REPORT 718

Response to submissions on CP 341 Review of the ePayments Code: Further consultation

March 2022

About this report

This report highlights the key issues that arose out of the submissions received on Consultation Paper 341 *Review of the ePayments Code: Further consultation* (CP 341) and details our responses to those issues.

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.

Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the relevant legislation and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Contents

A Overview

Key points

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

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

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

Review of the ePayments Code

1 In March 2019, ASIC issued Consultation Paper 310 *Review of the ePayments Code: Scope of the review* (CP 310), in which we consulted on the topics to include within our review. The consultation was open for a period of four weeks, between 6 March 2019 and 5 April 2019.

2 In May 2021, we issued Consultation Paper 341 *Review of the ePayments Code: Further consultation* (CP 341), in which we consulted on proposals to amend the Code. The consultation was open for a period of six weeks, between 21 May 2021 and 2 July 2021.

Submissions received

3 We received three confidential and seventeen non-confidential submissions to CP 310. We received four confidential and fourteen non-confidential responses to CP 341. Respondents represented a diverse range of stakeholders, including the banking industry and other Code subscribers, industry associations, consumer and small business representatives, financial technology firms and government agencies or regulators.

4 In addition to receiving submissions, we engaged in roundtables and a range of other discussions with a number of stakeholders to give them the opportunity to raise questions and share their feedback, and to ensure that the process was transparent and involved a high degree of stakeholder input. We are grateful to stakeholders for taking the time to provide their feedback.

5 During our consultations, we also sought information from stakeholders about the regulatory costs of our proposals. Feedback on regulatory costs likely to be incurred was generally high-level and non-specific in terms of dollar amounts.

6 For a list of non-confidential respondents to CP 310 and CP 341, see Appendix 1 to this report. Non-confidential submissions have been published on ASIC's website on the landing pages for CP 310 and CP 341.

7 This report highlights the key issues that arose out of the submissions received in response to CP 341 and feedback received through our other stakeholder engagement, and our responses to those issues. While we have attempted to provide sufficient detail in this report to assist readers in understanding the matters we took into account in reaching our final positions, it is not intended to be a comprehensive summary of all feedback received.

Responses to consultation

8 The feedback in response to CP 341 and our other targeted stakeholder engagement confirmed a strong demand for an updated Code.

9 Given the significant volume and range of issues requiring updates to the Code, and in an effort to keep our process moving forward in implementing some key new positions, it has not been possible to address every single issue raised by stakeholders during this review. Our aim is to address some key issues now, in the context of this review being interim in nature ahead of further work to produce a mandatory Code.

10 For detailed summaries of feedback provided and our response to specific topics, see the relevant sections of this report.

Timing of our review

11 ASIC is required to commence a review of the Code within five years of completion of the previous review. The most recent review was completed in December 2010.

12 In 2014, the final report of the Financial System Inquiry recommended that the protections in the Code should be made mandatory. Initially, ASIC paused its work on commencing a review of the Code in 2015 in anticipation of upcoming work to implement the Inquiry's recommendation. However, we subsequently sought and received Treasury's agreement to proceed with our review of the Code, in its voluntary form, to ensure the Code could be updated in some key areas in which it had fallen out of date.

Note: See Financial System Inquiry, final report, Recommendation 16 (November 2014).

13 With the onset of the COVID-19 pandemic from early 2020 ASIC has also had to make appropriate adjustments to its internal priorities and the demands placed on stakeholders engaging with the review. This has meant that the completion of this review has taken longer than initially anticipated.

Making the Code mandatory

14 Since the recommendation in the final report of the Financial System Inquiry, other reviews have made similar recommendations. These include:

(a) in 2019, the Council of Financial Regulators in its review of the Regulation of Stored-value Facilities in Australia; and

(b) in 2021, Treasury in its Review of the Australian Payments System and the Parliamentary Joint Committee on Corporations and Financial Services in its inquiry into Mobile Payment and Digital Wallet Financial Services.

Note: See Treasury, Review of the Australian Payments System, final report, Recommendation 10 (June 2021) and *Transforming Australia's payments system* (December 2021).

15 The Government responded in December 2021 to Treasury's Review of the Australian Payments System, including agreeing with its recommendation for the Code to be mandated for 'payments licensees' (a new form of licensee). The Government stated that it would commence consultation in early 2022 to determine how the Code should be updated and brought into regulation.

16 We have obtained and analysed a significant amount of information throughout the course of our current review, which we anticipate will provide useful background for the Government's subsequent work to mandate the Code. We look forward to sharing insights from our review with the Government where it would assist.

17 ASIC proceeded with our review of the Code in its current voluntary form with the intention of ensuring that the Code's settings are appropriately positioned for today's consumers and service providers, given new technologies that have emerged and changes in the payments landscape since the previous review in 2010. While our review canvassed a range of significant issues and possible changes to the Code, we concluded that it is more appropriate that more significant policy issues be considered further during the process of developing and implementing a legislatively mandated Code.

18 Accordingly, the revised aim of our review has been to make some modest improvements to the Code to ensure it works as efficiently and appropriately as possible within its current parameters as an interim measure, noting that we have an obligation to conduct regular reviews of the Code.

19 We acknowledge the strong support from a significant proportion of stakeholders, including industry, for a mandated Code. We also acknowledge the many stakeholder concerns with the weaknesses inherent in a voluntary Code for such important issues.

20 We welcome the Government's recent proposal to commence work in 2022 on mandating the protections in the Code and consider that this report, setting out a range of stakeholder views on possible changes to those protections, may provide useful insights.

B Compliance monitoring and data collection

Key points

This section outlines stakeholder feedback on our proposals in CP 341 to:

- remove the requirement in clause 44.1 of the Code that subscribers must report annually to ASIC on unauthorised transactions;
- retain ASIC's power in clause 44.2 of the Code to undertake ad hoc targeted compliance monitoring of specific obligations in the Code; and
- extend the ad hoc monitoring power so that ASIC may seek data and information to monitor or survey matters relevant to subscribers' activities relating to electronic payments.

Consumer groups did not agree with our proposal to remove the requirement for subscribers to report to ASIC annually, but were otherwise supportive of the changes. Other respondents also supported the changes.

We will proceed with the proposals, noting that they will not diminish ASIC's capacity to collect data as we consider appropriate.

Proposal B1: Compliance and industry monitoring

21 In CP 341, we proposed to remove the requirement in clause 44.1 of the Code that subscribers must report annually to ASIC or its agent information about unauthorised transactions: see proposal B1(a).

22 We also proposed to retain ASIC's power to undertake ad hoc targeted compliance monitoring (currently in clause 44.2), but specifying two distinct functions:

(a) monitoring subscribers' compliance with Code obligations (which already exists in clause 44.2); and

(b) monitoring or surveying matters relevant to subscribers' activities relating to electronic payments: see proposal B1(b).

Feedback received

23 The banking industry generally supported removing the requirement for annual reporting in clause 44.1 of the Code, citing the significant resources needed to comply with this requirement—particularly for smaller entities—and the potential for duplication of some data that is already potentially available to ASIC from third parties.

24 For example, the Australian Payments Network reports twice-yearly on fraud statistics and the Australian Financial Crimes Exchange currently facilitates the listing of key transactional frauds for the purpose of collating

losses and sharing relevant intelligence. One subscriber that is not an authorised deposit-taking institution (ADI) commented that ASIC's cessation of annual reporting could free up resourcing and assist ASIC in being more proactive in its compliance monitoring by focusing on new and emerging issues.

25 Consumer groups generally did not support our proposal to remove the annual reporting requirement. They noted:

(a) the growing threat and incidence of electronic payment related frauds; and

(b) the importance of the reporting in ensuring transparency of industry practices in dealings with consumers and the extent of harm to consumers caused by unauthorised transactions and enabling systemic and/or conduct issues to be identified and acted upon by ASIC.

26 Consumer groups observed that it is important for ASIC to obtain regular and ongoing data to inform trends. They contrasted our proposal to the United Kingdom's Payment Systems Regulator's requirement on banks to publish data on performance relating to scams and reimbursement of victims.

27 In principle, the banking industry was generally supportive of our proposal to retain an ad hoc monitoring function as an alternative to annual data collection. However, this support was subject to ASIC consulting with industry within a reasonable amount of time in advance of any data or information requests to minimise the degree of manual work required by the industry in collecting and collating the data, to avoid potential duplication of data already available to ASIC from other third parties and to ensure consistency of respondents' interpretation of key terms in the requests.

28 Consumer groups generally supported our proposal for ASIC to retain the ability to make ad hoc requests and to extend this to requests for information beyond merely compliance-related information. They encouraged ASIC to consider collecting this type of information on an ongoing basis, rather than in one-off requests.

ASIC's response

ASIC will implement proposals B1(a)–(b) in CP 341 to:

- remove the requirement in clause 44.1 of the Code that subscribers must report annually to ASIC on unauthorised transactions;
- retain ASIC's power in clause 44.2 of the Code to undertake ad hoc targeted compliance monitoring of specific obligations in the Code; and
- extend the ad hoc monitoring power so that ASIC may seek data and information to monitor or survey matters relevant to subscribers' activities relating to electronic payments.

ASIC does not consider that the value produced from the requirement for annual collection of unauthorised transaction data outweighs the burden on subscribers (particularly smaller entities).

The data we collected over a three-year period (2015–17) was not readily comparable across all subscribers due to a number of factors, including mergers within industry (making comparison from year to year difficult) and an apparent divergence across industry in categorising data and interpreting key terms in our notice.

While the information we received offered some detail about the incidence of unauthorised transactions during that period, it did not give us information about the extent of subscribers' compliance with relevant Code obligations.

ASIC considers there is benefit in having tools in the Code that allow us to choose our particular focuses, as the needs arise, in terms of Code topics and particular segments of the industry (rather than necessarily always having to call on every single subscriber for particular data requests).

We acknowledge the desire by consumer groups for ASIC to gather data on an ongoing and regular basis to identify trends. We consider it likely, within the parameters of our ad hoc monitoring powers, that ASIC will have the option to focus on targeted areas either on a one-off basis or effectively, with industry and other stakeholder consultation and input, on a recurring basis over specified periods.

Extending the ad hoc monitoring power to other matters relevant to subscribers' activities relating to electronic payments (i.e. not only focusing on compliance with Code provisions) will allow ASIC to understand emerging trends and adapt the Code as necessary.

C Clarifying and enhancing the mistaken internet payments framework

Key points

This section sets out stakeholder feedback relating to our proposals in CP 341 for:

- allowing for the partial return of funds;
- ensuring ADIs act promptly on reports of a mistaken internet payment;
- requiring certain standards of record-keeping;
- informing the consumer of their right to make a complaint;
- recourse for consumers against the receiving ADI;
- the definition a mistaken internet payment; and
- making the on-screen warning more relevant.

Consumer groups were strongly opposed to our proposal to clarify the definition of 'mistaken internet payment' to exclude payments made as a result of scams and our inclination not to establish a framework to allow recourse by a consumer against a receiving ADI.

We do not consider the mistaken internet payments framework to be suitable to assist in the return of funds in relation to scams. The mistaken internet payments framework is a facilitative framework—rather than a mechanism for allocating liability—designed to assist a consumer in retrieving funds from an unintended recipient.

Further, the speed with which scammers withdraw their victims' funds from the receiving account means that the process of retrieving the payment through the Code's mistaken internet payments framework is generally unable to be carried out with sufficient speed to secure the lost funds.

We will proceed with our proposals, subject to some small adjustments.

Proposal C1: Partial return of funds

29 In CP 341, we proposed to amend the Code so that the mistaken internet payments process applies not only where there are sufficient funds available in the unintended recipient's account to cover the mistaken internet payment (i.e. the current position in the Code) but also where only a portion of the funds is available in the unintended recipient's account: see proposal C1.

30 The purpose of our proposal was to ensure that the consumer who made the mistake (the 'paying consumer') has an opportunity to retrieve at least a portion of the funds, rather than the current 'all or nothing' position.

Feedback received

31 We received general in-principle support from stakeholders for the proposal. Respondents—both industry and consumer groups alike—acknowledged that the proposed amendment offers better protection than the current situation for the paying consumer.

32 Consumer groups generally observed that the proposal aligns with the idea that an unintended recipient generally should not benefit from someone else's mistake and that the mere presence of only a portion of the funds in the unintended recipient's account does not make it fair for the recipient to keep those funds.

33 The banking industry generally observed that the proposal would benefit paying consumers, noting that there are potential benefits in limiting the paying consumer's loss and reducing the time taken to retrieve funds (albeit partially).

34 However, banking industry respondents also made the following observations:

(a) It would be appropriate for the receiving ADI to have discretion on whether to pursue the full or only a partial amount. Where there are insufficient funds in the unintended recipient's account, receiving ADIs should not be compelled by the Code to pursue one option over the other (i.e. partial versus complete return of funds).

(b) How the receiving ADI exercises the discretion would depend on the particular circumstances of the individual case, considering matters such as the financial impact on the unintended recipient and the time that has elapsed since the mistaken internet payment. This should form part of what contributes to the receiving ADI's use of 'reasonable endeavours' to retrieve the full amount of the funds under clause 32.1.

(c) It would be useful for ASIC to include guidance in the Code to assist the receiving ADI in how to exercise its discretion (with the interests of both the paying consumer and unintended recipient in mind) and what actions would meet the 'reasonable endeavours' requirement.

35 Some consumer groups observed that guidance by ASIC would clarify for consumers what assistance that they can reasonably expect to receive if they make a mistaken internet payment.

36 A range of respondents suggested that including a non-exhaustive list of what amounts to 'reasonable endeavours' should be considered as guidance only and should not necessarily indicate how a particular matter will be determined.

ASIC's response

ASIC will implement proposal C1 in CP 341 with the following adjustments:

- If there are insufficient funds in the unintended recipient's account, the Code will give the receiving ADI discretion to decide which option (i.e. complete funds, partial funds or no

funds) is appropriate to pursue in the circumstances (i.e. the Code will not mandate one particular approach over another).

- The Code will support the exercise of this discretion by including guidance in the form of a non-exhaustive list of the types of factors that may be relevant to a receiving ADI in deciding how to appropriately exercise its discretion and meet the 'reasonable endeavours' requirement.

We consider that consumers should receive Code protections regardless of whether there are full or partial funds available in the unintended recipient's account.

We agree there is a fine balance for the receiving ADI in how far they should pursue the unintended recipient for the full amount of the payment. We agree that it is appropriate for the receiving ADI to exercise its discretion, considering all information reasonably available to it about the unintended recipient and the circumstances of the mistaken internet payment.

We acknowledge that introducing a framework for the retrieval of partial funds involves a range of issues that may warrant some guidance in the Code to help consumers understand what to expect when reporting a mistaken internet payment and to support ADIs in exercising their discretion so they can meet the 'reasonable endeavours' requirement.

We will seek assistance from key stakeholders in finalising a non-exhaustive list of examples and refining them as needed. Examples might include, but will not necessarily be limited to:

- whether the return of funds would be inconsistent with provisions of the *Social Security (Administration) Act 1999* or with Services Australia's Code of Operation;
- whether the return of funds would put the unintended recipient into a position of financial hardship;
- whether the return of funds would result in an overdrawing of the unintended recipient's account;
- the relative size of the mistaken payment;
- the perceived likelihood of ever achieving a return of the full amount; and
- the desire for all parties (the paying consumer, the ADI and the unintended recipient) to have certainty about timing for conclusion of the process.

We will clarify in the Code that the examples are for guidance only, are not an exhaustive list and do not constitute a 'safe harbour'. Whether a particular consideration is relevant in a particular case will depend on the circumstances of that case.

We do not intend to allow the receiving ADI to exercise its discretion if its investigations show that the *full amount* of the mistaken internet payment is available in the unintended recipient's account. In such cases, we expect that the receiving ADI will follow the settings currently in Code (i.e. clauses 28–30). We have not received significant stakeholder feedback to satisfy us that those particular settings should be altered.

Proposal C2(a): Time limit for mistaken internet payment retrieval

37 In CP 341 we proposed that the Code should 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: see proposal C2(a).

38 We considered it appropriate that a time limit should apply as there is currently no time limit in the Code. We sought a solution that appropriately balanced the need to act quickly (to enhance the chances of retrieving the funds) against what industry is practically able to achieve.

Feedback received

39 Industry feedback indicated that five business days (as a worst-case scenario) is reasonable to allow the sending ADI to consider the validity of the mistaken internet payment. Industry acknowledged the concern that these are time-critical situations. Some observed that the Australian Financial Complaints Authority (AFCA), and its predecessor, the Financial Ombudsman Service (FOS), have previously issued decisions setting out expectations that a sending ADI should aim to initiate a return request within two business days of being informed of the mistaken internet payment.

40 Consumer groups welcomed the inclusion of a time limit, noting it is a vital Code feature for triggering the retrieval process. They agreed that a prescribed time frame would provide greater certainty to the paying consumer about when their report would be actioned. However, they considered five business days to be too long and that it would present a high risk of the funds being withdrawn before they can be returned to the paying consumer. They argued that there is a risk of five business days becoming the default. Many encouraged ASIC to consider a time limit of one to two business days, noting the approach by AFCA and, previously, FOS.

41 One non-ADI respondent suggested that an option may be to prescribe a time limit of two business days or, if the sending ADI can show a reasonable need to extend that period, no longer than is reasonably necessary. Banking industry associations considered our original proposal in CP 341 would achieve a more appropriately balanced outcome. They agreed that industry best practice is for mistaken internet payment investigations to be initiated within one to two business days—and ideally on the same day.

42 However, these associations argued that at the external dispute resolution (EDR) stage, such an option could result in an ADI being found to be in breach of the Code if it fails to initiate the process within two business days. The 'reasonable need' requirement, they also argued, could be applied quite narrowly at the EDR stage.

43 As an alternative, banking industry associations suggested ASIC could note that industry best practice is to initiate investigations within one to two business days as much as possible to maximise the chance of retrieval.

ASIC's response

In prescribing a time limit for mistaken internet payment retrieval, ASIC will address industry and consumer group concerns by:

- retaining the proposal from CP 341 that the sending ADI must investigate the mistaken internet payment report and (if satisfied that there was a mistake) send a request to the receiving ADI for a return of the funds 'as soon as reasonably possible and, by no later than five business days'; and
- including a note to the effect that ASIC's expectation is that industry best practice on what amounts to 'as soon as reasonably possible' is for the sending ADI to commence the process within two business days—however, this will ultimately depend on the facts of the individual case.

We agree that consumers will benefit from having the Code prescribe a time limit for the sending ADI to investigate and make a request to the receiving ADI for a return of funds. This will trigger the commencement of the process in a timely manner.

We agree with other respondents that the time-critical nature of mistaken internet payment reports means that five business days can be too long.

We acknowledge there may be situations in which an ADI may need to undertake more significant work to establish whether it is satisfied that a mistaken internet payment has taken place. However, we do not anticipate that a sending ADI's lack of appropriate systems, processes or resources (unless there are exceptional circumstances beyond the ADI's control) would generally come within the parameters of reasonableness.

Proposal C2(b): Record keeping by sending and receiving ADIs

44 In CP 341 we proposed that the Code should require both the sending and receiving ADIs to keep reasonable records of the steps they took and what they considered in their investigations: see proposal C2(b). We considered such record keeping would mean useful information was readily available for AFCA's consideration to assist with the efficiency of dispute resolution.

Feedback received

45 Consumer groups were supportive of our proposal in helping with transparency of the recovery process and any further complaint processes. They also considered the proposal would encourage subscribers to develop simple processes in responding to mistaken internet payment reports. Some

consumer groups suggested that a prescriptive approach to minimum record-keeping standards would be preferable compared to a 'reasonable records' requirement, to ensure consistency across subscribers.

46 It was apparent from the feedback of some consumer group and other non-ADI respondents that enhanced record-keeping would also benefit consumers in understanding the steps taken by ADIs to recover funds. Conversely, banking industry respondents, while generally being supportive of prescriptive record-keeping requirements, encouraged ASIC to be clear about the purpose for which the records would be required and suggested that the purpose should be solely for the benefit of efficiency and completeness of information available to AFCA.

47 Industry respondents expressed concerns about the sharing of records with the consumer who made the report, due to risk of breaches of privacy requirements. They were also concerned about sharing certain information with AFCA that might amount to personal—and sometimes sensitive—information about the unintended recipient. They suggested that any such obligations in the Code should be stated as being subject to any other legal (e.g. privacy) obligations.

ASIC's response

ASIC will include a requirement in the Code that both the sending and receiving ADIs must keep records that are sufficient to demonstrate the steps they took to comply with the (mistaken internet payment) Code obligations, for the purposes of EDR.

We expect ADIs will be guided by the mistaken internet payments obligations in the Code in determining what records to create and maintain.

We will accompany this requirement with a note that subscribers also have obligations under the *Privacy Act 1988* (Privacy Act) affecting what information they can collect, how they can collect it and what information they can disclose.

We expect that the Code will require the sending and receiving ADIs to provide that information to AFCA, during the EDR stage, if requested, to the extent permissible under AFCA's terms of reference and under other legislation (e.g. privacy laws).

We anticipate that this requirement should assist AFCA in efficiently obtaining the information it requires to make decisions on complaints put before it.

Proposal C2(c): Consumer's right to make a complaint

48 In CP 341 we proposed that the Code should require the sending ADI, when informing the paying consumer of the outcome of the investigation into the reported mistaken internet payment, to include details of the consumer's right to:

(a) complain to the sending ADI about how the report was dealt with; and

(b) complain to AFCA about the sending ADI if they are not satisfied with the outcome of that complaint: see proposal C2(c).

Feedback received

49 Respondents generally supported this proposal. Consumer groups commented that it offers transparency, promotes increased trust by consumers and enhances access to justice when something goes wrong. Industry respondents did not voice significant concern with the proposal.

ASIC's response

ASIC will implement the proposal as set out in CP 341. We agree with respondents' feedback about the benefits of this proposal.

Proposal C2(d): Actions of the receiving ADI and unintended recipient

Assessing the sending ADI's compliance with the Code

50 In CP 341 we proposed that the Code should clarify that non-cooperation by the receiving ADI or the unintended recipient is not, by itself, a relevant consideration in assessing whether the sending ADI has complied with its Code obligations: see proposal C2(d).

Recourse against the receiving ADI

51 We noted in CP 341 that we were not proposing to alter the settings in the Code or consider changing the AFCA Rules to accommodate complaints by the paying consumer against the receiving ADI.

52 We also noted that the lack of a contractual or financial services relationship between the paying consumer and receiving ADI may present complexities in establishing arrangements for paying consumers to lodge complaints against the receiving ADI. AFCA cannot presently consider complaints against a receiving ADI because the ADI has not provided a financial service to the complainant: see Rule B.2 of the AFCA Rules.

Feedback received

53 Respondents generally supported our proposal to clarify that non-cooperation by the receiving ADI or the unintended recipient is not, by itself, a relevant consideration in assessing the sending ADI's compliance with the Code. Some consumer groups observed that it will help subscribers and consumers understand the sending ADI's obligations under the Code.

54 Industry respondents suggested that the words 'by itself' in our proposal should be removed because there should never be a situation in which the receiving ADI's or unintended recipient's conduct is relevant to assessing the sending ADI's Code compliance. They noted that the prospect of recovering funds for the paying consumer depends heavily on the receiving ADI's and/or unintended recipient's conduct.

55 Consumer groups voiced strong opposition to our positions about recourse against the receiving ADI. They argued that the inability of the paying consumer to complain against the receiving ADI presents a significant access to justice issue. They also observed that this position is at odds with the expectation that both ADIs should cooperate with one another under a Code that each has voluntarily subscribed to.

56 Consumer groups consistently argued that the lack of contractual obligations or provision of a financial service should not preclude a complaint by the paying consumer against the receiving ADI and that there is no clear reason why the AFCA Rules could not be altered to accommodate these scenarios. They observed that the AFCA Rules already allow AFCA to hear complaints in a range of situations which do not involve contractual or financial services relationships between the complainant and the financial institution.

57 Examples of these situations include third-party benefits under some insurance policies, a legal or beneficial interest arising out of financial investments or similar risk products, breaches of obligations arising from the Privacy Act or the Consumer Data Right (CDR) framework, or prospective consumers' rights to rely on commitments made under the Banking Code of Practice: see Rule B.2.1 of the AFCA Rules.

ASIC's response

ASIC will implement the proposal. However, we will remove the words 'by itself' so the paragraph reads:

> Non-cooperation by the receiving ADI or the unintended recipient is not a relevant consideration in assessing whether the sending ADI has complied with its obligations.

We agree that the actions or omissions of the receiving ADI and/or unintended recipient should not be relevant to assessment of the sending ADI's compliance with the Code.

We also do not intend to consider changes to the AFCA Rules at this time to allow for complaints by the paying consumer against

the receiving ADI. We recognise that this is a significant access to justice issue requiring further consideration and work by ASIC to assess the complexities and feasibility of potential solutions.

We note that AFCA can hear disputes in other situations without a financial services link between the complainant and the financial services provider, and it is not impossible to extend the AFCA Rules in this way. However, those situations are subject to some qualifications (e.g. lower monetary caps) and their inclusion in the AFCA Rules is based on detailed policy considerations.

Even if ASIC were to find a strong policy basis for amending the AFCA Rules, some complexities could arise for complaints against receiving ADIs. For example, there may be issues in protecting the privacy of the unintended recipient and it may allow the paying consumer to bring multiple complaints (i.e. against both the sending and receiving ADIs).

We acknowledge consumer groups' counterarguments that there does not appear to be a requirement to interfere with the unintended recipient's privacy and, in appropriate matters, it would be possible to join all parties into a single complaint so as to prevent multiple complaints by the paying consumer.

However, unlike the scenarios covered by exceptions in the AFCA Rules, the receiving ADI has no apparent legal relationship with the paying consumer. It is difficult to see how Code obligations, which only create contractual obligations between the consumer and their payment facility provider, can be used to create obligations in the absence of a contractual or other legal relationship.

Proposal C3: Definition of 'mistaken internet payment'

58 In CP 341 we proposed to clarify the Code's definition of 'mistaken internet payment' so it only covers actual mistakes in inputting the account identifier and does not extend to payments made to a scammer: see proposal C3.

59 This proposal was similar in effect to proposal E1 (see Section E), which related to the definition of 'unauthorised transaction'.

Feedback received

60 Consumer groups had significant concerns with this proposal and proposal E1, which they considered would result in a consumer protection void in relation to scams, if implemented.

61 In addition to feedback from respondents on proposal E1 as summarised in Section E of this report, the following key themes were raised in feedback from consumer groups:

(a) ASIC's proposal is inconsistent with the concept of the 'customer mandate', which requires ADIs to act in accordance with the customer's instructions when processing payments. If there are discrepancies

between that instruction and the identity of the recipient of the funds, ADIs should have a positive obligation to act with due care and skill and to make further enquiries.

(b) Where a consumer is tricked by a scammer into inputting an incorrect identifier into a payment instruction, that is essentially a 'mistaken internet payment' because the consumer made a mistake in inputting the identifier and/or has made a mistake about the identity of the recipient and the purpose of the payment.

(c) While industry has taken some steps to address scam conduct, their actions are not transparent. The lack of any standard offers no certainty for the consistent treatment of consumers in accordance with best practice.

62 Consumer groups also strongly advocated for obligations on ADIs to confirm the payee for the paying consumer before acting upon a payment instruction—something akin to the United Kingdom's 'Confirmation of Payee' framework. They commented that the risks associated with mistaken internet payments should not be assumed solely by consumers. If a subscriber fails to implement systems to ensure authentication of the payee, the subscriber should be liable for any loss suffered by the paying consumer.

63 While consumer groups recognised that the legacy payment infrastructure of the Bulk Electronic Clearing System (BECS) is being replaced, in due course, with other infrastructure such as the New Payments Platform (NPP), which has greater capability around account matching, they noted that the banking industry has been very slow in rolling out the NPP.

64 Respondents from the banking industry generally supported our proposal. They argued that applying the mistaken internet payments framework would be an inappropriate way to deal with the complex and evolving problem of fraud and scams. Payments made as a result of scams involve unique features that the Code does not cater for and, therefore, should be treated differently to mistaken internet payments. The Code does not consider the increasingly sophisticated nature of scams and associated consumer behaviour.

65 Further, recovery of transactions involving scams under the mistaken internet payments framework is increasingly challenging due to fraudsters quickly moving the funds out of the receiving account. Clarifying that scams processes are not subject to the mistaken internet payments process in the Code would allow better consumer outcomes to be achieved because scam transactions could be managed sooner (if not required to go through the mistaken internet payments process).

66 Some respondents acknowledged that the banking industry should play a greater role in providing accessible education and awareness-raising material to consumers through a range of channels and that the industry also has an important role to play in actively promoting and encouraging the roll-out of the NPP's 'PayID' (which has a name and account matching feature).

67 Industry respondents acknowledged that other actions on their part (and not focusing solely on what the *consumer* can do to protect themselves) is a necessary ingredient in finding solutions to the problem of scams.

> *ASIC's response*
>
> ASIC will implement the proposal as described in CP 341.
>
> We refer to the details of our response below in relation to proposal E1, which raises similar issues.
>
> Additionally, the mistaken internet payments framework has not been designed to allocate liability between the consumer and subscriber for lost funds. Rather, it is a process for the sending and receiving ADIs to assist the consumer, who has made the mistaken payment, in retrieving their funds from the unintended recipient.
>
> The framework is only of benefit to the consumer if the misdirected funds remain in the recipient's account. We note that, in the case of scams, funds are generally quickly withdrawn from the recipient's account.

Proposal C4: Onscreen consumer warning

68 In CP 341 we proposed to require additional important information in the onscreen warning about mistaken internet payments (required by clause 25 of the Code): see proposal C4.

69 In particular, we proposed that the warning should:

(a) contain a 'call to action' for the consumer to check that the bank/state/branch (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).

Feedback received

70 Respondents generally supported a warning that explains as clearly as possible the fact that matching of account identifiers (i.e. the BSB and account number) and names does not routinely occur. Consumer groups observed that their clients are generally surprised to discover that matching does not occur (despite payment instructions that involve the use of a BSB and account number also requiring inclusion of the account name).

71 Consumer groups were generally in favour of the Code being prescriptive in relation to the wording of the onscreen warning because it facilitates consistency across subscribers and will provide subscribers with certainty about their obligations.

72 However, consumer groups also observed the limitations of this type of disclosure, as noted in Report 632 *Disclosure: Why it shouldn't be the default* (REP 632) and as observed in their own case-work experience. They cautioned against this being used as a proxy for meaningful change to the verification process used by industry. They argued that it places an unreasonable level of responsibility on consumers to take care with a system offered by industry that is designed in a way that presents a high risk of user error.

73 Consumer groups strongly argued that the limitations of BECS—which, unlike the NPP, does not feature a matching mechanism—should not negate an ADI's need to use due care and skill when processing electronic payments.

74 Industry respondents preferred flexibility in the wording of the warning—they commented that prescribed wording could potentially cause issues for different payment platforms and could also be an issue depending on screen designs (e.g. a customer's screen is generally smaller on a mobile phone compared to a desktop computer). Industry also commented that allowing flexibility in the wording will allow institutions to stay 'on brand' in their messaging to customers and to adjust the messaging to the audience.

75 Industry has indicated support for exploring solutions such as (but not necessarily limited to) PayID, outside the Code context, to offer consumers better certainty regarding the payee's identity. ASIC has recently established regular quarterly meetings with industry associations and other relevant government regulators on this topic. Through these discussions, we aim to understand industry's initiatives in giving customers greater certainty about their payees' identities and to require industry to demonstrate the impact that their initiatives are having (e.g. on the incidence of certain types of mistaken internet payments and/or scams).

ASIC's response

ASIC will implement the proposal in CP 341 with some adjustments, as follows, for payment transactions involving the use of a BSB and account number.

The onscreen warning must include a 'call to action' for the consumer to check that the BSB and/or account number are correct and must state (in no particular order and not in a prescribed form or wording) that:

- if the consumer provides an incorrect BSB and account number, funds will be sent to the wrong account and it may not be possible to get the funds back; and

- if the subscriber does not match names and numbers to process payments—to state that the names and numbers will not be matched, verified or checked.

The current proposal is a slight modification to our proposal in CP 341, to ensure greater clarity around the fact that account name and number matching by ADIs generally does not occur.

We are anecdotally aware that many customers presume (incorrectly) that ADIs match name and account numbers and believe that, if they get the number wrong, the fact that they have correctly entered the account name will prevent a mistaken internet payment. This, we know, does not reflect the practice of almost all ADIs.

We understand that one driver for this misconception is that ADIs routinely require the paying consumer to enter the recipient's account name in the payment instruction. In practice, this information tends not to be used by the ADIs for the purpose of ensuring the funds are transferred to the intended recipient.

We consider it preferable to allow some flexibility in the wording of the onscreen warning to adjust to the target audience and to allow for improvement by individual ADIs in clarity and comprehension of the warning, should the ADI have the benefit of consumer research. We consider it appropriate that subscribers should, in wording their onscreen warnings, consider developing it in consultation with culturally and linguistically diverse users or communities.

We acknowledge a wealth of research indicating that many consumer warnings may be less effective than intended, may be ineffective or may backfire. However, the fact that a warning requirement already exists in the Code allows us an opportunity to make modest improvements to it.

While we do not intend to include a specific Code requirement on subscribers to undertake consumer testing and data collection on, for example, the relative success of their warnings, we would expect subscribers, as a matter of best practice, to test and adapt their warnings according to impacts on their customers.

D Extending the Code to small business

Key points

In CP 341, we proposed to extend the Code's protections to small businesses and include a definition of 'small business', while providing an opt-out arrangement where subscribers may elect not to extend the protection to their small business customers.

We had previously considered an extension of the Code to provide small business protections without an opt-out arrangement. However, industry were generally opposed to this and noted the lack of evidence to support an extension. We also considered an extension to businesses that are 'sole traders'. While there was some level of industry support for exploring the idea, we observed a general unwillingness to extend Code protections in this way. We then proposed an opt-out arrangement from small business protections as a compromise.

There was very little support for this compromise proposal. Some stakeholders noted that an opt-out proposal would have complexities (e.g. concerning how it would work in practice if some subscribers were to opt out while others did not). There was also a view that the question of whether to extend the Code to small businesses warranted further evidence-based consideration rather than having an interim opt-out process.

Others observed a number of practical issues with extending the Code to small businesses. For example, many small business payment facilities are designed with specific businesses and purposes in mind. The Code would need significant re-thinking to accommodate such facilities.

In the absence of industry support for this proposal (support which is necessary given the voluntary nature of the Code), we do not intend to extend the Code's protection to small business through this review mechanism, at this point in time. This may be a matter for further consideration in the process of mandating the Code.

Proposal D1: Opt-out arrangement

76 The Code does not apply to transactions performed using 'a facility that is designed primarily for use by a business and established primarily for business purposes': clause 2.1(a). Throughout our review, we considered a number of options for expanding the protections of the Code beyond just individual consumers. These included extending the Code to provide protections either to sole traders or small businesses more broadly.

77 In CP 341, we proposed extending the Code's protections to small business on an opt-out basis (i.e. subscribers may elect not to extend the protections to their small business customers): see proposal D1.

78 Our proposal in CP 341 was presented as an option to allow, in effect, for a transition from the current situation (in which the Code does not protect small business) to a future mandatory Code, for which the question of small business protections could again arise. We sought, through that proposal, to encourage subscribers to consider the merits of extending some enhanced protections to their small business customers and to do so if they could.

79 In the context of electronic payments, stakeholder feedback tells us that small businesses can have similar vulnerabilities and problems to individual consumers.

Feedback received

80 ASIC first proposed an extension of at least some of the Code's protections to small businesses in our 2010 review of the then Electronic Funds Transfer Code of Practice (EFT Code). However, there was insufficient support at the time for such an extension and limited data on the prevalence of electronic banking problems for small business customers.

81 Although there remains limited concrete data available to us that would support a need for an extension to small business, we proposed in our current review to explore extending some protections to small business on the basis that, since 2010, there has been a steady move to extend a variety of consumer protections in other contexts to small businesses.

82 While some respondents suggested an extension to small business was worthwhile, they did not point to concrete evidence or data to support this position. Some noted that small businesses now more than ever are vulnerable to mistaken internet payments and unauthorised transactions, as many have recently transitioned to e-commerce for the first time during the COVID-19 pandemic. Some, acknowledging the complexities in a Code extension at the current time, urged ASIC to revisit this question in the near future, with a focus on moving to a mandatory Code and expanding it to small business.

83 In contrast, a number of issues with the extension were identified by other—particular industry—respondents. These issues included that:

(a) the payments issues business owners face can be different from issues with consumer payments (e.g. businesses are more likely to have payment disputes rather than 'mistaken' payments);

(b) business customers use different products such as payroll systems, file-based direct entry payments, Health Industry Claims and Payments Service (HICAPS) payments, merchant acquiring and commercial cards, for which the Code was not designed, so many clauses of the Code would not correctly apply or may lead to unintended outcomes;

(c) some ADIs offer small businesses the use of payment platforms that are subject to their own set of security and authentication requirements and procedures, which are tailored to the needs of the small business in question and may not easily align with liability frameworks in the Code;

(d) there are complexities in ascertaining where liability for unauthorised transactions should sit for a small business whose staff, contractors or agents authorise transactions or breach pass code security requirements;

(e) it is difficult to find an appropriate definition of 'small business' (i.e. one that captures those businesses that require protection), including the point in time at which the definition is applied (e.g. when the payment facility is acquired or, instead, when a cause of action arises);

(f) costs would be incurred in updating systems and processes, with no guarantee that the Government would seek to maintain protections for small business in a subsequently mandated Code; and

(g) there is a risk that some subscribers could query their ability to continue subscribing to the Code if it is extended to protect small businesses.

84 Given the risks associated with a full extension of the Code to cover small business, we considered coupling such an extension with an opt-out mechanism to enable subscribers to opt out of providing the additional protections to small businesses where they decided it was not feasible for them. We considered that such a mechanism could:

(a) provide a transitional period between a Code that doesn't protect small businesses to one that does; and

(b) allow subscribers, who are unable to extend protections to small businesses, to opt out without unsubscribing from the Code entirely.

85 There was very little support for an opt-out mechanism, even among some small business representatives and independent government bodies. Some of the issues included the following:

(a) Applying the protections for some subscribers but not others would create a lack of clarity about the scope and application of the Code—the opt-out mechanism would result in an unequal application of the Code to customers across subscribers, causing inequity and confusion.

(b) The proposal would leave a significant regulatory policy question with individual industry participants to decide (i.e. whether to extend protections to their small business customers).

(c) Given the Code is voluntary, there may be reputational advantages for those subscribers with the resources to offer such protections and, therefore, disadvantages for smaller subscribers with fewer resources.

(d) Arguably, insufficient work has been done by ASIC to identify a regulatory policy rationale for the proposal and how it can be implemented.

86 Our first round of consultations asked questions about the potential inclusion of 'sole traders' within the scope of the Code. While some in industry appeared to be open to the idea, some noted the definitional complexities and complexities relating to the fact that the distinction between a sole trader's business and personal accounts is not always clear.

87 They also commented that extending the Code to sole traders as an initial step, followed by an expansion to all small businesses later on, would have significant cost implications for industry and would not be a straightforward or low-cost transitional step for them.

ASIC's response

ASIC does not propose to expand the protections of the Code beyond individual consumers in this review.

We agree that a phased approach of extending first to sole traders and then later to small businesses would not be a simple process for industry—noting that each step would require significant system and process changes that would then become obsolete at the second phase (i.e. expansion to all small businesses).

Despite this, we remain of the view that the extension of consumer protections to small businesses would be sensible and that it broadly supports the position presented by a number of stakeholders that small businesses can be equally as vulnerable as individual consumers in relation to electronic payments.

We strongly encourage industry to continue considering the merits and viability of extending protections to some or all small businesses. We also note that this question is likely to arise again in the context of the process to mandate the Code.

Proposal D2: Definition of 'small business'

88 In CP 341 we proposed defining 'small business' as a business employing fewer than 100 people (similar to the AFCA definition). We proposed to apply the definition as at the time the small business acquires the relevant facility (i.e. at commencement of the contractual relationship with the subscriber): see proposal D2.

Feedback received

89 Industry respondents generally opposed the definition, on the basis that it was a 'blunt metric' (employee numbers) or that it could capture a large number of businesses that do not require Code protections, such as customers whose behaviour is not 'consumer-like'.

90 Stakeholder representatives urged consideration of the nature of payments issues experienced by small businesses and the unique types of payment facilities used by small businesses. They argued that our proposed point-in-time test for defining small business would create complexities and uncertainty for small businesses about whether they are covered for a particular event. For example, facilities in operation before the Code is updated would not be covered, while facilities that commenced after the update would be covered (causing inconsistencies across various small businesses and facilities).

91 Small business representatives suggested that a definition of 'small business' may not be as complex to implement as industry might suggest, referring to the Government's recent creation of a legislated Small Business Indication Tool, created to help industry decide which entities to report on for specific purposes in the COVID-19 economic environment.

92 We did not receive feedback from these respondents on ADIs' arguments about the different nature of small business payment functions and platforms.

ASIC's response

In light of our response on the proposal for an opt-out arrangement, ASIC has not provided a substantial response on the proposal for the definition of small business.

E Clarifying the unauthorised transactions provisions

Key points

In Section E of CP 341, we proposed some clarifications of the Code's unauthorised transactions provisions, including those provisions concerning pass code security and the allocation of liability.

The responses we received were diverse and often in opposition to one another, particularly where the proposals concerned screen-scraping practices and consumer protection from scam losses.

ADIs were generally supportive of our proposals. Consumer groups, however, strongly disagreed with our proposal to clarify when the unauthorised transactions provisions apply.

We intend to proceed with the proposals for the reasons set out below. In relation to scams, this does not preclude—and we would strongly encourage—further work to address scam losses outside the Code.

Proposal E1(a): How the provisions apply

93 In CP 341, we proposed amendments to the Code to clarify the existing position that the unauthorised transactions provisions in Chapter C apply only where a third party has made a transaction on a consumer's account without the consumer's consent: see proposal E1(a).

94 The provisions do not apply where the consumer has made the transaction themselves. We noted, though, that some types of 'remote access scams' (where the scammer initiates the payment without authority from the consumer, after having gained access to the consumer's internet or mobile banking, for example) may still meet the definition of an unauthorised transaction.

95 The focus of our position in CP 341 was not whether or not a transaction stemmed from a scam but, rather, whether the transaction was made by the consumer or a third party. Our proposal stemmed from what we perceived as a lack of clarity about when the provisions apply—in particular, when the consumer has made a transaction as a result of a scam (i.e. 'authorised push payment' (APP) scams).

Feedback received

96 Industry and consumer respondents alike strongly emphasised the current lack of clarity around how scams should be dealt with under the law. Both groups saw value in developing ASIC guidance specifically about scams, which could also guide AFCA's decision-making.

Industry feedback

97 Industry generally supported this clarification of the current position in the Code. However, while industry considered it clear that a transaction made by the consumer as a result of a scam should not fall within the definition of 'unauthorised transaction', they also suggested that some forms of remote access scams should not meet the definition of an unauthorised transaction despite such transactions having been made by a third party (i.e. the scammer) without the consumer's informed consent.

98 A key focus in the feedback from industry was that *all* scams should be expressly excluded from the Code (noting that our proposal would still result in possible subscriber liability for remote access scams as a type of unauthorised transaction covered by the Code). To allow some remote access scams to be covered by the Code, they argued, would result in a lack of clear delineation excluding all types of scams and could be a source of significant confusion and inequity for some consumers who are not protected while others are.

99 Industry respondents suggested that the Code go further and clarify what amounts to an 'authorised' transaction in situations where the consumer does not authorise a specific payment but has, for example, permitted access to a phone or mobile banking application, has provided pass codes (including one-time pass codes) to a scammer or has downloaded remote access software.

100 Failing to provide this clarity, they argued, may result in subscribers spending significant amounts of time seeking evidence to determine how a transaction occurred and whether it amounts to an unauthorised transaction. They suggested these factors should also be relevant in determining whether a consumer contributed to a particular loss.

Consumer-group feedback

101 Consumer groups strongly opposed our proposal and considered it a narrowing of the application of the current Code in relation to scams (when coupled with our proposal in C3 to exclude scam payments from the definition of 'mistaken internet payment').

102 They noted that scam losses are a significant and growing problem. They took the view that our proposal will result in a reduction in consumer protection and a regulatory void in relation to scam losses, as there is presently no clear alternative framework to offer protection.

103 Consumer groups noted that Australia does not have a framework similar to the United Kingdom's Contingent Reimbursement Model Code, which allows for reimbursement of customers' scam losses in certain circumstances if the customer has taken proper care of their account.

104 They also noted that, while there exists a range of legal principles as well as details of case law that provide some guidance about what steps an ADI should take in relation to scams, there remains a lack of clarity about a consistent standard expected of ADIs.

105 Consumer groups strongly emphasised ADIs' contractual duty to question a valid customer mandate—that is, they should exercise reasonable care and skill to ensure that transactions processed are consistent with a customer's wishes.

106 While some consumer groups appeared to acknowledge that the unauthorised transactions provisions—and the mistaken internet payments provisions—might in some cases be an awkward fit for a scam scenario, they considered it was important to retain the level of protection offered by the current interpretations of the Code provisions in the interim while there remained gaps in protection (e.g. in the general law or in the lack of a coordinated industry commitment to offering enhanced protections).

107 They argued that financial institutions should shoulder more responsibility for money lost to scams made by internet transfer, just as they generally reimburse customers who lose money to unauthorised card transactions or other fraudulent account activity.

108 Consumer groups also referred to some types of scams where the consumer may be said to be 'under the influence' of a third party such that the transaction should be taken to be unauthorised, citing romance scams or trust-based investment scams as examples. By limiting the scope of the unauthorised transactions provisions to transactions conducted by third parties without the consumer's consent, the Code overlooks situations in which a consumer is a victim of financial abuse or is coerced into transferring funds (such that their consent cannot be considered to have been genuine).

109 Further, where financial institutions are on notice about financial abuse, consumer groups argued that the Code should oblige subscribers to take reasonable steps to protect the customer's accounts. They further commented that they consider their interpretation is aligned with good public policy—that it is appropriate that financial firms bear greater liability for these sorts of scams given they are in a much better position to identify fraud risk and invest in capabilities to mitigate such risk.

110 Consumer groups commented that our Code review offers a timely opportunity to establish a robust regulatory framework in the Code for addressing a broad range of issues arising from unintended funds transfers, regardless of whether the transfers are performed by the consumer themselves or a third party with or without the consumer's consent.

111 Some consumer groups appear to acknowledge that the Code does not serve as a comprehensive model to address scams. However, they observe that there is a significant regulatory gap in this area—restricting the Code without first providing a comprehensive and binding framework for scams elsewhere (whether in the Code or elsewhere) at this time only makes the gap more harmful.

CDR framework

112 Finally, and separately from the issue of scams, some respondents suggested that the Code may need to be reviewed in light of the intention for the CDR framework to expand to include the capability to initiate third-party payments. In particular, the Chapter C liability provisions relating to unauthorised transactions may need to be reconsidered.

ASIC's response

ASIC intends to implement the proposal as described in CP 341 to clarify that an unauthorised transaction occurs only where a third party has made the transaction without the consumer's consent.

The aim of our intended update is to address the ambiguity currently in the Code, which has led to various interpretations. While we acknowledge that particular interpretations of the Code's provisions have in some instances had beneficial outcomes for individual consumers, we consider it appropriate to clarify that the provisions are, from the time of issue of the updated Code in 2022, not intended to cover scenarios in which a consumer themselves has made the transaction in question.

We acknowledge consumer representatives' feedback that, even if the original intention was not to cover scams under the unauthorised transactions provisions, various types of scams (and their associated transactions) were not in existence or anticipated at the time when the Code was previously issued and so the Code should adapt to cover these.

However, we note that such adaptation, if it were to work effectively and appropriately, would require significant policy considerations and a completely new set of Code rights and obligations. Such a framework could not simply fit within the existing unauthorised transactions provisions without affecting the transparency and simplicity of the existing Code settings.

We have considered leaving things as they are in the interim (that is, maintaining the current level of ambiguity, with the outcome that in some cases consumers may continue to benefit from an alternative interpretation of the provisions) pending clarification of this issue at the time when the Code is mandated. However, in ASIC's view, a code of practice that is ambiguous and lacks transparency is likely to be ineffective in achieving its aims.

Remote access scams

We appreciate the banking industry's concern that some types of remote access scams (where the scammer, and not the consumer, has made the transaction) will continue to meet the definition of 'unauthorised transaction. However, given this is only an interim Code position, we have chosen to prioritise clarity and transparency in the Code's provisions.

We do not intend to categorise matters into either 'scam' or 'non-scam' groups as the means for determining which ones are covered by the Code. It is not always clear what is and is not a scam. Rather, we think the greatest level of clarity in the Code can be achieved (in terms of what types of outcomes a consumer can expect) if the focus is on differentiating between 'authorised' and 'unauthorised' transactions. This reflects the current position in the Code.

Accordingly, we anticipate the following:

- It may generally be that a scammer's transaction as a result of having gained remote access to the customer's account will be prima facie *unauthorised*. It would then be the responsibility of the subscriber to undertake an investigation to determine appropriate allocation of liability in accordance with the Code's existing rules.
- It may generally be that a consumer's own transaction (e.g. as a result of an APP scam) will be prima facie *authorised*. That is the *Code's* position. However, we acknowledge that AFCA has a broader role in relation to scams, in terms of what it may take into account (e.g. considerations of vulnerability, the general law and fairness). Therefore, we anticipate that, in some cases, the outcome of a complaint may differ from what the Code strictly provides, as that outcome would be based on considerations external to the Code.

We acknowledge that this approach does not provide the clarity that industry or consumers seek on the predictability or certainty of outcomes in scams-related complaints. However, as noted in consumer group feedback (see paragraph 104), there is not an established or clear set of rules in Australia on how to deal generally with scams, and each case very much depends on its own unique circumstances.

We also acknowledge the strong concern by consumer groups about the gap in regulatory architecture relating to scams. However, at this time, in the absence of a clear and effective mechanism for protecting consumers against scams, our considerations and consultations in this review have led us to the view that, at this point, the Code is unlikely to be able to accommodate a regulatory framework for industry to respond to scams in a way that achieves the best outcomes for consumers as a whole.

Our approach does not contribute to enhanced availability of general law protections against scams, but it does allow a more tailored focus by industry on other options that may more successfully protect consumers from scams.

UK Model Code

ASIC is supportive, in principle, of the suggestion to explore a model similar to the United Kingdom's Contingent Reimbursement Model Code.

However, this is not something that ASIC can initiate and we consider it requires a Government-led approach to assess whether such a model can be accommodated within the Australian payments regulatory environment.

Industry engagement

ASIC and other regulators will continue their engagement with the banking industry to ensure we see the development of solutions that will have an impact on the incidence of scams.

We have recently commenced regular quarterly discussions with banking industry associations and other relevant government regulators to maintain a dialogue aimed at:

- sharing details about industry's current initiatives; and
- industry being able to point to tangible results from such initiatives.

Further developments in the CDR framework

We acknowledge feedback from respondents that the Code's liability provisions may need to be revisited to ensure consistency with future settings for third-party payment initiation under the CDR framework.

We will revisit the Code's relevant provisions as we develop a greater understanding of likely features of this framework.

Proposals E1(b)–(d): Pass code security requirements

113 In CP 341, we proposed amendments to the Code to:

(a) clarify the existing position 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 indemnified by the subscriber for that loss (see proposal E1(b));

(b) 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 prove, on the balance of probability, that the consumer's breach of the pass code security requirements contributed to the loss (see proposal E1(c)); and

(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 (see proposal E1(d)).

Feedback received

Clarifying that a consumer must not disclose their pass code

114 Consumer groups and the banking industry generally shared the view that it was not appropriate for consumers to be inputting their pass codes to service providers when the CDR framework is being rolled out by the banking industry as an efficient and secure way for consumers to share data about themselves without the need to share pass codes. Some argued that providing a pass code to any third party weakens the security of consumers' accounts and a failure to discourage the practice confuses the message that a person should *never* share a pass code.

115 Some respondents in the digital data capture industry have argued that the CDR framework, while aimed at allowing for the safe and efficient sharing of consumer data, is not yet at a stage where it is considered by the industry as a viable alternative offering to 'screen scraping' and other forms of digital data capture of such value as to outweigh the regulatory costs of participating in the CDR framework.

116 These respondents submit that digital data capture is used widely in the financial services sector by lenders, mortgage brokers, personal finance management solutions and accounting products to retrieve customer data. They comment that it is secure and cost-effective and is a valuable mechanism to empower consumers and facilitate competition in the provision of consumer credit and that its ease of operation is highly valued by consumers.

117 One respondent commented that, while they share the view that uptake of the CDR framework will eventually result in other digital data capture methods becoming redundant, they are concerned about the slow uptake and accessibility of this framework for a large majority of industry participants. They also noted that digital data capture is connected to a number of activities that currently sit outside the CDR framework (e.g. trading accounts and superannuation). Therefore, digital data capture will need to continue in parallel with the CDR framework until its reach is significantly expanded.

118 We have observed that, while some in the industry have considered CDR framework accreditation, some might use a hybrid (CDR framework and screen scraping) model and others are not keen to explore using the CDR framework at all for now.

119 Industry participants have submitted that the proposal to clarify in the Code that a consumer risks being liable for loss from an unauthorised transaction if they disclose their pass code presents some disadvantages to consumers. For example, preventing data sharing:

(a) creates inconvenience for customers when applying for a product (e.g. a loan);

(b) prevents customers from viewing multiple banking accounts within the same interface (therefore not allowing a complete view of a customer's financial position); and

(c) does not allow a lender to gain a more holistic understanding of a prospecting borrower's financial behaviours over a given period.

120 Those respondents appeared to acknowledge ASIC's appreciation of the complexities associated with transition to the CDR framework. While noting that maintaining the 'status quo' in relation to pass code security requirements in the Code does not deliver a resolution, they commented that ASIC's proposal, to an extent, provides a layer of certainty that has been sought by service providers and consumer advocates alike.

121 However, such respondents were concerned that ASIC's proposal makes a strong implication that consumers will not be protected from financial loss related to the use of a third-party service unless it is explicitly promoted, endorsed or authorised by the subscriber—and this could justify subscribers' continued proactive efforts to forbid the use of digital data capture technology, which itself creates substantial barriers to competition.

122 Participants in the digital data capture industry have consistently commented to ASIC that their security arrangements and terms of service are such that a consumer's inputting of internet banking credentials will not amount to 'disclosure' of a pass code—for example, the use of encryption ensures that no third party ever views the pass code and could not use it to make transactions on the consumer's account.

123 However, the banking industry observed that, while it may be possible in some situations for a consumer to share a pass code with a 'screen scraping' service without *disclosing* it, this very much depends on the particular security arrangements and terms of service of the individual service providers. Therefore, it cannot be said with certainty that in all cases there would never be 'disclosure' of a pass code in breach of the Code.

124 Some consumer groups argued that it is not possible in any scenario for a consumer to input a pass code to a screen scraping service without it amounting to 'disclosure'. The banking industry generally supported a clarification in the Code that consumers cannot disclose their pass code to anyone without risking being liable for a subsequent unauthorised transaction.

125 While some consumer groups supported encouraging consumers to instead use the CDR framework for sharing of their data, they were concerned the proposal could result in consumers in vulnerable situations being considered in breach of the pass code security requirements if they were to disclose their pass code to a person who is subjecting them to duress, financial abuse, elder abuse or domestic violence.

126 The banking industry argued that 'disclose' should have the broadest meaning possible, as there are many ways in which a consumer may disclose their pass code in a manner that may lead to loss. They also observed that it is often the case that the subscriber does not have sufficient information available (compared to what the consumer may know about the circumstances of the transaction) to determine whether disclosure has occurred.

127 Some respondents queried whether the Code could be updated to reflect consumers' increasing use of digital password managers. They observed that clause 12.3 implies that keeping an electronically stored record of pass codes should be permitted. (A note to this clause suggests that keeping a written record of a pass code in a locked container is adequately protecting one's pass code security, in the context of considering whether there was 'extreme carelessness' by the customer.)

The need for subscribers to evidence a contributory link

128 Consumer groups generally welcomed the proposal to clarify the general rule that, unless a subscriber could show that a consumer's breach of the pass code security requirements contributed to an unauthorised transaction, the consumer would not be liable for the financial loss—that is, a breach of the pass code security requirements *in itself* (without evidence by the subscriber of the contributory link) is not sufficient to allocate liability to the consumer.

129 They urged ASIC to further state in the Code that inputting one's pass code into a screen scraping service will not result in a consumer losing their protections under the Code. Conversely, the banking industry suggested that the Code clarify that screen scraping can result in unintended disclosure of pass codes and could be one factor that contributes to loss from an unauthorised transaction.

Implicit promotion, endorsement or authorisation of the use of a service

130 Some in the digital data capture industry argue that an ADI implicitly endorses the use of a third-party service if the ADI either:

(a) is aware that its customers are using the service, yet fails to prevent such use; or

(b) uses that third-party service for its own specific purposes.

131 Other stakeholders do not share this view. In particular, some in the banking industry argue that there are no circumstances in which it should be implied that a subscriber is promoting a particular service. Some note that the challenge for subscribers is that they are unlikely to be aware of when a consumer uses a screen scraping service. Others appear to think it may be possible in some cases for a subscriber to identify their customers' use of such services and that they can therefore mostly prohibit the use of the services.

132 Some in the banking industry note that the difference between the subscriber using a third-party service for their own purpose and one of their customers using the same service for other purposes is that the subscriber, in the former scenario, has control over the terms of that use. In the latter scenario, the subscriber has limited or no control over their customer's relationship with the third-party provider.

133 Some consumer groups oppose any clarification that a subscriber has not approved a customer's use of a third-party service merely because the subscriber has chosen to use that service provider for its own purposes or has failed to actively prevent a particular customer's behaviour. They consider that if subscribers are promoting the use of a service in their general operations, it is unfair to place the risk of loss associated with use of that technology on the consumer.

ASIC's response

ASIC intends to implement the proposals from CP 341 except that, where we proposed to provide some examples of scenarios that amount to express or implicit promotion, we instead intend to provide clarification on what *does not* amount to 'implicit authorisation' by the subscriber.

That is, a subscriber is not taken to have approved the consumer's use of a particular service merely because the subscriber has:

- chosen to use that service provider for its own purposes; or
- failed to actively prevent particular consumer behaviour.

Our proposal does not prevent consumers from using screen scraping services. It does aim to clarify the existing position that a consumer does so at their own risk that, should the inputting of their internet banking credentials for this purpose amount to 'disclosure' and contribute to an unauthorised transaction, they may be liable for the resulting financial loss.

Our proposal also aims to address the current 'grey area' regarding interpretation of what amounts to implicit authorisation of a consumer's use of a third-party service. Note 1, immediately below the current clause 12.9 in the Code, describes a scenario in which a subscriber permits a consumer to give their pass code to an account aggregator service offered by the subscriber—this is an example of promotion, endorsement or authorisation referred to in clause 12.9.

However, we consider it a step further to suggest that the scenarios noted (i.e. the subscriber has chosen to use that service provider for its own purposes or has failed to actively prevent particular consumer behaviour) should meet the tests in clause 12.9—these appear quite distinct from the scenario in Note 1.

In maintaining the status quo (but with the proposed clarifications), it would remain the case that the consumer would only be liable for an unauthorised transaction if the use of that

service amounted to the 'disclosure' of a pass code and the subscriber could prove, on the balance of probability, that the use of the service contributed to the loss.

We think this position maintains an appropriate balance, allowing the use of potentially beneficial services to continue while industry gradually transitions to the CDR framework and as the regulatory and operational aspects of this framework gradually evolve.

The final report following the 2017 Review into Open Banking in Australia stated that 'Open Banking should not prohibit or endorse "screen scraping", but should aim to make this practice redundant by facilitating a more efficient data transfer mechanism'.

> Note: See Treasury, *Open banking: Customers, choice, convenience, confidence*, final report, December 2017, p. x.

More recently, the Senate Select Committee on Australia as a Technology and Financial Centre recommended that the Government 'maintain existing regulatory arrangements in relation to digital data capture'.

> Note: See *Interim report*, September 2020, Recommendation 22.

The final report following the Inquiry into Future Directions of the Consumer Data Right stated, 'due to the risk involved, the eventual prohibition of screen scraping for payment initiation would be in the interests of consumers', and recommended that 'strong consideration should be given to prohibiting the making of a payment through third party access to digital banking portals'.

> Note: See Treasury, *Future directions for the consumer data right*, final report, October 2020, p. 97 and Recommendation 5.17.

However, it was suggested that this should only occur once equivalent CDR framework functionalities are fully implemented as viable alternatives.

We acknowledge the various requests for clarity within the Code on what amounts to 'disclosure'—namely the following:

- Digital data capture service providers argue that inputting one's credentials into the service does not amount to disclosure because the credentials are not human-readable.
- Consumer groups argue that there should be exceptions to the rule against disclosure of a pass code in situations where a personal is experiencing vulnerability such as financial abuse, elder abuse or domestic violence.
- The banking industry argues that what can amount to 'disclosure' is potentially very broad.

However, we do not propose to include guidance within the Code to clarify this concept in individual scenarios. This is because it would require the Code to reach a significant level of specificity that we think is best considered on a case-by-case basis by the subscriber or dispute resolution body—that is, the subscriber's internal dispute resolution (IDR) procedures or AFCA.

For example, we anticipate that the term 'disclosure' should take its ordinary meaning and that subscribers, when investigating an

unauthorised transaction involving the potential disclosure of a pass code to a third-party service provider, will need to examine things such as the security arrangements and terms of service that the third-party service provider had in place.

Although we acknowledge that this requires more work on the part of the subscriber to ascertain whether the specific scenario involved 'disclosure', we consider it appropriate that it not be assumed in all cases that use of a third-party service provider necessarily involves disclosure (within the ordinary meaning of the term) of a pass code.

With regards to consumer groups' desire for exceptions to the disclosure prohibition in situations of vulnerability, again, we consider it a complex and inappropriate task to include within the Code a range of exceptional situations, which will need to be considered on a case-by-case basis.

We note that a significant portion of Code subscribers already make considerations relating to vulnerability in a range of situations in providing their banking services. For example, members of the Australian Banking Association have agreed across their industry to adhere to best practice guidelines relating to vulnerable consumers.

We would expect that all subscribers to an extent would take into account various matters relating to vulnerability when applying particular Code settings if individual cases should warrant it. We do not agree that the Code can appropriately strike the right balance in this regard, given the unique factors in each case, without risking an unintentionally broad or narrow application or interpretation of such wording. This would risk detracting from our aims of clarity and simplicity in the Code.

Further, we anticipate that, in circumstances where a consumer has disclosed their pass code because of financial abuse, duress or other unconscionable conduct, AFCA may continue to consider matters of reasonableness and fairness in appropriate cases in accordance with its terms of reference.

Proposal E1(e): Unauthorised transactions provisions and chargebacks

134 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.

135 In CP 341, we proposed amendments to the Code to clarify that the provisions concerning the allocation of liability for an unauthorised transaction are separate from any chargeback arrangements available under card scheme rules: see proposal E1(e).

Feedback received

136 We observed general support for this proposal from respondents.

137 Some consumer groups observed previous issues where subscribers had failed to comply with the six-year limitation period under the Code for unauthorised transactions where chargebacks were also applicable. That is, consumers had been barred from seeking any remedy due to having exceeded the time limit prescribed in the card scheme rules, when they should have had up to six years under the Code to report the unauthorised transaction and have it investigated according to the Code's liability framework.

138 Some other respondents agreed that the difference between the unauthorised transactions provisions and card scheme chargeback processes may be a source of confusion for subscribers and consumers.

ASIC's response

ASIC intends to implement the CP 341 proposal.

We agree that the distinction between the two frameworks—the Code's unauthorised transactions provisions and the card scheme chargeback frameworks—can be a source of confusion. We have observed occasions where Code subscribers have failed to investigate consumers' reports of unauthorised transactions due to the consumer having missed the cut-off date (which is generally around 120 days) under the card scheme rules, despite the six-year limitation period in the Code not having yet elapsed. We have taken the view that a representation by a subscriber to their customer to this effect is likely to be misleading.

Our proposal is intended to ensure that the two distinct frameworks are treated as such, and that consumers continue to have protections under the Code's unauthorised transactions provisions even if they have missed the deadline under the chargebacks framework.

F Modernising the Code

Key points

In this section we have outlined the feedback received in relation to a range of proposals that would modernise the Code. These included:

- accommodating biometrics in the Code;
- modernising the definitions of 'device', 'identifier' and one-time passwords;
- applying the Code to the NPP; and
- aligning the rules for digital receipts with those for paper receipts.

Respondents generally supported introducing biometrics into the Code but some were concerned about the unintended consequences of doing so and the need to place some responsibility on consumers to better protect their personal devices. After considering the feedback and conducting further analysis, we have decided not to proceed with this proposal.

We received feedback in support of modernising some definitions and we will proceed with some of our proposals and will also make other adjustments.

All respondents supported applying the Code to the NPP. We intend to proceed with this proposal.

We will also align the rules for digital and paper receipts, but we received only very limited feedback about this proposal.

Proposal F1: Biometrics

139 In CP 341, we proposed to define 'biometric authentication' in the Code and to 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 or facial recognition) where previously only pass codes could be used: see proposal F1.

Feedback received

140 Consumer groups generally supported the proposal to accommodate biometric authentication within the Code, because it will allow the Code to respond to improvements in technology that have emerged since the previous update of the Code.

141 These groups supported the position that biometric authentication should not be included within the existing definition of 'pass code', given the inherent differences between a pass code and biometric authentication (in particular, that the latter cannot be kept secret in the way that a pass code can).

142 The banking industry, while generally acknowledging the need to accommodate biometric technology within the Code, expressed some hesitation towards introducing a new defined term 'authentication method' and simply accommodating biometric authentication within existing Code clauses without more clarity on the problem that ASIC is attempting to address with its proposal.

143 Instead, the banking industry encouraged ASIC to consider a more fulsome modernisation of the Code and more holistic approach to accommodating biometric authentication—rather than identifying specific existing provisions for accommodating the concept within existing parameters of the Code.

144 In particular, they urged ASIC to consider updating settings in the Code and establishing a unique set of rules to address more broadly:

(a) how consumers can protect themselves when using personal electronic devices to make payments; and

(b) what subscribers' obligations are regarding access to and use of consumers' personal devices that have been manufactured by entities who do not subscribe to the Code.

145 This is broader than just the issue of biometrics and goes towards consumers' protection of personal electronic devices more broadly. For example, industry noted the current example of 'extreme carelessness' (in protecting one's account) relating to the keeping of a pass code on a computer that is not password protected and/or in a file named 'internet banking codes'.

146 The banking industry respondents suggested that the modern-day equivalent could be a consumer allowing another person to:

(a) have remote access to their computer or smartphone and giving away passwords (or one-time passwords) allowing remote access while logging into their internet banking; or

(b) register fingerprint or facial recognition access to an electronic device that has payment functionalities enabled.

147 Industry suggested that existing ASIC proposals to modernise the Code also require ASIC to consider how consumers use their mobile phones and other electronic devices and, for example, how this affects the security of virtual credit and debit cards in the event that the consumer's personal electronic device is compromised or lost.

148 They argue that biometric authentication may warrant a number of standalone rules because, for example:

(a) A consumer does not record biometric information or keep a biometric 'secret'—it is therefore not meaningful to refer to biometrics being expired or cancelled or whether a consumer has 'received' a biometric in the mail (all of which is possible in the case of traditional pass codes).

(b) The Code would need to clearly address how biometric authentication would be treated under the Code's contribution rules relating to unauthorised transactions. For example, a consumer cannot 'give away' or disclose a biometric in the same way as they can a pass code, and the Code does not clarify what amounts to 'extreme carelessness' by a consumer in protecting their account.

(c) The Code may need to prohibit users from allowing third-party biometric access to their personal electronic devices (e.g. smartphone), if that device has digital payment methods enabled or access to mobile banking.

149 To not consider the above, and to only attempt to work biometrics into the existing Code provisions, banking industry respondents argue, addresses only one side of a multi-faceted issue that is best addressed more holistically with the benefit of further detailed considerations by ASIC with stakeholder input.

150 Further, the banking industry argues that biometrics are sensitive information under the Privacy Act and they caution against ASIC defining biometric authentication in a way that diverges from the Privacy Act or effectively establishes a distinct privacy regime for biometric information. They instead encourage the use of cross-referencing to definitions used in other legislation such as the Privacy Act.

151 They also note that any ASIC changes to the Code in this regard should be guided by the outcome of the Australian Government's review of the Privacy Act. That review remains underway and will extend into 2022. Submissions to ASIC's current Code review noted that the Government's review may result in further guidance on terms such as 'biometric information', 'automated biometric verification', 'biometric identification' and 'biometric templates'.

152 Some banking industry respondents also noted that it may be difficult to define biometric authentication in this rapidly evolving environment. The biological features that we use today for authentication of transactions or access to devices may evolve over time. There may also be movement towards the use of behavioural biometrics in the future, as opposed to physical characteristics.

ASIC's response

ASIC has decided not to proceed with our proposal in CP 341 at this time.

While we acknowledge that the emergence of biometric authentication is a key area of development since ASIC's previous review of the Code—and is a key area in which the Code has not kept up with technology—we agree that further work is needed to ensure that the benefits of accommodating biometric authentication within the Code are balanced appropriately against implications stemming from consumers' use of such technology.

For example, we consider it would only be addressing part of the picture if we were to try to accommodate biometric authentication within existing Code provisions (by replacing the term 'pass code' with 'biometric authentication' as appropriate in relevant provisions) without also looking at the other side of the picture regarding consumers' appropriate use of their personal electronic devices that have biometric access enabled.

We consider that our Code review should proceed towards completion so that we can achieve various other important updates, and that the question of accommodating biometrics into the consumer electronic payments regulatory space needs further engagement with stakeholders as a distinct piece of work.

We will apply further thought to the options for commencing such work, noting any progress in terms of likely timing for eventual mandating of the Code. This may assist us in determining whether ASIC should commence its own piece of work in the context of the voluntary Code or, instead, await Government initiation of work to mandate the Code before considering the policy settings relating to this topic.

Proposal F2: Defining 'device'

153 In CP 341 we proposed replacing the definition of 'device' with 'payment instrument': see proposal F2(a).

154 We noted that the Code defines 'device' as 'a device given by a subscriber to a user that is used to perform a transaction'. We also observed that the use of the term 'device' in the Code may be confusing for readers given that, since the previous review of the Code, many consumers have transitioned from initiating transactions using a subscriber-issued device (e.g. credit or debit card) to using their own personal electronic devices (e.g. smartphone or tablet).

155 We have observed that 'device' is now in common usage to describe one's own electronic devices, and we queried whether it may be helpful to use different terminology in the Code to describe subscriber-issued devices.

156 We also observed in CP 341 that, in many cases now, 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). We proposed to expand the definition of 'device' 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: see proposal F2(b).

157 We considered that a consequential amendment to the definition of 'identifier' may also be required to cover virtual cards and the increased use of 'tokenisation' in place of traditional identifiers such as card numbers.

158 In CP 341 we did not propose to accommodate the following:

(a) one-time passwords—that is, passwords generated for single-use for a particular access or transaction (e.g. sent via SMS) and sometimes used in conjunction with other pass codes or authentication as part of 'multi-factor authentication'; or

(b) concepts of 'tokenisation', 'card-on-file' or QR codes, which can be used in place of traditional identifiers such as card numbers.

159 We expressed the view in CP 341 that the Code appears to adequately capture concepts of one-time passwords and tokenisation, despite the Code not expressly referring to them. For example, when using tokenisation, we considered that the token is itself an 'identifier' within the Code's current definition of 'identifier'.

160 Further, regarding 'card-on-file', while the consumer is not re-entering their card identifier each time they make a transaction, we considered there is still use by the consumer of the device's identifier (e.g. the card number) to make the transaction. Accordingly, we did not consider it necessary to provide these clarifications in the Code.

Feedback received

161 The banking industry did not generally favour use of the term 'payment instrument'. They preferred to retain 'device' because the term is a commonly used term within the payments self-regulatory framework and has a settled meaning and it would not be a simple process to change. The new terminology would, for example, necessitate significant changes to subscribers' 'terms and conditions' documents.

162 Some consumer groups also did not favour the use of the term 'payment instrument', but for different reasons. They welcomed a change in terminology (agreeing with our views about the potential for confusion with the term 'device') but considered 'payment instrument' could be equally difficult to relate to. Some suggested instead using terminology such as 'what I use to pay' or 'what I pay with'.

163 Industry also had reservations about our proposal to clarify that virtual cards fall within the definition of 'device'. They argued that this would not make sense in relation to Code provisions that mention the loss, theft or misuse of a device or faulty devices, which presuppose the existence of a physical device.

164 Some respondents 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 and card-on-file. We did not observe opposition from any respondents to such an idea.

165 While appearing to acknowledge that the definition of 'pass code' already caters for one-time passwords, some banking industry respondents agreed that it would not be harmful to nevertheless include one-time passwords in the definition for avoidance of doubt.

166 Some respondents from the financial technology industry observed that one-time passwords perform vastly different functions from pass codes generally and that it is, therefore, important that each mention of 'pass code' in the Code is reviewed to determine whether it is appropriate to include one-time passwords as a subset of pass codes in that instance. They argued that one-time passwords and pass codes should not be placed in the same category.

ASIC's response

ASIC has decided not to replace the term 'device' with 'payment instrument'. In our view, the value in replacing the term 'device' with terminology that consumers can better relate to is relatively minor when compared with the likely costs to industry in reflecting such a change in, for example, their terms and conditions and their regulatory instruments.

We will clarify that virtual cards fall within the definition of 'device'. Despite there not being a physical device in the case of virtual cards, we think a virtual card (i.e. where only a number is available and not the physical card itself) can fairly seamlessly fit within the Code's existing definition of 'device' with only minimal change to the Code.

While we agree that references in the Code to loss and theft of a device, or faulty devices, might not be relevant to virtual cards, we do still see potential at least for 'misuse' of a virtual card (which is another scenario mentioned in the unauthorised transactions provisions in Chapter C of the Code). To retain references to loss or theft or faulty devices in relation to *all* devices (even though it will not be of relevance to virtual cards), in our view, causes no harm. We think it will be clear to the reader when certain concepts in the Code are not applicable to a virtual device. In the absence of further information, we are unconvinced that the approach needs to be more nuanced.

We will clarify that tokenisation and 'card-on-file' can be examples of 'identifiers'. A token is an identifier that replaces the user's known or readable identifier for the purpose of enhancing security for the user. We observe that it is used in the same way and for the same purpose as a regular identifier (e.g. card number) in order to perform a transaction.

We think the definition of 'identifier' probably does not go far enough to include tokens, at present. This is because 'identifier' is defined as 'information that a user knows but is not required to keep secret and must provide to perform a transaction'. The first part of that definition may not be met in some circumstances because the user might not be able to see the token. We see it as entirely within the policy intent of the current definition of 'identifier' to capture tokenisation.

While we are not convinced that it is strictly necessary to clarify that 'card-on-file' is an example of an 'identifier', we see no harm in making this clarification in the Code.

We will also clarify that one-time passwords are a type of 'pass code'. We consider that the Code's current definition of 'pass code' probably already caters for one-time passwords. We note that an example already given in the definition is a 'code generated by a security token', which we consider is of a similar purpose or nature to an SMS code, albeit generated through different means and perhaps an outdated example that was more common before the use of smartphones). Despite this, there appears to be no harm in adding a further example to the list of examples in the Code's definition of 'pass code', for the sake of clarity.

We are not convinced by the argument that one-time passwords should not fall within the definition of 'pass code'—this is because we still consider a one-time password, as is the case with other pass codes, is something that a consumer must keep secret that may be required to authenticate a transaction or user.

Proposal F3: Payment platforms

167 In CP 341 we proposed to expressly extend all relevant provisions to situations in which a 'Pay Anyone' payment is made through the NPP: see proposal F3(a).

168 We had observed that the Code's mistaken internet payment framework is presently 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.

169 In particular, the Code's definition of 'mistaken internet payment' and the mistaken internet payment 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 or account number. We considered that 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 the NPP's PayID).

170 While we had considered trying to make the Code payment platform neutral, earlier stakeholder feedback had 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 or bespoke arrangements in place by particular providers). Given the pace at which new payment platforms emerge, we considered it acceptable to refer specifically in the Code to the NPP and BECS rather than striving for neutrality. We indicated that, if any other relevant platforms were to emerge in the future, we would consider further amendments to the Code at the relevant time.

171 We also proposed to introduce a definition for 'Pay Anyone internet banking facility'—defined 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': see proposal F3(b).

Feedback received

172 There was general support from respondents for the proposal to accommodate the NPP within the Code. Some consumer group feedback supported technology neutrality, in order to remain flexible to the development of further payment platforms and new technology, but industry feedback was generally that express application to BECS and the NPP is necessary so as not to inadvertently include other payment platforms as described in paragraph 170.

173 We queried with respondents, including NPP Australia Limited (NPP Australia), whether there were any specific parts of the Code that would need to be adjusted to avoid unintentionally altering the intended operation of the Code simply by extending it to the NPP. Respondents generally did not identify anything requiring our specific attention in this regard. However, NPP Australia suggested we could align commencement of the Code's listing and switching rules for the NPP with the proposed commencement date of the NPP's upcoming 'PayTo' third-party payment initiation feature.

174 There was general support for the intent behind our proposal for the definition of 'Pay Anyone internet banking facility'. However, there was some industry feedback that the definition should be generalised to cater also for telephone and mobile banking, for example, as not all consumers use internet banking to conduct their Pay Anyone transactions.

ASIC's response

ASIC will extend the Code to transactions made using the NPP. The Code will expressly refer to BECS and the NPP and will not be platform neutral in its scope.

While we acknowledge the potential benefits of remaining platform neutral (e.g. allowing flexibility for the Code to apply to any new platforms that may emerge in the future), we also acknowledge the risk that platform neutrality may inadvertently capture other frameworks (as described in paragraph 170) that are not intended to be captured by the Code. We consider it preferable that ASIC revisit the Code's scope if/when a new consumer payments platform emerges.

As industry has not drawn our attention to any substantial likelihood of problems associated with extending the Code to the NPP generally, we do not propose to carve any particular Code provisions out of application to the NPP.

In particular, NPP Australia commented that the NPP's upcoming 'PayTo' (third-party payment initiation) service was designed with the Code in mind.

Further, while we acknowledge NPP Australia's suggestion to align commencement of application of the listing and switching rules to the NPP with the NPP's PayTo feature, we do not consider there to be any practical effect in not setting a future date for commencement of these particular provisions (and, instead, simply applying all of the Code to the NPP from commencement of the updated Code).

If adjustment is necessary once we are familiar with the specifics of PayTo and the types of service it enables, or if any issues emerge following our review that indicate any carve-outs may be necessary for the NPP, then it will be possible for ASIC to revisit this and potentially update the Code with further stakeholder consultation.

We also intend to proceed with our definition of 'Pay Anyone' facilities but, instead of using the term 'Pay Anyone internet banking facility', we intend to use the term 'Pay Anyone banking facility' to ensure this does not exclude transactions made by means other than internet banking.

Proposal F4: Transaction receipts

175 In CP 341 we proposed to amend the Code to accommodate the increased use of electronic transaction receipts and to align, to the extent it is appropriate, the rules applying to them with those already applicable to paper receipts (in clause 5 of the Code): see proposal F4.

Feedback received

176 There were limited comments from respondents on this proposal. Some industry respondents suggested that certain aspects of the requirement (e.g. stating the remaining balance, the type or general location of the equipment used or a reference number linking the transaction to a merchant-issued invoice) are not necessary or may in some instances give rise to privacy

risks. We did not receive further elaboration from those respondents on the particulars of these issues.

177 Some industry respondents also suggested ASIC could provide clarity in the Code on what is meant by 'complete identifier' in clause 5.3. Clause 5.3 requires that a paper transaction receipt must not include information that would increase the risk of unauthorised transactions, such as a 'complete identifier', which is not defined in the Code.

178 The banking industry generally observed that our proposal will offer further protection for subscribers and consumers.

179 Consumer groups also did not object to our proposal but suggested that information currently required on paper receipts should be required on electronic receipts.

ASIC's response

ASIC will implement our proposal from CP 341—that is, to ensure the clause 5 requirements apply equally to receipts regardless of whether they are first created in digital or paper form.

Most of the clause 5 requirements apply already to both paper and electronic receipts. The only requirement that applies only to paper receipts (and for which there is no requirement for electronic receipts) is clause 5.3, which details certain information that must not be included on a paper receipt.

We agree that there is value in defining 'complete identifier' for the purposes of clause 5.3 of the Code. Bearing in mind that fraud can be made possible in certain instances by the piecing together of information about a customer, we think it is appropriate that the rules about which portion of the identifier can be stated on a receipt should be consistent in all cases.

We note that the Payment Card Industry Data Security Standards (PCI DSS) (which all card scheme participants must adhere to) require the masking of all but four digits of the card number. Accordingly, we intend to define 'complete identifier' consistently with the PCI DSS.

However, we consider it appropriate that the requirement in clause 5.3 relating to 'complete identifiers' should not apply to transaction receipts stemming from Pay Anyone electronic funds transfers.

In Report 218 *Electronic Funds Transfer Code of Conduct review: Feedback on CP 90 and final positions* (REP 218), we noted stakeholder reservations about applying the receipt requirements to all electronic payment transactions. For example, non-truncated account details on a receipt may be required to establish that a payment has been made to a particular BSB and account number for an internet banking transaction or in-branch transaction.

This was in contrast to EFTPOS and ATM receipts, which we observed were rarely used for reconciliation purposes. Further, in ASIC's view, the possibility of a third party obtaining a receipt is lower for internet banking than for ATM and EFTPOS receipts, which are often printed and discarded in public places.

In REP 218, we accepted that consumers may benefit from having non-truncated account numbers on receipts as proof of payment to the right account, particularly when large amounts of money are involved. In response, we stated, 'We have therefore amended our proposal so that it applies to transactions initiated by credit card or debit card, including EFTPOS and ATM transactions, but not internet banking or in-branch transactions.'

We note that this appears to be the reason for the current clause 5.3 being limited to paper receipts. However, we suspect that, at the time of REP 218 (in 2010), ASIC understood that the only prevalent form of electronic receipts was for bank transfers and that other forms of electronic receipts available today (which are increasingly becoming the main medium of receipts for all sorts of goods and services) were not generally issued.

Just as a paper receipt can be discarded in public places, today's electronic receipts can be easily lost through security breach or misdirection through emails.

G Complaints handling

Key points

We will:

- replace references in the Code to RG 165 with RG 271, as ASIC has issued RG 271 to replace RG 165;
- retain the two distinct complaints frameworks that are currently in Chapter F and Appendix A of the Code, rather than combining them into a single framework;
- not require Appendix A subscribers to have EDR scheme membership;
- change references in Chapter F of the Code from 'complaints' about an unauthorised transaction to 'reports' (or similar) of an unauthorised transaction;
- relocate to Chapter C of the Code aspects of Chapter F that deal with investigation of unauthorised transactions, so that all aspects of the unauthorised transactions investigation process are housed within Chapter C of the Code; and
- retain the six-year limitation period for reporting unauthorised transactions.

Proposal G1: Internal and external dispute resolution

180 In CP 341 we proposed 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) (see proposal G1(a));

(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 investigations (see proposal G1(b));

(c) require all subscribers to have IDR procedures that are set out in RG 271 (see proposal G1(c)); and

(d) require all subscribers to be members of AFCA (see proposal G1(d)).

181 Following publication of CP 341, we raised with key stakeholders the option of replacing references in Chapter F to 'complaints' about unauthorised transactions with 'reports' of unauthorised transactions. We also considered relocating aspects of Chapter F of the Code to Chapter C so that all aspects of the unauthorised transaction investigation process are housed within Chapter C of the Code.

Feedback received

182 Consumer groups generally supported our proposal as a sensible way of consolidating the complaints handling framework and providing greater access to free dispute resolution mechanisms for consumers. Consumer groups generally were strongly supportive of updating references to RG 165 with new references to RG 271 and requiring all subscribers, even those subject to Appendix A ('Appendix A subscribers'), to be members of AFCA.

183 The banking industry generally supported the requirements, noting that having a consistent set of requirements for dispute resolution can help consumers understand how the Code protects them when using electronic payments. Further, they observed that RG 271 is of a high standard and contains obligations that need to be consistently applied in order to effectively manage complaints and assist customers. They were not aware of any reasons that may warrant retaining the two separate complaints frameworks within the Code (i.e. Chapter F and Appendix A).

184 We had limited feedback from subscribers identifying as Appendix A subscribers. However, those who did provide feedback noted that a transition to compliance with RG 271 (specifically, compliance with AS/NZS 10002:2014 to the extent required by RG 271) with regards to IDR capability would likely cause them to incur set-up and ongoing costs due to increased volumes and, for example, the need to train staff.

185 One other subscriber argued that ASIC's proposal to combine Chapter F and Appendix A appeared to still feature a two-tiered approach that seems to mimic what is already in place rather than making a substantial change in positioning. They noted that Appendix A provides the flexibility needed when Appendix A subscribers are not customer facing and do not necessarily receive direct complaints. They also argued that a change of the regime, given some subscribers were previously not customer facing, will also cause confusion for customers who have become accustomed to a certain process.

186 We didn't receive objections to the idea of updating the terminology relating to lodgement of reports of unauthorised transactions or to the idea of relocating aspects of Chapter F dealing with unauthorised transactions to Chapter C. Some consumer groups voiced support for this proposal but wanted to ensure it would not mean a reduction in rights of consumers who make reports of unauthorised transactions.

187 A number of banking industry respondents queried whether the six-year limitation period for reporting unauthorised transactions was too long—they noted that for some types of transactions (e.g. ATM transactions), producing evidence to support an investigation may be problematic for a subscriber.

ASIC's response

References to RG 165

ASIC will replace references in the Code to RG 165 with RG 271. This reflects the fact that ASIC has since issued RG 271, which will shortly replace RG 165.

For Appendix A subscribers—currently, the Code states that an Appendix A subscriber 'must have IDR procedures that comply with AS ISO 10002-2006 *Customer satisfaction—Guidelines for complaints handling in organizations*, or its successor, to the extent required by RG 165'.

The replacement in the Code with references to RG 271 will mean that AS ISO 10002-2006 will now be replaced by AS/NZ 10002:2014 *Guidelines for complaint management in organizations*.

Combining Chapter F and Appendix A

We will retain the two distinct complaints frameworks that are currently in Chapter F and Appendix A. We will not combine them into a single framework.

While we note the general feedback from respondents that the Code would be more accessible and simpler to understand if we could house all complaints-related obligations within the one chapter, we are not satisfied that our earlier proposal offered any substantial benefit to justify the complexity of implementing the proposal.

EDR scheme membership

We will not require Appendix A subscribers to have EDR scheme membership.

EDR scheme membership is currently not a requirement for Appendix A subscribers. Consumer groups and banking industry subscribers generally supported requiring Appendix A subscribers to have EDR scheme membership but could not point to sufficient benefits to outweigh such a significant change to those subscribers' obligations.

Further, there is the possibility that, should they become EDR scheme members, Appendix A subscribers may become subject to the scheme's dispute resolution process in relation to a wider range of disputes than only those relating to the Code. We have not received sufficient feedback in this regard to justify a change at this time.

Clarification of what amounts to a 'complaint'—unauthorised transactions

We will change references in Chapter F from 'complaints' about unauthorised transactions to 'reports' (or similar) of an unauthorised transaction. We think there is the potential for confusion in the current wording between 'reports' of unauthorised transactions and 'complaints' about how a subscriber has dealt with a report of an unauthorised transaction.

We will relocate to Chapter C of the Code aspects of Chapter F that deal with investigation of unauthorised transactions so that all aspects of the unauthorised transactions investigation process are housed within Chapter C of the Code. It is not our intention that this should reduce any consumer protections—rather, it is aimed at enhancing readability of the Code. It will mean that Chapter C contains all relevant detail about the unauthorised transactions investigation process.

We will retain the six-year limitation period for reporting unauthorised transactions. We do not see justification in reducing the limitation period for reporting unauthorised transactions. Subscribers' inability to retain evidence to support investigations does not, in our view, outweigh the potential consumer detriment in reducing the limitation period.

H Facility expiry dates

Key points

We received broad stakeholder support for our proposal to align the expiry date requirements for certain facilities under the Code with the expiry period in the Australian Consumer Law (i.e. 36 months), while clarifying that these requirements do not apply to debit and credit cards.

We will implement this proposal.

Proposal H1: Aligning requirements with the Australian Consumer Law

188 In CP 341, we proposed to align the expiry date requirements in the Code for certain types of facilities (see clauses 4.8, 18.1 and 18.2) with requirements under the Australian Consumer Law (i.e. 36 months): see proposal H1.

> Note: The Australian Consumer Law is set out in Sch 2 to the *Competition and Consumer Act 2010*.

189 We noted that, 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.

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

Feedback received

191 Respondents were generally supportive of our proposal. Consumer groups commented that the proposal improves the consistency of how expiry dates for certain facilities are regulated.

192 Respondents from the banking industry suggested that the expiry date requirements in the Code should be clarified as not applying to credit and debit cards (which have their own separate expiry dates). They noted that reloadable scheme cards should not be subject to this carve-out, though.

193 Expiry date requirements in the Code generally relate to gift cards that are designed to be spent as soon as possible (being facilities for which loss of funds due to reaching the expiry date is acute and consumers need to understand what will happen to their funds). Industry also noted that, for reloadable scheme cards, the card expiry date generally aligns with the facility expiry date.

194 One banking industry respondent noted that their no-objection position to our proposal assumed the definition of 'facility' in the Code would not be expanded or changed, and that the proposal merely aligned the requirements and scope for gift card products with the Australian Consumer Law.

195 This respondent noted that the expiry period under the Australian Consumer Law applies only to gift cards supplied in trade or commerce, whereas the expiry period in the Code applies more broadly, and that this distinction might be relevant where subscribers provide facilities to consumers on behalf of certain types of third parties.

196 Similarly, one consumer representative and a subscriber noted that not all facilities subject to the Code have a mandatory 36-month expiry period required by law. Therefore, applying such a period will be inconsistent with the legal requirements for those facilities.

ASIC's response

ASIC will implement the proposal with a clarification that the expiry date requirements in the Code do not apply to credit cards or debit cards that relate to a deposit product.

This change will be implemented by inserting the following note under clauses 4.8, 18.1 and 18.2:

> Note: Facility expiry dates must comply with the expiry date requirements, as applicable, in the Australian Consumer Law.

The wording 'as applicable' is intended to acknowledge that not all facilities under the Code will have a mandatory 36-month expiry period under the Australian Consumer Law.

We consider our proposal is consistent with feedback we have received from respondents and is generally supported.

We agree that the protections in the Code were not designed to apply to credit cards or debit cards that relate to a deposit product and that reloadable cards should remain subject to the Code's expiry date requirements.

Unlike credit card and debit card accounts for a deposit product, the funds on reloadable cards may have an expiry or forfeit date under the terms of those facilities.

I Transition and commencement

Key points

Based on the submissions received, we will provide a 12-month transition period for the updated Code.

However, we encourage subscribers to comply with the updated Code earlier, if possible.

Proposal I1: Transition period

197 In CP 341 we stated our intention to apply an appropriate transition period for commencement of updates to the Code: see proposal I1. We asked for feedback from industry on an appropriate timeframe.

Feedback received

198 Consumer groups generally favoured a relatively short transition period of no more than six months, noting that the Code is outdated and compliance with an updated Code needs to commence so that consumers can benefit from the changes as early as possible.

199 Respondents from the banking industry generally indicated that a longer transition period would be necessary. While some changes could be accommodated within six to twelve months (e.g. the on-screen warning), other changes would require significantly longer. For example, some subscribers indicated that they would need around 18 months to implement changes to allow for partial returns of funds for mistaken internet payments.

200 Industry respondents also noted that changes requiring updates to terms and conditions may require up to nine months. Estimates were based the need to alter or introduce processes and systems, and in some instances the need to make significant changes to different parts of the business, and also current compliance schedules and workloads.

201 We observed little consistency in what individual institutions submitted as reasonable timeframes in their individual circumstances. Overall, it appeared to be the *general* industry consensus that, for a range of updates, a period of six months may be possible but, for certain updates, 12–18 months would be an appropriate transition period. Industry respondents noted that the burden of implementation would be felt significantly by smaller institutions.

ASIC's response

ASIC will apply a 12-month transition period to the updated Code.

We note consumer groups' feedback that the transition needs to be as brief as possible so that consumers can enjoy the updated protections in the Code.

However, we also appreciate the need for industry to have a sufficient period of time to implement necessary changes to accommodate the updated provisions. We also acknowledge that industry is presently having to accommodate a significant volume of regulatory changes across various fields. We want to strike a reasonable balance between these competing considerations.

We note that the move from the EFT Code to the current Code involved an 18-month transition period. There was no transition period for subsequent changes to the Code in 2011, 2012 and 2016 as the changes were minor or reflected banking reforms.

> Note: For more information on previous changes to the Code, see Modifications to the ePayments Code.

Code subscribers may choose to implement some changes earlier than 12 months, while taking up to 12 months for more significant changes.

J Other issues

Key points

We will update the privacy guidelines in the Code to replace the reference to the National Privacy Principles with the Australian Privacy Principles.

We will not increase the low-value facility threshold in the Code.

Privacy guidelines

202 After publication of CP 341, we considered whether the privacy guidelines in clause 22 of the Code should be updated to ensure continued relevance and consistency with the current state of the law (e.g. Privacy Act).

203 Clause 22 of the Code sets out rules to assist subscribers in ensuring they comply with the National Privacy Principles when undertaking certain Code related activities. Examples of such compliance include informing consumers when the subscriber is using surveillance mechanisms such as recording devices and ensuring that no equipment or system the subscriber operates can give personal information about a consumer to a person who is not authorised to access that information.

204 The National Privacy Principles have since been replaced with the Australian Privacy Principles.

Feedback received

205 We did not receive significant stakeholder feedback on this topic. While some respondents supported having some guidance in the Code on privacy considerations relating specifically to electronic payment-related scenarios, others queried why the Code should contain such guidance.

206 Some respondents highlighted a risk in divergence between the Code's guidance and privacy law, while some noted potential inconsistencies between the guidelines and the current privacy law. Other respondents observed that a Government review of the Privacy Act is currently underway, and it would be preferable to await the outcome of that review.

ASIC's response

ASIC will not update the Code's current privacy guidelines, except to replace the reference to the National Privacy Principles with the Australian Privacy Principles.

Low-value facility threshold

207 The Code contains tailored and more limited requirements for low-value facilities that can hold a balance of no more than $500 at any one time, on the basis that these facilities are low-risk and do not justify more onerous regulation.

208 The tailored regime for low-value facilities applies to Code requirements for:

(a) providing information or disclosure to the consumer;

(b) notifying the consumer of changes to terms and conditions;

(c) providing transaction receipts and statements; and

(d) complying with the unauthorised transactions provisions (the unauthorised transactions provisions do not apply to low-value facilities).

209 During our review, we considered whether the threshold for facilities that meet the definition of 'gift facility' in *ASIC Corporations (Non-cash Payment Facilities) Instrument 2016/211* (ASIC Instrument 2016/211) should be increased to $1,000. ASIC Instrument 2016/211 provides licensing and disclosure relief for low-value non-cash payment facilities. The Code's low-value threshold would remain at $500 for other low-value facilities such as debit cards attached to deposit products.

210 'Gift facility' is defined in ASIC Instrument 2016/211 to capture features such as a pre-set (i.e. time of issue) and non-adjustable monetary value, limitations on the ability to redeem the value in cash, requirements that the facility be promoted as a gift product, rules around expiry dates and the inability for the facility to form part of another financial product. These are the hallmarks of facilities commonly marketed as gifts (rather than as continuous every-day transactional facilities).

Feedback received

211 We received only one submission to CP 341 suggesting an increase in the threshold. Some respondents expressed a view that $1,000 remains a significant amount for some consumers. The submission suggesting an increase expressed concern that the Code's low-value monetary threshold is inconsistent with the threshold in ASIC Instrument 2016/211.

212 This submission observed that there is no, or very limited, consumer benefit in applying the Code to high-value gift cards or pre-paid cards under $1,000 on the basis that they are typically simple products, do not present material risks to the average consumer and are unlike banking products.

213 The submission noted that the limited risks that exist are already managed by general conduct obligations that apply to all financial products under Div 2 of Pt 2 of the *Australian Securities and Investments Commission Act 2001* and that any consumer benefit would be outweighed by the commercial cost of complying with the Code.

214 The submission queried how issuers of existing high-value gift cards could continue to offer these products should the Code be mandated, if the limit for the tailored regime stays at $500. One difficulty is that, for some facilities, the user or holder is not identifiable and this can make it difficult for a subscriber to meet certain obligations under the Code (e.g. investigations for unauthorised transactions provisions or certain types of disclosure).

215 Some respondents from the financial technology industry queried whether the additional complexity in the Code resulting from separate low-value requirements continues to be useful. They noted that, in practice, most gift cards and similar facilities allow balances above $500, so all products will need to meet all relevant Code requirements.

216 One respondent suggested that it may be more relevant to distinguish products where there is an ongoing account relationship with a consumer from products where there is not such a relationship (e.g. gift facilities).

ASIC's response

ASIC will not increase the threshold in the Code for tailored requirements for low-value facilities from $500 to $1,000.

While we acknowledge feedback on the value of the Code's protections for high-value gift cards or prepaid cards under $1,000, we think there is a risk that the increase could cover reloadable cards issued by ADIs that consumers, in practice, may treat like debit/transaction cards for a deposit product.

Given that the protections in Chapter C of the Code for unauthorised transactions do not apply to low-value facilities and that amounts between $500 and $1,000 can be significant amounts for some consumers, we consider the absence of these protections in particular poses a significant risk for consumers.

In the absence of further feedback pointing to significant justification for an increase of the low-value threshold, we are not satisfied that an increase can be justified at this time.

We are not satisfied that there is justification to remove the tailored requirements for low-value facilities in the Code. We understand that a market for facilities of less than $500 remains and we consider the value in allowing for a tailored low-value regime outweighs any regulatory burden.

Appendix: List of non-confidential respondents

Submissions to CP 310	• 86 400 Limited • Australian Competition and Consumer Commission • Australian Financial Complaints Authority • Australian Payments Network • Australian Retail Credit Association • American Express Australia • Consumers' Federation of Australia • Customer Owned Banking Association • eftpos Payments Australia Limited • FinTech Australia • illion • National Australia Bank • NPP Australia Limited • PayPal Australia Pty Limited • Peter Maganiotis • Raiz Invest Limited • Westpac Group
Submissions to CP 341	• Australian Banking Association • Australian Small Business and Family Enterprise Ombudsman • Australian Payments Network • Consumer Credit Legal Service (WA) • Consumers' Federation of Australia • Customer Owned Banking Association • Department of Mines, Industry Regulation and Safety • eftsure • illion • Indue • Legal Aid NSW • Legal Aid QLD • WEstjustice • Westpac Group