in some specific clauses where required (to recognise that present day transactions can be authenticated by use of biometrics (e.g. fingerprints) where	F1Q1 Do you agree with the proposal to define biometric authentication in the Code? If not, why not? F1Q2 How would you suggest biometric authentication be defined in the Code? F1Q3 Which particular clauses in the Code do you think need to include a reference to biometrics in order for the clauses to	ABA agrees the ePC needs to be modernised, but refer to our introductory comments on how this could be done in a more holistic way. On the specific proposal to refer to biometric authentication, ABA seeks further information about the intended policy outcomes and/or the problem ASIC is seeking to address. For example, is it to clarify customers and subscribers' obligations relating to biometric authentication, and what about matters that are related to security of the phone/tablet. In response to ASIC's questions, ABA generally agrees pass codes and biometric authentication should not be used interchangeably. This is not a question of cost (per F1Q4), the two concepts are not the same and should not be defined together. Further, ABA queries whether changes should be limited to adding biometric authentication to existing clauses (including clauses 9-14). Biometric

previously only pass codes could be used). However, we do not propose to incorporate biometrics into the definition of 'pass code' in a way that would mean that pass codes and biometrics could be used throughout the Code interchangeably.	continue to have their intended effect? 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?	authentication may merit a number of stand-alone rules. This is because, for example: • A user does not record biometric information or keep a biometric 'secret'; it is not meaningful to refer to biometric being expired or cancelled, or whether a user has 'received' a biometric in the mail. • The ePC would need to clearly address how biometric authentication would be treated under the contribution rule (a user cannot 'give away' or disclose a biometric in the same way as a user gives away a pass code) and what uses of biometric authentication may amount to extreme carelessness. - The ePC may need to prohibit users from allowing third party biometric access to their phone devices, if that device is set up to facilitate payments. For example, not allowing a third party to register their fingerprint on a user's phone, if the phone has a digital payment method enabled. On the other hand, biometric is sensitive information under the Privacy Act. ABA cautions against a definition of biometric that could diverge from the Privacy Act or amount to a distinct privacy regime for biometric information. To avoid this outcome, ABA believes the ePC should not seek to define biometric or biometric information, and should cross-reference these terms as defined in other legislation such as the Privacy Act.
We propose to: (a) revise the Code's use of the term 'device' and instead refer to 'payment instrument'; and (b) include virtual debit and credit cards in the definition of 'payment instrument'.	F2Q1 Is the term 'payment instrument' more appropriate and easier to understand than 'device? Can you foresee any problems with this terminology? F2Q2 What costs would be involved in industry adjusting to the new terminology? F2Q3 Are there other new virtual payment instruments that should be covered by the	In principle, ABA agrees with ASIC updating the ePC to include or cater for new products that subscribers are offering, and new features that offer new ways to access payments. However, ABA refers to AusPayNet's comment that the term 'device' has a settled meaning in the payments industry which may not be properly reflected in the term 'payment instrument'. As for proposal F1, ABA seeks more information about the policy outcome ASIC is seeking and/or the problem. ABA cautions against using a single term to include devices (as currently defined) and virtual cards. • A number of ePC provisions are drafted on the basis that the device is a thing, not just information. As such any changes would

	definition of 'payment instrument' or 'device'? F2Q4 Do you see any unintended consequences from including virtual cards in the definition of 'payment instrument' or 'device'? F2Q5 What are the costs or regulatory burdens in catering for virtual cards within the definition of 'payment instrument'?	need to address questions such as what it means to have loss, theft or misuse of a virtual card. • Many provisions are drafted on the basis that the device is a thing that subscribers can issue and send to the customer (or cancel/withdraw). This is not the case for a phone with a mobile wallet that contains details of a virtual card. The ePC would need to review the customer's obligation to report a 'loss' and review subscriber's obligations if the customer has lost (for example) a phone.
We propose to amend the Code to: (a) expressly extend all relevant provisions to situations in which a 'Pay Anyone' payment is made through the NPP; and (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.	F3Q1 Do you agree that the Code's protections should apply to transactions made through the NPP? If not, why not? 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? F3Q3 Can we accommodate the NPP in the wording of the listing and switching rules in Chapter E of the Code? If so, how? F3Q4 Do you support the Code's provisions, as relevant, expressly relating only to BECS and the NPP? Or would your preference be	ABA generally supports the ePC being updated to cater for new retail payment channels and ways for retail customers to access payments. Specifically, ABA agrees with the proposal to extend the ePC to transactions made through the NPP and refer to AusPayNet's detailed comments.

	that the Code is payment platform agnostic? What are your reasons? F3Q5 Do you foresee any costs or regulatory burden implications of our proposals?	
We propose to amend the Code to cover the provision of electronic transaction receipts as well as paper receipts.	F4Q1 Do you agree with our proposal? If not, why not? F4Q2 Is there any particular information that the Code presently requires to be included on paper receipts that should not be required in electronic receipts? What are your reasons? F4Q3 What are the costs or regulatory burdens of our proposal?	ABA generally supports changes and refer to AusPayNet's comments.

G. Complaints handling

Proposal	Questions	ABA response
We propose to amend the Code to: (a) replace references to Regulatory Guide 165 Licensing: Internal and external dispute resolution (RG 165) with references to Regulatory Guide 271	G1Q1 Do you agree with our proposals? Why or why not? G1Q2 Are you aware of any particular reasons that may warrant retaining two separate complaints handling frameworks in the Code? G1Q3 Do you think we have adequately identified the	ABA generally supports these proposals, noting ASIC is continuing consultation on RG 271. Having a consistent set of requirements for internal dispute resolution can help consumers to understand how the ePC protects them when using electronic payments. The recommendations of the Treasury Payments System Review, particularly any recommendations about the regulatory and licensing regimes for payments, could affect assessment of this proposal's costs.

Internal dispute resolution (RG 271); (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; (c) require all subscribers to have IDR procedures that are set out in RG 271; and (d) require all subscribers to be members of AFCA.	important differences that require recognition in a merged complaints handling Chapter in the Code? Why or why not? G1Q4 What would be the costs of imposing the same requirements (e.g. AFCA membership, setting up complaints frameworks, disclosure) on all subscribers?	

H. Facility expiry dates

Proposal	Questions	ABA response
We propose to align the facility expiry period in the Code with the expiry period in the Australian Consumer Law, which is 36 months.	H1Q1 Do you support this proposal? Why or why not? H1Q2 Are you aware of any types of facilities subject to the Code that are not subject to the Australian Consumer Law expiry date requirements? Should the 36-month expiry date period also apply to those facilities? Why or why not?	ABA seeks clarification that credit and debit cards are not covered by this proposal. On this basis ABA does not object to the proposal.

H1Q3 What are the costs or regulatory burdens of our proposal?

I. Transition and commencement

Proposal	Questions	ABA response
We propose to apply an appropriate transition period before the updated Code commences. The specific period will be guided by submissions to this consultation paper.	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? I1Q2 Could you provide details as to where each proposal sits on a scale, compared to the other proposals, in terms of the amount of time that is needed for transition? Please provide anticipated timeframes, where possible. I1Q3 What are the particular costs (in terms of financial and other resources) that ASIC should be aware of in setting a transition period for commencement of the updated Code? Are there considerations that we need to make for particular	In the time available, ABA provides the following. On a number of proposals, further detail would be required to properly assess implementation requirements. • Changes that require banks to update T&Cs will require up to 9 months transition period. Changes such as to cover electronic transaction receipts may require technical change, with a similar material lead period. • Some proposals would require significant changes to different parts of the business, and would require much longer transition periods. Specifically, If the ePC is to extend to small business: - Ensuring systems and processes are updated to capture information about small business metrics - Review products offered to small businesses to identify which ones may be subject to the ePC - Updating terms and conditions for relevant business customers, which requires system and process changes, as well as legal resources to update documentation. - Cost of any periodic review of customer eligibility including any requests to customers for information. • It is not possible to estimate the implementation costs of some proposals without further detail, such as the proposal to include biometric authentication.

categories of subscribers? Please be as specific as you can.