CONSULTATION PAPER 341

Review of the ePayments Code: Further consultation

May 2021

About this paper

This consultation paper is the second of two papers ASIC has issued on our review of the ePayments Code (Code).

This paper seeks further feedback from stakeholders on our proposals for modifications to the Code to ensure it remains relevant and effective.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- Explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Document history

This paper was issued on 21 May 2021 and is based on the legislation as at the date of issue.

Disclaimer

The proposals, explanations and examples in this paper do not constitute legal advice. They are also at a preliminary stage only. Our conclusions and views may change as a result of the comments we receive or as other circumstances change.

Contents

The consultation process

You are invited to comment on the proposals in this paper, which are only an indication of the approach we may take and are not our final policy.

As well as responding to the specific proposals and questions, we also ask you to describe any alternative approaches you think would achieve our objectives.

We are keen to fully understand and assess the financial and other impacts of our proposals and any alternative approaches. Therefore, we ask you to comment on:

- the likely compliance costs;
- the likely effect on competition; and
- other impacts, costs and benefits.

Where possible, we are seeking both quantitative and qualitative information. We are also keen to hear from you on any other issues you consider important.

Your comments will help us develop our approach to updating the ePayments Code. In particular, any information about compliance costs, impacts on competition and other impacts, costs and benefits will be taken into account in assessing the regulatory and financial impact of our proposals.

Making a submission

You may choose to remain anonymous or use an alias when making a submission. However, if you do remain anonymous we will not be able to contact you to discuss your submission should we need to.

Please note we will not treat your submission as confidential unless you specifically request that we treat the whole or part of it (such as any personal or financial information) as confidential.

Please refer to our privacy policy at www.asic.gov.au/privacy for more information on how we handle personal information, your rights to seek access to and correct personal information, and your right to complain about breaches of privacy by ASIC.

Comments should be sent by Friday 2 July 2021 to:

ePaymentsCode@asic.gov.au

What will happen next?

Stage 1	21 May 2021	ASIC consultation paper released
Stage 2	2 July 2021	Comments due on the consultation paper
Stage 3	August/September 2021	Report on submissions, attaching draft Code for comments on the technical wording and format of the Code
Stage 4	Late 2021	Updated Code released

A Background to the proposals

Key points

The ePayments Code is a voluntary code of practice that regulates electronic payments.

It contains important consumer protections that complement other regulatory requirements such as financial services and consumer credit licensing, conduct and disclosure obligations.

ASIC is reviewing the Code to assess its continued relevance and effectiveness, noting significant developments in financial technological innovation and the need to ensure the Code is simple to apply and easy to understand.

This consultation paper seeks feedback on a range of proposals for some modifications to the Code to ensure it remains relevant and effective.

About the ePayments Code

1 The ePayments Code (Code) is a voluntary code of practice that regulates electronic payments, including automatic teller machine (ATM) transactions, online payments, BPAY, EFTPOS transactions, credit and debit card transactions and internet and mobile banking.

2 Most banks, credit unions and building societies in Australia, as well as a small number of other providers of electronic payment services, subscribe to the Code.

3 It contains important protections that complement the consumer and investor protections in ASIC-administered legislation such as the *Australian Securities and Investments Commission Act 2001* (ASIC Act), the financial services regulatory regime in Ch 7 of the *Corporations Act 2001* (Corporations Act) and the *National Consumer Credit Protection Act 2009* (National Credit Act).

4 Key protections in the Code include:

(a) requirements for disclosure to consumers of product terms and conditions and ATM fees;

(b) a general position that consumers will not be liable for any unauthorised transactions on their accounts if they have taken reasonable precautions to protect their accounts;

(c) procedures for authorised deposit-taking institutions (ADIs) to assist consumers to seek a return of their money if they have mistakenly transferred funds to the wrong recipient; and

(d) complaints handling processes for consumers who are dissatisfied with a subscriber's conduct.

5 The Code's requirements are part of the terms and conditions between the consumer and their subscribing financial institution.

ASIC's review and initial consultation

6 There have been significant developments in the electronic payments environment since our previous comprehensive review of the Code. These developments have implications for the ongoing relevance and effectiveness of the Code's provisions.

7 We are undertaking a review of the Code in its voluntary form to ensure that:

(a) the policy settings in the Code are appropriately positioned for today's—and, to the extent possible, tomorrow's—consumers and electronic payments service providers; and

(b) the Code is simple to apply and easy to understand for both subscribers and consumers.

8 In March 2019, ASIC issued Consultation Paper 310 *Review of the ePayments Code: Scope of the review* (CP 310). Non-confidential submissions have been published on ASIC's website under CP 310.

9 Since issuing CP 310 and receiving submissions, ASIC has held targeted discussions and consultations with a range of stakeholders, including various Code subscribers, payments industry bodies, consumer and small business representatives and advocates, financial technology firms ('fintechs'), industry associations and a range of state and Commonwealth organisations and regulatory bodies. We thank these stakeholders for their significant contributions to our understanding of the issues and potential options.

10 While we have considered the full breadth of the Code in this review, this consultation paper and our proposals focus on eight key matters:

(a) compliance monitoring and data collection;

(b) mistaken internet payments, including retrieval of partial funds and the responsibilities of the sending and receiving ADIs;

(c) extending the Code protections to small business customers;

(d) unauthorised transactions and the pass code security requirements;

(e) modernising the Code;

(f) complaints handling;

(g) facility expiry dates; and

(h) transition and commencement of the updated Code.

11 It is beyond the scope of this review to mandate the Code or to change key aspects of the Code in a way that significantly changes the entities to whom the Code is relevant (i.e. the subscriber base).

Next steps

12 This consultation paper presents our proposals for updates to the Code. We invite submissions on this consultation paper from any member of the public.

13 After receiving submissions, we will form our final positions on updates to the Code. We will issue a report on submissions, stating those final positions. At or around that time, we intend to also provide a draft updated Code, reflecting our final positions, for stakeholder feedback purely on the format and technical wording (not the policy positions in the Code).

14 We will then replace the current Code with the updated Code, with an appropriate transition period. Once the new Code takes effect, entities will no longer be able to subscribe, or continue subscribing, to the current Code. Entities who wish to subscribe to the updated Code will need to request ASIC to list them as a subscriber.

Proposal to make the Code mandatory

15 Our review is an interim measure to take into account new technologies that have emerged since the previous review. A fuller consideration of outstanding policy issues will be undertaken by the Australian Government, or other appropriate body, ahead of the Code becoming mandatory through legislation.

16 In 2019, the Council of Financial Regulators (CFR) recommended that ASIC be given the power to make compliance with the Code mandatory, such as through a legislative rule-making power. In November 2020, The Assistant Minister for Superannuation, Financial Services and Financial Technology issued a media release stating she had asked Treasury to work with APRA and ASIC to develop the reform package to implement the CFR's recommendations.

> Note: See CFR, *Regulation of stored-value facilities in Australia: Conclusions of a review by the CFR*, October 2019. See also Senator the Hon Jane Hume, 'Supporting competition and innovation in payment services', media release, 6 November 2020.

17 The proposals in this paper reflect the interim nature of our review of the Code in its voluntary form and are designed to ensure the Code is relevant and effective in the short to medium term. The positions set out in this consultation paper, and those ultimately in an updated voluntary Code, may be revisited when the Code is mandated at a future date.

Timing of ASIC's review

18 The Code requires ASIC to commence a review of the Code within five years of the conclusion of each preceding review. ASIC completed its last review of the Code in 2010.

19 ASIC initially delayed the timing of the current review in light of the recommendation in the final report of the 2014 Financial System Inquiry, which was accepted by the Government, to mandate the Code. In 2019, we considered it appropriate to conduct a separate review of the Code in its voluntary form (i.e. this current review) as an interim measure. Our review was further delayed as we adjusted our work in light of the COVID-19 pandemic.

> Note: See Financial System Inquiry, Final report, December 2014 and Department of the Treasury, *Government response to the Financial System Inquiry*, October 2015. See also Media Release 20-086MR *Details of changes to ASIC regulatory work and priorities in light of COVID-19*, 14 April 2020.

20 In the future, ASIC intends to review the Code every five years (subject to any changes to the review period introduced in the process of mandating the Code, or the need for ad-hoc targeted reviews). We agree with stakeholders that the time between this review and the preceding review was too long.

B Compliance monitoring and data collection

Key points

We propose to remove the requirement in the Code for subscribers to report annually to ASIC on the incidence of unauthorised transactions.

Instead, the Code will include a power that will allow ASIC to conduct targeted ad hoc monitoring of compliance with the Code and other matters relevant to subscribers' activities relating to electronic payments.

Compliance and industry monitoring

Proposal

B1 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 (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.

Your feedback

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?

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?

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)?

Rationale

The annual data reporting requirement

21 We collected annual data from subscribers about unauthorised transactions for a period of three years (the calendar years 2015 to 2017). We collected the data under clause 44.1 of the Code, which requires subscribers to report annually to ASIC or its agent information about unauthorised transactions as specified in a notice published on ASIC's website.

22 The data request sought the following key types of information from subscribers for the previous 12 months:

(a) the number of unauthorised transactions initiated by:

(i) credit and debit cards (including point-of-sale, card-not-present and ATM);

(ii) other (non-credit or debit) cards; and

(iii) internet or mobile application banking and telephone banking;

(b) the total number of transactions processed (to understand the proportion that were unauthorised); and

(c) the number and outcomes of complaints received by subscribers about how consumers' reports of unauthorised transactions had been dealt with.

23 The data collected did not include data on the incidence of consumer-initiated payments (whether by card or electronic funds transfer) as a result of falling victim to a scam.

Removing the annual data reporting requirement

24 The resource intensiveness of responding to the requests, particularly for smaller ADIs, has been a significant concern. While regulatory burden is sometimes unavoidable, it is important to measure this burden against the value that the exercise produces.

25 We appreciate the potential value in maintaining data collection, and reporting on it publicly in some way, as a form of 'reputational regulation' and benchmarking against peers. However, we think the better approach is to retain and enhance our ability to focus on a range of matters as appropriate.

26 This approach gives ASIC the flexibility to focus on particular areas of Code compliance at any given time, based on priorities or issues of concern, rather than being compelled to focus on a single topic (unauthorised transactions) on an ongoing basis. It also allows us to appropriately tailor information or data requests, in consultation with subscribers, keeping in mind our information needs and the burden on industry.

27 Industry may be well placed to take on (or continue) a role in collecting data about unauthorised transactions, given its direct interaction with these issues. Since the Code commenced, we note that industry has done significant work in monitoring the volume of and contributing factors for unauthorised transactions and collectively tackled the issues involved.

28 The Australian Payments Network (AusPayNet) currently publishes twice-yearly data on card-related fraud, which overlaps to some extent with the data ASIC collected. Unlike the data ASIC collected under the Code, the AusPayNet data does not cover unauthorised transactions initiated through 'Pay Anyone' electronic funds transfers.

29 After our review of the Code, we intend to hold discussions with industry and other stakeholders to assess the most valuable and effective approach to data collection.

Retaining and enhancing ASIC's ad hoc monitoring capabilities

30 ASIC already has an ad hoc targeted compliance monitoring function under the Code in clause 44.2. This function would remain and form part of our usual regulatory monitoring functions.

31 We intend to adjust the wording of the clause so that our information or data requests extend to monitoring not only *compliance* but also matters involving subscribers' activities, initiatives and experiences with their consumers that relate to the Code.

32 This would allow us to explore issues that are key to ensuring the Code remains relevant to contemporary business operations and consumer behaviour and experiences. For example, understanding consumer and subscriber behaviours could help us to identify any need to modernise the Code for contemporary technologies and behaviours.

33 The proposed change does not remove the prospect of future data collection on unauthorised transactions or other topics. Rather, it allows a more targeted approach so ASIC can get the information we need to address a specific purpose.

C Clarifying and enhancing the mistaken internet payments framework

Key points

We propose to extend the mistaken internet payments (MIP) framework in the Code to allow consumers to retrieve partial funds if the full amount of the payment is not available in the unintended recipient's account.

The Code would include a non-exhaustive list of examples of what a receiving ADI can do to meet the requirement to make 'reasonable endeavours' to retrieve the consumer's mistaken internet payment (while acknowledging that what amounts to 'reasonable endeavours' depends on the individual case).

There would be a number of additional responsibilities on ADIs to ensure that the process starts promptly and that consumers are made aware of their rights to lodge a complaint with the subscriber and then with the Australian Financial Complaints Authority (AFCA).

We also propose to:

- clarify the consequences for the sending ADI where the receiving ADI and/or unintended recipient do not cooperate in the process; and
- clarify the definition of 'mistaken internet payment', limiting it to situations in which the consumer has made a genuine mistake in typing the account identifier (and not extending it to scam scenarios); and
- enhance the content of the existing on-screen warning about mistaken internet payments so that it is clear to consumers that typing a correct account name will not remedy an incorrect BSB and/or account number.

Purpose of the MIP framework

34 Internet and mobile banking allow consumers to transfer funds from their account to someone else's account. These transfers are often referred to as 'Pay Anyone' transactions.

35 An electronic transfer traditionally involves entering the recipient's bank/state/branch (BSB) number and account number. More recently, an alternative option is to enter a 'PayID' (if the recipient has registered their own PayID). The PayID service is offered under the New Payments Platform (NPP). A PayID is an identifier that is unique to the recipient but is already attached to them for other purposes (e.g. a mobile telephone number).

36 Sometimes consumers transfer funds to the wrong person because they enter the wrong payment details or have been given the wrong account information. The Code sets out a framework for subscribers to help a consumer retrieve these funds. A consumer who has made a mistaken internet payment is unlikely to know the identity of the person who receives the funds (the unintended recipient) or, in many cases, the name of the receiving financial institution.

37 Without the MIP framework in the Code, the consumer who made the mistaken internet payment would have a limited ability to seek a return of their funds.

38 The four key elements of the MIP framework in Chapter E of the Code are described in Table 1.

Table 1: How the MIP framework operates

Element	Description
Recovery if there are sufficient funds	The Code requires that the facility terms and conditions disclose the processes for retrieving mistaken internet payments and the circumstances in which a consumer will be able to retrieve their funds. The Code sets out a process for consumers to be able to report mistaken internet payments, which requires the sending and receiving ADIs to establish whether there are sufficient funds in the unintended recipient's account and, if so, to take particular steps to try to help the consumer.
Recovery if there are not sufficient funds	If there are not sufficient funds available in the unintended recipient's account, the Code requires the receiving ADI to make 'reasonable endeavours' to facilitate the return of the full amount from the unintended recipient.
Access to dispute resolution	The consumer may complain to the sending ADI about how their report of the mistaken internet payment was handled. The consumer may also complain to AFCA about the sending ADI if they are not satisfied with the outcome of a complaint.
Consumer information	The Code requires an on-screen warning for consumers about the importance of entering correct details and the risk of making a mistaken internet payment.

Partial return of funds

Proposal

C1 We propose to amend the Code so that:

(a) the processes in clauses 28, 29 and 30 apply not only where there 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 retrieve the remainder of the funds.

Your feedback

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 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.

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'?

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

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?

Rationale

Partial return of funds

39 The Code states that the process of retrieving mistaken internet payments applies where the sending ADI is satisfied that such a payment has occurred and there are sufficient credit funds available in the account of the unintended recipient to the value of the payment.

40 If a sending ADI and receiving ADI are satisfied that a mistaken internet payment has occurred but there are not sufficient funds available in the unintended recipient's account to allow return of the full value of the payment, the Code requires the receiving ADI to use 'reasonable endeavours' to retrieve the funds from the recipient: see clause 32.1. The Code does not provide for the return of partial funds.

41 We think there is a strong benefit in allowing consumers to retrieve *some* of the funds, even if they cannot retrieve the total amount of the mistaken internet payment. We see no material difference in principle, in terms of necessary subscriber efforts and the respective consumers' necessary protections, in requiring an ADI to seek return of partial funds (where

complete funds are not available) compared to return of the complete funds. As a general rule, we consider that unintended recipients should be aware that they are not entitled to money that is mistakenly credited to their account.

42 The MIP framework provides a graduated approach, depending on whether the report about the mistaken internet payment was made:

(a) within 10 business days of the payment;

(b) between 10 business days and seven months of the payment; or

(c) more than seven months after the payment.

43 The longer the period, the more steps there are, recognising that, as time passes, returning the funds becomes potentially more burdensome or harmful for the unintended recipient. However, if the report is made relatively quickly, the harm to the recipient is arguably less, and there is less justification for allowing the unintended recipient to keep the funds.

'Reasonable endeavours'

44 Apart from the example in clause 32.1 (facilitating repayment by instalments), the Code does not provide any guidance on what amounts to 'reasonable endeavours' by the receiving ADI for retrieval of funds where the funds in the unintended recipient's account are not sufficient.

45 It is not possible to provide complete certainty about what amounts to 'reasonable endeavours' in all cases. This is because what is reasonable is determined on a case-by-case basis. Stakeholder feedback generally indicated that there are no hard and fast rules for what amounts to 'reasonable endeavours'. However, some asked for guidance in the Code on the range and type of factors that could be relevant.

46 We think a non-exhaustive list of scenarios might usefully serve as a benchmark for receiving ADIs about what types of options they might need to consider in individual cases. However, it would also make it clearer for ADIs that every case differs according to its particular facts and that the receiving ADI need only do what is reasonable.

47 We note that the Code does not allocate liability (for indemnity) for mistaken internet payments (unlike the unauthorised transactions framework in Chapter C of the Code). Rather, it is a framework that ADIs must follow to help the consumer in trying to retrieve their funds. The framework should facilitate this and not be rigid in its requirements. The fact that the Code does not allocate liability for mistaken internet payments does not prevent AFCA from awarding compensation where it is fair in the circumstances to do so.

Responsibilities of the sending and receiving ADIs

Proposal

C2 We propose to amend the Code to:

(a) require the sending ADI to investigate whether there was a mistaken internet payment 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 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 consideration in assessing whether the sending ADI has complied with its obligations.

Your feedback

C2Q1 Do you agree with the proposed timeframe in proposal C2(a)? If not, why not?

C2Q2 What are the costs associated with compliance 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?

Rationale

48 Table 2 sets out the obligations that apply to the sending and receiving ADIs under the MIP framework.

Table 2: Mistaken internet payments—Obligations of sending and receiving ADIs

Situation	Sending ADI	Receiving ADI
Overview of the MIP framework	The sending ADI must: • have effective and convenient processes for consumers to report mistaken internet payments; • acknowledge receipt of each report about such a payment (not necessarily in writing); • investigate whether such a payment occurred; • inform the consumer of the outcome of the report about the payment in writing within 30 business days of the day on which the report was made; • if it receives a complaint about how the report was dealt with, handle it under internal dispute resolution (IDR) procedures and not require the complainant to complain to the receiving ADI; and • cooperate with AFCA, including complying with any decision from AFCA (e.g. about whether a mistaken internet payment occurred). If the sending ADI is not satisfied that a mistaken internet payment occurred, no further action is required.	The receiving ADI must: • if both the sending and receiving ADIs are satisfied that a mistaken internet payment occurred but there are not sufficient credit funds available in the recipient's account, use reasonable endeavours to retrieve the funds and return them to the consumer who made the mistaken internet payment; and • cooperate with AFCA, including complying with any decision from AFCA (e.g. about whether a mistaken internet payment occurred).
Reports made within 10 business days	The sending ADI must: • if satisfied that a mistaken internet payment occurred, send the receiving ADI a request for return of the funds; and • If the funds are returned by the receiving ADI, return the funds to the consumer who made the mistaken internet payment as soon as practicable.	The receiving ADI must: • within 5 business days acknowledge the sending ADI's request for return of the funds and advise the sending ADI whether there are sufficient funds in the recipient's account to cover the payment; and • if satisfied that a mistaken internet payment occurred, return the funds to the sending ADI within 5 business days, if practicable (if not, within a longer period as is reasonably necessary up to 10 business days) of receiving the sending ADI's request for return of the funds. If not satisfied that a mistaken internet payment occurred, the receiving ADI may seek the consent of the recipient to return the funds.

Situation	Sending ADI	Receiving ADI
Reports made between 10 business days and 7 months	If the funds are returned from the receiving ADI, the sending ADI must return the funds to the consumer who made the mistaken internet payment as soon as practicable.	The receiving ADI must: • complete an investigation of the mistaken internet payment within 10 business days of receiving a request from the sending ADI for return of funds; and • prevent the recipient from withdrawing the funds for a further 10 business days and notify the recipient that the funds will be withdrawn from the account if the recipient does not establish they are entitled to the funds within 10 business days (of the date on which they were prevented from withdrawing the funds). If the recipient does not establish they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days of the expiry of the 10 business day period (during which the recipient was prevented from withdrawing the funds). If not satisfied that a mistaken internet payment occurred, the receiving ADI may seek the consent of the recipient to return the funds.
Reports made after 7 months	If the funds are returned from the receiving ADI, the sending ADI must return the funds to the consumer who made the mistaken internet payment as soon as practicable.	—

Timeframe for requesting the return of funds

49 We received stakeholder feedback that the more detailed the steps and associated timeframes, the more complex the process would be and the higher the risk of slow ADI responses (in a time-sensitive scenario).

50 However, we think there is value in setting a timeframe for the sending ADI to submit a request for return of funds to the receiving ADI. There is presently no timeframe for this step, despite it being the trigger to start the process for trying to get the consumer's funds back. Setting a timeframe could expedite the outcome of a claim for a mistaken internet payment and potentially enhancing the consumer's chances of getting their funds returned.

51 We think setting a maximum of five business days for initiation of the mistaken internet payment process is a relatively short period of time (therefore increasing the consumer's chances of a return of their funds) but long enough to allow the sending ADI a reasonable period of time to

undertake necessary investigations to assess whether the payment was in fact mistaken. In setting a time limit, we wish to ensure that requirements of ADIs match current practices and capabilities and that any regulatory burden is outweighed by consumer and regulatory benefits.

Record keeping

52 We acknowledge there may be limited value in giving the consumer precise details in the outcome report about what the sending and/or receiving ADI did to reach an outcome, given the potential complexity of that information. We believe the level of detail should be determined by Chapter F of the Code and ASIC's regulatory guidance on IDR procedures.

53 However, we think more detailed information can be useful if the complaint proceeds to external dispute resolution. Having all the information ready for AFCA's consideration in a dispute would, in our view, ensure efficient dispute resolution for the consumer.

54 We think the Code should require both ADIs to make and keep reasonable records for the duration of the limitation period. However, the Code will not prescribe this information, other than stating generally that ADIs must keep records of the steps taken and matters considered. Keeping the requirement relatively high-level will reduce the time taken for ADIs to complete the investigation into the mistaken internet payment, compared to more prescriptive requirements.

Complaints

55 While consumers have the right to make a complaint to AFCA about the sending ADI, clause 33 does not expressly require the sending ADI to include in its outcome report details of the right to complain. The ADI is simply required to inform the consumer of the outcome of the reported mistaken internet payment in writing within 30 business days. The benefit in requiring the sending ADI to inform the consumer of their dispute resolution rights is that the consumer will know exactly how to proceed if they are unhappy with the outcome of the process.

Cooperation of the receiving ADI and unintended recipient

56 We think the sending ADI needs to have confidence that, if it has complied with its requirements in the Code, it cannot be considered responsible for a consumer's loss from a mistaken internet payment, despite any lack of cooperation by the receiving ADI or unintended recipient.

57 The MIP framework relies on cooperation by the sending and receiving ADIs and, depending on how long the consumer takes to report the payment, the responsiveness of the unintended recipient. If there is non-compliance by

the receiving ADI, or the receiving ADI or the unintended recipient is otherwise non-cooperative or takes a particular view about whether a payment was mistaken, the sending ADI has little (if any) ability to ensure return of the funds despite having complied fully with the requirements.

58 We considered whether AFCA Rules should be amended to enable determinations against the receiving ADI (e.g. for failure to cooperate). However, ultimately, we considered it inappropriate to allow complaints against the receiving ADI because the receiving ADI does not have contractual obligations to the consumer who made the mistaken internet payment.

Definition of 'mistaken internet payment'

Proposal

C3 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.

Your feedback

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').

Rationale

59 Following our consultations to date during this review, we have formed the initial view that it will not be appropriate for an updated Code to include payments made as a result of scams within the scope of the MIP framework in Chapter E.

60 Some stakeholders interpret the current MIP framework as extending to cases where a consumer has fallen victim to 'authorised push payment (APP) fraud' or business email compromise fraud, on the basis that the consumer is technically making a mistake in inputting the wrong BSB and account number.

61 However, based on discussions with industry, we agree that the approach to responding to scams, if scams were to be addressed in an updated Code, would need to be different than the approach to mistaken internet payments. Detecting and responding to scams involves a range of different considerations. These include different time sensitivities, specialised communications (both with victims of the scams and with other financial institutions that are affected) and the involvement of potentially multiple recipient accounts across a number of financial institutions.

62 If scams were to be addressed through the Code, it would need to be through a set of bespoke rules, modelled on current industry practice to address instances in which a consumer has made a payment in response to a scam, not through the MIP framework. However, we understand that the processes currently undertaken by industry in scam scenarios are continually changing in response to the ever-evolving nature and complexity of scams.

63 We do not think the Code is an ideal place to set rules for preventing and responding to scams. We think that the issue of whether to extend the Code to deal with industry's response to scams should be considered as part of the process of making the Code mandatory. We do not believe we can deal appropriately with subscribers' response to scams in a voluntary Code.

64 However, we accept that scams are a significant and increasing problem. Therefore, we intend to work with stakeholders to contribute to addressing the problem as best we can through mechanisms other than the Code.

65 This includes exploring ways for ASIC to facilitate enhanced cross-stakeholder collaboration and information sharing on scams and firmer and more timely industry commitments to addressing the causes of the problems. We have already taken some steps in establishing a regular inter-regulator teleconference on scams that now includes industry and consumer group representatives.

66 Consistent feedback from some stakeholders is that consumers should not suffer losses through mistaken internet payments and scams as a result of deficiencies in the way the industry has designed the payment instruction and processing systems. We support that view.

Name and account number matching

67 In Australia, ADIs generally do not match an account name with BSB and account numbers when a consumer makes a Pay Anyone transaction (though, some may have processes for doing this). Matching is also not required by the Bulk Electronic Clearing System (BECS) Procedures. Matching only occurs systematically when consumers make transfers using the 'PayID' of the recipient (e.g. mobile phone number) under the NPP.

68 We are not proposing to include an account name and number matching requirement (for Pay Anyone transactions using a BSB and account number) as part of our current interim review of the Code in its voluntary form.

69 We think the merits of implementing a 'confirmation of payee' service in Australia (similar to that started in the UK in recent years) requires additional consideration and is likely to require a policy position from Government.

70 Necessary considerations may include:

(a) the feasibility of investment for improving dated payments infrastructure (BECS) that, in time, will be phased out and replaced by the NPP; and

(b) the continued gradual roll-out of the NPP and opportunities for significantly enhanced promotion and consequent voluntary uptake by consumers of the NPP's account matching service, 'PayID', as an alternative to the use of BSB and account numbers in Pay Anyone instructions.

On-screen consumer warning

Proposal

C4 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).

Your feedback

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?

Rationale

71 The BECS Procedures allow ADIs to process payment instructions by account number only (i.e. not matching with the account name).

72 Clause 25.1 of the Code requires subscribers to clearly warn users about the importance of entering the correct identifier and the risks of mistaken internet payments, including that:

(a) the funds may be credited to the account of an unintended recipient if the BSB number and/or identifier do not belong to the named recipient; and

(b) it may not be possible to recover funds from an unintended recipient.

73 The warning must, where practicable, be delivered:

(a) on-screen;

(b) when a user is performing a 'Pay Anyone' transaction using an internet banking facility; and

(c) before the transaction is finally confirmed, at a time when the user can cancel the transaction or correct the error.

74 We think that consumers who make Pay Anyone payment instructions using BSB and account numbers (which is also possible under the NPP, if a PayID is not used) should be presented, when the transaction is about to take place, with a timely and effective message about the fact that BSB and account numbers are not matched by the ADI (unless the ADI has a clear process of doing so in all cases) and that the ADI only uses the BSB and account number when acting on the instruction.

75 Ideally, the ADI would match *all* of the information that is requested from the consumer about the payment, and we think it is reasonable for a consumer to assume that this is what happens in practice. If this is not an ADI's practice, we consider it worthwhile proposing some changes to the consumer warning obligation (which already exists in the Code) to directly address stakeholder feedback that the warning does not require a clear statement that Pay Anyone instructions using BSB and account numbers do not involve account name and number matching by the ADIs involved.

76 We think something similar to the following wording could be useful as a benchmark, for example:

> Your money will be sent to the wrong account and you may not be able to get it back if the BSB or account number you give is wrong (**even if** you give the right account name).

77 We acknowledge that some mistakes may result in a payment being directed to a particular ADI (whose BSB number matches that entered by the consumer) but not necessarily to a customer of that ADI (if no such account number exists at that ADI). Therefore, it may not be accurate to state that the consumer's money will necessarily be sent to the wrong account.

78 We welcome stakeholder feedback on how the warning can address this subtlety while not inadvertently suggesting (as we consider might be the case in the current warning requirement with the use of the word 'may' in paragraph 25.1(a)) that the funds won't in all cases be misdirected.

79 We note the limitations of consumer warning messages. See, for example, the findings in this regard in the October 2019 joint publication by ASIC and the Dutch Authority for Financial Markets in Report 632 *Disclosure: Why it shouldn't be the default* (REP 632).

80 Whether the warnings will lower the risk of mistaken internet payments and potentially APP scams or business email compromise scams (because consumers will be prompted to check the details in their Pay Anyone payment instructions) will be borne out in practice. We strongly encourage ADIs to monitor the incidence of mistaken internet payments after they revise their warning message as a result of changes to the Code.

81 We would also like to see the NPP's PayID service more actively promoted. We intend to engage shortly with industry and other stakeholders such as consumer and business representatives with this goal in mind.

82 We think enhanced consumer and business familiarity with, and use of, the PayID service—a purpose built account name and account identifier matching service—will present a number of important 'roadblocks' for scammers who currently take advantage of the shortcomings of the BECS arrangements in the context of the electronic payment behaviours of today's consumers and businesses.

D Extending the Code to small business

Key points

We propose to extend the Code's protections to small businesses, but to provide an opt-out arrangement whereby subscribers may elect not to extend the protections to their small business customers.

We propose to 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 to apply the definition as at the time the small business acquires the relevant facility.

Opt-out arrangement

Proposal

D1 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 who have opted out and will consider options for any enhancements to the experience under the Code for both subscribers and small businesses.

Your feedback

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?

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

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

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.

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

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?

Rationale

83 The Code presently does not apply to transactions performed using a facility that is designed primarily for use by a business and established primarily for business purposes.

84 A number of stakeholders, including small business representatives, told us that, in the context of electronic payments, small businesses can have the same or similar vulnerabilities and need for protection as consumers.

85 It has been accepted in various other contexts that many small businesses need the same or similar protections as individual consumers. For example, the unfair contract terms legislation was extended to protect small businesses in November 2016 and we have seen the ASIC-approved Banking Code of Practice apply significant protections to small businesses.

86 The consumer protection provisions of the ASIC Act also apply to small businesses. On the other hand, the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry recommended against extending responsible lending protections in the National Credit Act to small businesses.

87 However, other stakeholders have expressed the following concerns about extending the Code to protect small businesses:

(a) Because small businesses might engage in a greater volume and frequency of transactions, they present subscribers with a higher risk of mistaken internet payments and unauthorised transactions.

(b) Small businesses typically engage in other activities and behaviours that present higher risks of unauthorised transactions—for example, sharing corporate cards and pass codes and using external accounting software and batch processing.

(c) Small business is defined in many different ways for different purposes. Agreeing on a common definition of 'small business' for the Code would be challenging and subscribers would be exposed to the risk of inadvertent non-compliance through having to continually assess whether a customer was a small business.

(d) Extending the Code to small business would be a significant change which would require an appropriate transition period.

(e) Longer timeframes (compared to the timeframes that apply in the individual consumer scenario) are likely to be required to ensure that, for example, complaints, unauthorised transactions and mistaken internet payments can be properly investigated and resolved. The amounts transacted by small businesses are commonly much larger than those by consumers. This, coupled with the potential for complex financial structures within businesses, means the impact of investigating and rectifying matters is likely to be greater for both the ADI and the customer involved.

88 Earlier in our review of the Code, we considered whether the Code could be extended to small businesses that are sole traders. We saw the extension to sole traders as a way to transition to an expanded cohort of customers covered by Code protections.

89 There was some stakeholder support for extending the Code's protections to sole traders, but the following issues were highlighted:

(a) Defining 'sole trader' is not straightforward. Extending the Code to sole traders would require subscribers to have the capability to identify such businesses.

(b) Businesses that are sole traders could include some sophisticated businesses not intended to have Code protections.

(c) Failing to apply the Code to all small businesses would be a missed opportunity.

(d) If the Code were first expanded to sole traders and later to all small businesses, subscribers would need to update systems, processes and documentation (both internal and external) twice, at significant expense.

Purpose of the 'opt-out' arrangement

90 In updating the Code, we need to consider reasonable positions of various stakeholders and acknowledge sometimes starkly opposing views. As a voluntary code, the Code needs to be a product of reasonable compromise. Considering a proposal to extend the Code to sole traders was an attempt at this, and our current proposal—for an opt-out arrangement relating to small businesses—is our further attempt to reach a reasonable compromise.

91 In addition to recognising small businesses' vulnerabilities and increasing their protections, we think our position has the benefits of:

(a) encouraging subscribers who feel able to expand their protections to small businesses to do so;

(b) creating a mechanism for subscribers who do not feel able to expand their responsibilities for now to opt out, but with the opportunity to opt back in when they are able to;

(c) placing obligations on subscribers who opt out—encouraging them to carefully consider whether they can transition towards expanding their protections to small businesses; and

(d) recognising the important role small businesses play in our economy and their need for appropriate protections.

92 The Code would no longer carve out 'transactions by a holder or user other than transactions performed using a facility that is designed primarily for use by a business and established primarily for business purposes': clause 2.1. Instead, it would apply generally to 'users' as defined in the Code, which would include small businesses and their employees, contractors and agents.

Differences in small business behaviours and activities

93 We acknowledge concerns about the behaviours and activities of small businesses that are different from those of individual banking consumers (as described above) and the consequential perceived heightened risk of unauthorised transactions and mistaken internet payments.

94 However, the MIP framework is, and will remain, a mechanism for helping a consumer to have their funds returned—it is not designed as a mechanism for the ADI itself to reimburse funds. Combined with improvements to the on-screen warning (see proposal C4) and targeted information about the importance of inputting correct account identifiers in Pay Anyone instructions, we do not foresee any greater risk to ADIs.

95 In relation to the unauthorised transactions provisions, we propose to modify the definition of 'user' so that an employee, contractor or agent of the business making a transaction will be considered to be authorised to make the payment. Any transactions conducted by the employee, contractor or

agent outside the permission granted to that individual will be a private matter for the employer and employee, contractor or agent to deal with separately from the framework under the Code.

96 We do not foresee an increase in the risk of liability to ADIs for unauthorised transactions in these circumstances.

Retrospective application

97 While, ideally, the Code's protections would apply to all small businesses who have a facility at the time of commencement of the new Code, we anticipate this would be practically difficult for subscribers to implement.

98 Instead, we propose that the Code should apply only to those small businesses who acquire a facility after the new Code has commenced. This means subscribers do not need to identify all existing customers who meet the definition of small business. It also has the benefit that small businesses will be able to ascertain whether they have Code protections by referring to their facility terms and conditions.

99 We acknowledge that our proposal means that small businesses that acquired their facilities before the updated Code commences will not have protection under the Code. The duration of this unprotected status may be many years, depending on how long the business holds that particular facility.

100 In the case of a subscriber who opts back in following an initial opt-out period, the small business protections in the Code would apply to that subscriber from the date that they reverse their opt-out status.

Definition of 'small business'

Proposal

D2 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).

Your feedback

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

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 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?

Rationale

101 We acknowledge the complexities in defining 'small business' and appreciate that there are different definitions for various purposes.

102 Rather than creating a new definition for the Code, we propose a definition that substantially aligns with the definition already used for ascertaining AFCA's jurisdiction to hear complaints by a business. Given that AFCA can hear consumer complaints relating to the Code, we consider it appropriate to apply the AFCA definition to businesses protected by the Code.

103 ASIC has recently issued *ASIC Corporations, Credit and Superannuation (Internal Dispute Resolution) Instrument 2020/98*, which modifies the definition of 'small business' in s761G(12) of the Corporations Act in relation to the obligation to have IDR procedures. That instrument defines 'small business', for the purposes of IDR procedures, as a business having fewer than 100 employees.

104 Our proposed definition differs from the AFCA Rules in that we propose that a business would only be defined as a small business for the purposes of the Code if it met the definition of a small business *at the time the business acquired the electronic payment facility*. The AFCA Rules define a small business as a business that had fewer than 100 employees '*at the time of the act or omission by the financial firm*' that gave rise to the complaint.

105 Our proposed approach removes the requirement to constantly monitor the size of businesses to determine whether they should have the benefit of the Code. We note that the Banking Code of Practice also applies a point-in-time definition for small business (being at the time the consumer acquires the product in question).

106 We acknowledge that this approach may result in the Code applying to a business that started out as a small business but later grows to be much larger and not the kind of entity ordinarily requiring the Code's protections.

E Clarifying the unauthorised transactions provisions

Key points

We propose to clarify that:

- the unauthorised transactions provisions of the Code apply only where a third party has conducted a transaction without the consumer's consent;
- a breach of the pass code security requirements by itself is not sufficient to find a consumer liable for a transaction (the consumer must have contributed to the loss); and
- the protections available under the Code are separate to the chargeback processes available through card schemes.

How the provisions apply

107 Chapter C of the Code explains how to allocate liability arising from unauthorised transactions and system or equipment malfunction. It sets out rules for when an account holder is and is not liable for loss.

108 Under clause 10, an account holder is not liable for loss arising from an unauthorised transaction where it is clear they have not contributed to the loss. If the circumstances in clause 10 do not apply, the account holder can only be liable for loss as set out in clause 11. This includes where the subscriber can prove on the balance of probability that a user contributed to a loss through fraud or breaching the 'pass code security requirements' in clause 12.

109 A 'pass code' is a password or code that a user must keep secret that may be required to authenticate a transaction or identify a user. It can consist of numbers, letters, other characters (or a combination) or a spoken phrase. Examples include a personal identification number (PIN), internet or telephone banking password and a code generated by a security token.

110 Under clause 12, where one or more pass codes are needed to perform a transaction, an account holder must not:

(a) voluntarily disclose one or more pass codes to anyone, including a family member or friend;

(b) where a device (e.g. a credit or debit card) is also needed to perform a transaction—write or record a pass code on a device, or keep a record of the pass code on anything:

(i) carried with a device; or

(ii) liable to loss or theft simultaneously with a device,

unless the account holder makes a reasonable attempt to protect the security of the pass code; or

(c) where a device is not needed to perform a transaction—keep a written record of all pass codes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the pass codes.

111 An account holder must not act with extreme carelessness in failing to protect the security of all pass codes. 'Extreme carelessness' means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour.

112 Where a subscriber expressly or implicitly promotes, endorses or authorises the use of a service for accessing a facility, a user who discloses, stores or records a pass code that is required or recommended for the purpose of using the service does not breach the pass code security requirements in clause 12.

113 A note in the Code immediately under clause 12.9 states:

> If a subscriber permits users to give their pass code(s) to an account aggregator service offered by the subscriber or an associated company, a user who discloses their pass code(s) to the service does not breach the pass code security requirements in clause 12.

Proposed clarification of the provisions

Proposal

E1 We propose to adjust the wording of the Code to:

(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);

(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 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).

Your feedback

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

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

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?

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?

Rationale

Application of the unauthorised transactions provisions

114 We consider that, as currently drafted, the provisions on unauthorised transactions do not provide sufficient clarity about whether consumer transactions made as a result of scams could be captured. In particular, it is not clear whether the provisions cover APP fraud.

115 We propose to amend the Code to clarify that the unauthorised transaction provisions do not apply where a consumer made the transaction instructions, whether as a result of third-party inducement, a scam or otherwise. In ASIC's view, the Code should continue to apply separately from any initiatives to address scams. Our reasons for this proposed clarification are the same as those for our proposal C3 relating to mistaken internet payments.

116 We think it more appropriate that measures to address APP fraud form part of an overall broader approach to scams prevention, outside the Code.

117 With highly skilled personnel, resources and direct links with the systems and consumers affected by scams, industry is well positioned to—and must—continue to undertake the task of preventing and responding to scams. Various industry-wide initiatives currently focus on proactively monitoring scams through observing system vulnerabilities and perpetrators' techniques.

118 Some examples of these initiatives are described in Table 3.

Table 3: Industry-wide initiatives to proactively monitor scams

Initiative	Description
TrustID	AusPayNet recently completed a targeted consultation on certain aspects of an initiative aimed at allowing individuals to access online services with enhanced security, privacy and convenience. AusPayNet is now developing the governance, branding and accreditation frameworks in consultation with interested stakeholders. A by-product of the initiative will, it is hoped, be a reduction in some types of scams.
Card-not-present (CNP) fraud	The first year of reporting following work AusPayNet undertook with issuers and merchants to mitigate the risk of CNP fraud showed a decline in instances of fraud. The CNP Fraud Mitigation Framework is designed to address CNP fraud by, among other things, encouraging protective behaviours and systems by merchants (e.g. tokenisation—discouraging inputting of card details into websites—and multi-factor authentication). In addition, AusPayNet has, for some years, published six-monthly CNP fraud statistics (and provided non-public further information to members) to allow industry players to benchmark their successes and weakness against others.
Fraud in Banking Forum	Since 2013 the Fraud in Banking Forum (led by AusPayNet) has held quarterly meetings to promote informal dialogue between fraud specialists from financial institutions and law enforcement communities. The forum covers all types of financial fraud (including identity theft, card fraud, investment fraud and scams). This allows industry to share information on a strategic level about current and emerging banking fraud issues. AusPayNet states that this has translated into quicker and more effective engagement when responding to fraud events. AusPayNet is presently looking at improving information exchange to help with criminal investigations and prosecutions.

119 The Code will continue to play a role where a scam has led to an unauthorised transaction, such as in the case of some remote access scams. Where the consumer has not made the transaction in question themselves and the consumer did not authorise that payment, this in our view is an ‘unauthorised transaction’ as defined in the Code and should be investigated and liability apportioned in accordance with the Code’s rules.

Linking a breach of pass code security requirements to unauthorised transactions

120 We received stakeholder feedback that some ADIs may consider that a breach of the pass code security requirements alone (and not necessarily supported by a contributory link to the subsequent loss) is sufficient for the subscriber to find the consumer liable for an unauthorised transaction.

121 We consider this is an incorrect application of the Code's rules. Rather, the subscriber must prove on the balance of probability that the breach of the pass code security requirements has contributed to the unauthorised transaction in question. The onus of proving this contributory link is on the subscriber, not the consumer.

122 Making this position clear in the Code will reduce the risk of uncertainty or inconsistency in application.

Unauthorised transactions and chargebacks

123 Liability for an unauthorised transaction under the Code, and the process that applies in reporting an unauthorised transaction (including the timeframe in which a report should be made), sit separately and are distinct from chargeback arrangements available through card schemes.

124 We are aware of situations where a subscriber has failed to investigate a consumer's report of an unauthorised transaction because the consumer missed the 120-day cut-off under the relevant card scheme rules, despite the Code providing a six-year limitation period. The consumer was then told that the report would not be investigated because it fell outside the time limit. We have taken the view that such representations are likely to be misleading.

125 Clarifying this distinction in the Code will ensure subscribers and consumers are clear about the relevant limitation period that applies to their right to report unauthorised transactions under the Code.

Screen scraping

126 ASIC has previously observed (for example, in a submission to the Productivity Commission's 2016 inquiry into Data Availability and Use) that many entities rely on access to consumers' banking and transaction data via 'screen scraping' to provide information analytics services to consumers or to other commercial organisations.

127 Screen scraping in this context generally involves the consumer inputting their internet banking credentials (i.e. login and password). There are some views amongst stakeholders that inputting one's pass code in this context does not amount to 'disclosure' of one's pass code and, therefore, is not in breach of the Code's pass code security requirements and a consumer's

terms and conditions with their ADI. There are also mixed views on the extent to which ADIs implicitly promote, endorse or authorise the use of such services in certain circumstances.

128 It is not ideal, in our view, that the Code should give rise to this 'grey area' (comprising various interpretations) and leave consumers, their financial institutions and, indeed, screen scraping providers with the uncertainty as to what consumer behaviours amount to practices permitted under the Code.

129 Because our review is an interim measure, pending mandating of the Code, we propose to maintain the status quo. That is, we propose to maintain the position that consumers are unable (under the terms of the Code and, accordingly, under their terms and conditions with their financial institution) to disclose their pass code 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 on the consumer's account, the consumer will be unable to get indemnity from the subscriber for that loss.

130 A consumer will only be liable for loss arising from an unauthorised transaction following use of a screen scraping service if:

(a) the use of the service amounted to 'disclosure' of the consumer's pass code; and

(b) the subscriber can prove on the balance of probability that the use of that service contributed to the loss. (We note that, at this stage, ASIC has seen no evidence to suggest that consumers' use of screen scraping services has contributed to loss from unauthorised transactions.)

131 Our proposal provides clarity and reinforces the long-standing position taken by government agencies generally that sharing a pass code is a risky practice. It is not a prohibition on the use of screen scraping but clarifies the position that a consumer takes particular actions at their own risk.

132 Maintaining the status quo is our temporary position, bearing in mind there is Government policy work still to be done in both the roll-out of the Consumer Data Right and options for eventually mandating the Code.

Note: For details of the Consumer Data Right, see 'Key terms' in this paper.

F Modernising the Code

Key points

We propose to:

- define biometric authentication in the Code and incorporate it into specific provisions of the Code where it is relevant;
- revise the Code's use of the term 'device' and instead use the term 'payment instrument' to avoid confusion with consumer-owned smart devices;
- include virtual debit and credit cards in the definition of 'payment instrument';
- extend the Code's protections to NPP payments; and
- include electronic receipts in the Code's provisions relating to transaction receipts.

Biometrics

Proposal

F1 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 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.

Your feedback

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 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?

Rationale

133 The Code does not currently refer to the use of biometrics to authenticate a payment. When we last reviewed the Code, biometric authentication was not widely used as a means to access banking services and initiate payments. Pass codes were the dominant form of authentication and they are likely to remain so for some time, either alone or in combination with biometric authentication (e.g. as a secondary authentication factor sent to a payer by SMS or in a mobile application).

134 In ASIC's view, biometric authentication cannot be treated in a similar way to pass codes under the Code. Essentially, they represent different 'factors' of authentication: knowledge, possession and inherence:

(a) A pass code is usually something the consumer knows (knowledge) or is delivered by means of something the consumer possesses, such as a phone (possession).

(b) Biometric authentication is based on something inherent to the consumer—e.g. their fingerprint or facial features (inherence).

135 We consider it would be unworkable to apply principles designed for a knowledge factor to an inherence factor—for example, we cannot ask consumers to 'keep their fingerprints safe'.

136 Our preferred approach is to add references to biometric authentication into the Code on a provision-by-provision basis, identifying where such references are needed to modernise the Code. This provides certainty for stakeholders about their rights and obligations under the Code in specific circumstances where biometric authentication is used in place of a pass code.

137 We are also guided by a potential benefit in ensuring that the Code supports innovation in payments by not imposing additional liability where overall security levels can be higher despite the subscriber not requiring 'traditional' or legacy credentials such as a passcode.

138 Because biometric authentication is generally linked to a consumer's personal device, we consider that ongoing consumer education about device security has a role to play in responding to newer device-based methods of payment authentication.

Defining ‘device’

Proposal

F2 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’.

Your feedback

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 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’?

Rationale

139 The Code defines ‘device’ as:

> a device given by a subscriber to a user that is used to perform a transaction. Examples include an:
>
> - ATM card;
> - debit card or credit card;
> - prepaid card (including gift card);
> - electronic toll device;
> - token issued by a subscriber that generates a pass code; and
> - contactless device.

140 When the Code was drafted, consumers generally used subscriber issued devices (e.g. those devices listed above) or subscriber issued payment facilities (e.g. internet banking for ‘Pay Anyone’ payments) to initiate transactions or consumer authentication. Physical electronic tokens were sometimes used to access internet banking, as a form of multi-factor authentication to produce an additional pass code. It is now more common to generate a token and have it sent to one’s mobile telephone.

141 Over time, there has been an increase in the use of consumer-owned devices (e.g. mobile phones, tablets and watches) to authenticate access to banking facilities or initiate payments. Further, in many cases a device (e.g. a credit card) is not physically issued to a consumer; instead, the consumer is given a virtual card (simply a card number).

142 We consider that the current use of 'device' in the Code may potentially confuse consumers, given that the ordinary meaning and use of 'device' relates to a consumer-owned device such as a smartphone or watch. Also, consumers may not be reasonably expected to consider a card a 'device', given a card's lack of electronics. We therefore consider that a change in terminology may help with the readability and clarity of the Code, particularly for consumers.

143 We propose to expand the definition of payment instrument to include virtual cards. For example, the loss, theft or misuse of a virtual card accessed through a consumer-owned device would be treated in a similar way to the loss, theft or misuse of a physical card in a wallet.

144 Reporting the loss of the virtual card on the device, in much the same way as reporting the loss of a physical card in a wallet, would help to limit the consumer's liability under clause 11.2 of the Code in a scenario not anticipated when the Code was drafted.

145 We consider that a consequential amendment to the definition of 'identifier' may also be required to cover virtual cards.

146 Some stakeholders considered that the Code provisions referring to identifiers and devices should be updated to cover electronic payments made without such a device or identifier, such as the concepts of tokenisation or card-on-file. Tokenisation means replacing one identifier (e.g. a credit card number) with another unique identifier (the token) so that the original identifier is not made visible during the payment transaction process.

147 We think the Code deals with these concepts adequately, despite not expressly referring to them. For example, when using tokenisation, we think the token is itself an 'identifier' for Code purposes. Further, with card-on-file, while the consumer is not re-entering their card identifier each time they make a transaction, there is still use of the identifier (e.g. the card number) to make the transaction.

Payment platforms

Proposal

F3 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.

Your feedback

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 that the Code is payment platform agnostic? What are your reasons?

F3Q5 Do you foresee any costs or regulatory burden implications of our proposals?

Rationale

148 As we observed in CP 310, the Code's MIP framework (for helping banking consumers retrieve mistakenly transferred funds) is worded on the presumption that the credits to and debits from consumers' banking accounts are made through 'direct entry' as defined by the BECS Procedures.

149 In particular, the Code's definition of 'mistaken internet payment' and the MIP framework assumes that mistaken internet payments occur only where a consumer, through a 'Pay Anyone' internet banking facility processed by an ADI through direct entry, pays funds into an unintended recipient's account due to entering the incorrect BSB number or account number.

150 The NPP is a more recent payments infrastructure that was launched in Australia in February 2018. It allows for almost real-time clearing and settlement of funds transfers between accounts of participating financial institutions. NPP transfers can be made by the user entering either the recipient's BSB and account number or the recipient's registered 'PayID' (if they have chosen to register a PayID).

151 The NPP is governed by its own rules and regulatory framework administered by NPP Australia Limited.

152 'Pay Anyone' transactions may still be made using the NPP in a similar way to direct entry under BECS. Therefore, mistaken internet payments can and will continue to occur where payments are made to an incorrect BSB and account number.

153 The Code's protections should be available to consumers regardless of which platform they use to make payments. Consumers generally do not have a choice or visibility of the platform they are using (unless they use PayID).

154 While we considered trying to make the Code payment platform neutral, stakeholder feedback alerted us to the risk of inadvertently covering other platforms that were never intended to be covered by the Code (e.g. the High Value Clearing System). Given the pace at which new payment platforms emerge, we consider it acceptable to refer specifically in the Code to the NPP and BECS. If any other relevant platforms emerge, we would consider further amendments to the Code at that time.

155 We do not consider the NPP framework to be inconsistent with the Code. Also, we have previously informed industry of ASIC's expectation that the Code's protections should in practice be applied to NPP transactions.

Listing and switching rules

156 The listing and switching rules in Chapter E of the Code require an ADI to give a consumer a list of their direct debit and credit arrangements and periodic payments for the preceding 13 months, including specific pieces of information to help them switch to a new ADI. These rules are relevant only to BECS payments and do not cover payments arranged through the NPP.

157 The rules relate to 'direct debits arrangements', 'direct credit arrangements' and 'periodical payments'. Direct debit and credit arrangements are a product of the direct entry system and defined in the BECS Procedures. 'Periodical payments', while not explicitly defined as being based only on BECS, are assumed by the Code to involve the use of a BSB number and identifier: see, for example, clause 35.18.

158 While we received some feedback that these rules are not often relied on by consumers, we do not see a strong justification for removing them for now. Because we propose to retain the rules for the time being, we are keen to understand how the rules could be worded to accommodate the NPP or whether, instead, the rules are not relevant to NPP transactions.

159 In time, these rules may become less relevant and even redundant, given the intended availability in due course of new functionalities within both the NPP and the Consumer Data Right for third-party initiated transactions and/or payments.

160 These functionalities are likely to reduce the need for reliance on direct debit arrangements and provide alternatives to managing regular payments from an account. Over time, ASIC can review the status of these initiatives and assess the ongoing relevance of the Code's listing and switching provisions.

Transaction receipts

Proposal

F4 We propose to amend the Code to cover the provision of electronic transaction receipts as well as paper receipts.

Your feedback

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?

Rationale

161 The Code requires subscribers generally to take reasonable steps to offer consumers a receipt for payment transactions at the time of a transaction.

162 The Code's restrictions on the contents of receipts only apply to *paper* receipts. They do not apply to receipts sent electronically (e.g. by email or text message to a mobile phone or receipts made available through the retailer's website).

163 We received stakeholder feedback that the Code should apply to all forms of receipts sent electronically—not just paper receipts. We agree that the Code's protections should apply regardless of whether the receipt is provided in paper or electronic form.

G Complaints handling

Key points

We propose to amend the Code to require all subscribers to have IDR procedures that are set out in Regulatory Guide 271 *Internal dispute resolution* (RG 271) and to be members of AFCA.

We propose to combine Chapter F and Appendix A to adopt a single complaints handling framework.

Internal and external dispute resolution

Proposal

G1 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 *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.

Your feedback

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 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?

Rationale

Reducing complaints handling to a single framework for all subscribers

164 The Code contains requirements for complaints handling for subscribers. Presently, those obligations are split into two sections:

(a) Chapter F contains obligations for subscribers who are Australian financial services (AFS) licensees, unlicensed product issuers, unlicensed secondary sellers, Australian credit licensees or credit representatives.

(b) Appendix A contains obligations for subscribers who are not in the above categories. They do not need to meet the Chapter F requirements.

165 Chapter F relates to subscribers who tend to be consumer facing and provide products to individuals. Appendix A relates to subscribers who tend not to provide products to individuals.

166 The key differences between Chapter F and Appendix A recognise that:

(a) subscribers subject to Appendix A are not required to comply with RG 165;

(b) information about unauthorised transactions might be more difficult to obtain (and may not in all cases be relevant) for subscribers subject to Appendix A; and

(c) consumers need to know that the process for complaints might be different and that some subscribers might not be AFCA members (or have a process for external dispute resolution at all).

167 RG 165 explains that AFS licensees, unlicensed product issuers, unlicensed secondary sellers, credit licensees and credit representatives, among others, must have a dispute resolution system in place that meets ASIC's requirements. In essence, they must have IDR procedures that meet the standards or requirements made or approved by ASIC and must have membership of AFCA.

168 We received limited feedback on the merits of retaining two separate complaints processes. On the whole, there was support for a single framework.

169 We have not identified any reason to retain two separate frameworks or to otherwise exempt Appendix A subscribers from having IDR procedures in place that meet ASIC's requirements in RG 165 (or RG 271, after it commences) or from having membership with AFCA for this narrow purpose. If there is no justifiable reason otherwise, we think the Code should be simplified on this point to ensure consumers can understand and have access to protections.

Replacing references to RG 165 with RG 271

170 RG 165 applies to complaints received by financial firms before 5 October 2021, when RG 271 comes into effect. ASIC will withdraw RG 165 on 5 October 2022. RG 271 will also require entities to have IDR procedures and membership of an external dispute resolution (EDR) scheme.

171 As stated in paragraph 14 of this paper, we will apply an appropriate transition period before the updated Code commences. The current Code will continue to apply to complaints handling until the end of the transition period; any reference in it would have the effect, for all subscribers already subject to RG 165, of being read as RG 271 from 5 October 2021.

172 For those subscribers subject to Appendix A, the Code transition period would apply so that 5 October 2021 would not be the commencement date for their obligations for IDR procedures and membership of an EDR scheme (rather, the Code transition period would determine that commencement date).

173 We note that certain paragraphs in RG 271 are specified as being enforceable. While we propose that the RG 271 requirements should apply to all Code subscribers, we do not propose that the enforceability of specified RG 271 paragraphs would apply in relation to the Code.

174 This is because the Code sits separately from the regulatory regimes in the National Credit Act and the Corporations Act relating to consumer credit and financial services. While the Code exists in its current voluntary form, breaches of the Code would continue to be subject to resolution through IDR procedures and the EDR scheme or through private disputes in the courts.

Retaining important differences

175 We recognise that some requirements may need to be tailored in the new complaints handling chapter based on the subscriber's licensed status. For example, clauses 38.2 and A6 require subscribers to obtain different types of information from a user when the user reports an unauthorised transaction.

176 Under clause 38.2, the subscriber must obtain a series of detailed information, while clause A6 requires the subscriber to make reasonable efforts to obtain that information and only to the extent relevant. This is in recognition that the subscriber subject to Appendix A may have more limited access to the required information and their particular service might not be structured in such a way that all of that information is relevant.

177 We think our proposal has the benefit of continuing to recognise these practical differences in how different types of subscribers operate and what information they are privy to in the context of an unauthorised transaction.

H Facility expiry dates

Key points

We propose to update the minimum 12-month expiry period for certain facilities in the Code to adopt a minimum 36-month period, in line with the Australian Consumer Law.

Aligning requirements with the Australian Consumer Law

Proposal

H1 We propose to align the facility expiry period in the Code with the expiry period in the Australian Consumer Law, which is 36 months.

Your feedback

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?

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

Rationale

178 For facilities with an expiry date, the Code currently prescribes a minimum 12-month expiry period, which must, if ascertainable, be disclosed to the consumer: see Chapters B and D of the Code.

179 The Australian Consumer Law was amended to provide that most gift cards sold on or after 1 November 2019 must have a minimum three-year expiry period, display expiry dates and be free from most post-purchase fees.

180 The Code has minimum expiry date requirements for some types of products:

(a) If a facility is not reloadable and cannot be used after a certain date, the expiry date must generally be at least 12 months from the date the user activates the facility.

(b) If the facility is reloadable and cannot be used after a certain date, the expiry date must generally be at least 12 months from the date the user last reloads the facility.

181 We intend to align the requirements of the Code with those in the Australian Consumer Law.

182 This proposal is consistent with feedback we received from some stakeholders and provides consistent rules (and protections for consumers) across a variety of payment instruments (whether those instruments are subject to the Code or not).

I Transition and commencement

Key points

We propose to apply a transition period before the updated Code commences. We are requesting views from industry on an appropriate timeframe.

Transition period

Proposal

I1 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.

Your feedback

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

Rationale

183 We believe the updated Code should commence as soon as possible. However, we acknowledge that many of the proposals in this paper will require systems changes and a change in approach by subscribers and others such as AFCA. Further, consumers and small businesses will need some time to adjust—with the help of messaging and educational material—to the new positions in the Code.

Key terms

Term	Meaning in this document
ADI	An authorised deposit-taking institution—a corporation that is authorised under the *Banking Act 1959*. ADIs include: • banks; • building societies; and • credit unions
AFCA	Australian Financial Complaints Authority—the operator of the AFCA scheme, which is the EDR scheme for which an authorisation under Pt 7.10A of the Corporations Act is in force
APP fraud	Authorised push-payment fraud
ASIC	Australian Securities and Investments Commission
ASIC Act	*Australian Securities and Investments Commission Act 2001*, including regulations made for the purposes of that Act.
ATM	Automatic teller machine
AusPayNet	The Australian Payments Network Limited, which administers the BECS Procedures
Australian Consumer Law	The Australian Consumer Law contained in Schedule 2 to the *Competition and Consumer Act 2010*
Banking Code of Practice	The Banking Code of Practice, dated 1 March 2020
BECS	Bulk Electronic Clearing System
BSB number	The number that identifies the bank/state/branch for an account
CFR	Council of Financial Regulators
CNP fraud	Card-not-present fraud
Code	The latest version of the ePayments Code, a voluntary code of practice, effective from 29 March 2016, that regulates electronic payments in Australia, including ATM transactions, online payments, BPAY, EFTPOS transactions, credit and debit card transactions (e.g. through contactless and wearable technologies and other emerging payment methods linked to debit and credit cards) and internet and mobile banking
Consumer Data Right	The legal framework contained in Part IVD of the *Competition and Consumer Act 2010*

Term	Meaning in this document
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
EDR	External dispute resolution
facility	An arrangement through which a person can perform transactions
holder	An individual in whose name a facility has been established, or to whom a facility has been issued
IDR	Internal dispute resolution
MIP framework	The framework for handling reports of mistaken internet payments under the Code as described in Section C of this paper
mistaken internet payment	A payment where a consumer transfers money through an internet banking facility to the wrong recipient due to the consumer mistakenly entering the wrong BSB and/or account number
National Credit Act	*National Consumer Credit Protections Act 2009*, including regulations made for the purposes of that Act
NPP	The New Payments Platform, which is a platform administered by NPP Australia Limited that facilitates real-time, data-rich payments between accounts at participating financial institutions
PayID	A unique identifier (such as a mobile telephone number) offered under the NPP in place of BSB and account numbers for the purposes of electronic payments
related body corporate	A related body corporate, as defined in s9 of the Corporations Act
s9 (for example)	A section of the ASIC Act or the Corporations Act (in this example numbered s9)
subscriber	A subscriber to the Code

List of proposals and questions

Proposal	Your feedback
B1 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 (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.	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? 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? 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)?
C1 We propose to amend the Code so that: (a) the processes in clauses 28, 29 and 30 apply not only where there 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 retrieve the remainder of the funds.	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 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. 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'? C1Q5 What types of factors might affect whether a particular action is necessary to satisfy 'reasonable endeavours' in individual cases? 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?

Proposal	Your feedback
C2 We propose to amend the Code to: (a) require the sending ADI to investigate whether there was a mistaken internet payment 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 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 consideration in assessing whether the sending ADI has complied with its obligations.	C2Q1 Do you agree with the proposed timeframe in proposal C2(a)? If not, why not? C2Q2 What are the costs associated with compliance 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?
C3 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').

Proposal	Your feedback
C4 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?

Proposal	Your feedback
D1 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 who have opted out and will consider options for any enhancements to the experience under the Code for both subscribers and small businesses.	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? D1Q4 What are the costs and benefits for industry of our proposal? D1Q5 Do you agree with our proposal D1(b), that the Code should not apply retrospectively to small business facilities already acquired at the time of commencement of the updated Code? If not, why not? What are the costs and complexities versus benefits of our proposal and alternative approaches? 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. D1Q7 Does our proposed change to the definition of 'user' (by including employees, contractors or agents of a small business) address any concerns about any increased risks to subscribers as a result of extending the Code's protections to small businesses? If not, why not? Do you think this could have any unintended impacts? If so, what are they? 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?

Proposal	Your feedback
D2 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? 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 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?

Proposal	Your feedback
E1 We propose to adjust the wording of the Code to: (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); (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 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).	E1Q1 Do you agree with our proposals? If not, why not? E1Q2 What are the costs or regulatory burden implications flowing from our proposals? Do the benefits outweigh the costs or regulatory burdens? 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? 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?

Proposal	Your feedback
F1 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 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.	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 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?
F2 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 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'?

Proposal	Your feedback
F3 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 that the Code is payment platform agnostic? What are your reasons? F3Q5 Do you foresee any costs or regulatory burden implications of our proposals?
F4 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?
G1 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 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.	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 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?

Proposal		Your feedback	
H1	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?
		H1Q3	What are the costs or regulatory burdens of our proposal?
I1	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 categories of subscribers? Please be as specific as you can.