CONSULTATION PAPER 310

Review of the ePayments Code: Scope of the review

March 2019

About this paper

This consultation paper is the first of two papers ASIC plans to issue in 2019 on our review of the ePayments Code.

This paper seeks feedback from stakeholders on the topics we propose to consider as part of our review.

We anticipate engaging further with stakeholders to help us develop more detailed proposals for a second, more substantive, consultation paper later in 2019.

About ASIC regulatory documents

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

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

Regulatory guides: give guidance to regulated entities by:

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

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

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

Document history

This paper was issued on 6 March 2019 and is based on the ePayments Code as at that date.

Disclaimer

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

Contents

The consultation process

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

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

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

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

Where possible, we are seeking both quantitative and qualitative information.

We are also keen to hear from you on any other issues you consider important.

Your comments will help us develop appropriate parameters for ASIC's review of the ePayments Code. In particular, any information about compliance costs, impacts on competition and other impacts, costs and benefits will be taken into account if we prepare a Regulation Impact Statement: see Section C , 'Regulatory and financial impact'.

Making a submission

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

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

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

Comments should be sent by **Friday 5 April 2019** to:

ePaymentsCode@asic.gov.au

What will happen next?

Stage 1	6 March 2019	First consultation paper released
Stage 2	5 April 2019	Comments due on first consultation paper, with targeted stakeholder discussions in April–May to address any issues in submissions, if needed
Stage 3	July 2019	Roundtable stakeholder discussions to seek informal feedback on ASIC's proposed amendments to the Code
Stage 4	August 2019	Second consultation paper released, seeking stakeholder feedback on ASIC's proposals for amendments to the Code
Stage 5	September 2019	Comments due on second consultation paper
Stage 6	October–November 2019	Report on submissions released, with details of final amendments to the Code
Stage 7	December 2019–January 2020	Amended ePayments Code released

A Background to our review

Key points

The ePayments Code (Code) contains important consumer protections that complement other regulatory requirements such as financial services and consumer credit licensing, advice, training and disclosure obligations.

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

This consultation paper seeks feedback on the topics we propose to include in the scope of our review. A second, more substantive consultation paper will be issued later in 2019, setting out our proposed modifications to the Code.

About the ePayments Code

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

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

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

4 Key protections in the Code include:

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

(b) security safeguards relating to what types of identifying information can be included on customers' payment transaction receipts;

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

(d) procedures for customers to seek a return of their money if they have mistakenly electronically transferred it to the wrong recipient; and

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

5 The Code's requirements apply to any subscribing entity, including entities that are not already subject to the financial services and consumer credit regulatory regimes. These requirements are part of the terms and conditions between the customer and their subscribing financial institution.

6 As such, any breach of the Code is a breach of the subscriber's contract with their customer. In some cases, it may also be a breach of ASIC-administered legislation. For example, if a subscriber misrepresents customers' rights under the Code, this may be a breach of the prohibition against engaging in misleading or deceptive conduct in s12DA of the ASIC Act.

ASIC's review of the Code

7 While other industry codes of conduct are typically administered by an independent monitoring body appointed by the relevant industry, ASIC is responsible for administering and regularly reviewing the Code. This is because it covers a potentially broad and not necessarily homogenous industry, including a range of different industry peak bodies.

8 ASIC is required to review the Code every five years. Our most recent comprehensive review was completed in December 2010 (2010 review), although we have made some minor amendments to the Code since that time.

9 Our current review aims to assess the Code's fitness for purpose. There have been significant developments in financial technological innovation and customer uptake of digital technologies since our previous review.

10 We seek to ensure that:

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

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

Note: For further background on the development and governance of the Code, including the timing of this review, see the appendix in this paper.

B Proposed scope of our review

Key points

Since our previous comprehensive review of the ePayments Code, there have been significant developments in the payments environment, which have implications for the ongoing effectiveness and relevance of the Code's provisions.

In this review, we propose to focus on:

- future proofing the Code (see paragraphs 16–38);
- complaints handling (see paragraphs 39–46);
- unauthorised transactions (see paragraphs 47–70);
- data reporting (see paragraphs 71–86);
- mistaken internet payments (see paragraphs 87–103);
- small business access to Code provisions (see paragraphs 104–108); and
- other aspects of the Code that may need updating (see paragraphs 109–124).

Our review is an interim measure before any implementation of the Financial System Inquiry (FSI) recommendation to mandate the Code.

Limitations on scope

11 Our review—and any amendments resulting from it—is an interim measure while the Government undertakes further work to determine how best to implement the recommendation in the final report of the Financial System Inquiry (FSI) in 2014 to mandate the Code: see FSI final report, recommendation 16.

> Note: For details of this recommendation, see paragraphs 132–133 in the appendix to this paper.

12 We consider that it is beyond the scope of this review to:

(a) convert the ePayments Code to a mandatory code of practice or to introduce a legislative foundation for the Code; or

(b) change the key aspects of the Code in a way that significantly changes the entities to whom the Code is relevant (i.e. the subscriber base).

13 ASIC does not have a power to make the Code mandatory. Making the Code mandatory could require further changes, such as revising the provisions to make them more relevant to entities that are not authorised deposit-taking institutions (ADIs) and including provisions on compliance monitoring and enforcement of the Code.

14 Many provisions in the current Code (e.g. for mistaken internet payments and allocating liability for unauthorised transactions) are relevant primarily to ADI subscribers. Also, because the Code is not contained in legislation, being a contractual relationship between subscribers and their customers, it does not include any provisions for ASIC's enforcement of the Code's obligations.

15 These issues may need to be considered in detail when recommendation 16 of the FSI final report is implemented.

Future proofing the Code

Developments in payments in Australia

16 Since our 2010 review, many new technologies and innovative ideas have emerged to facilitate electronic payments by customers and improve cardholder and accountholder verification methods.

17 These developments include mobile banking, digital wallets, the New Payments Platform (which is new infrastructure in Australia used to process fast payments), contactless payment technology, two-factor authentication, tokenisation and biometrics as an alternative to the use of passcodes or PINs. With the emergence of these new payment options, we are seeing changes in the ways customers choose to carry out payment transactions.

18 Some examples include the following:

(a) *Increasing use of debit and credit cards*—In its 2018 annual report, the Payments System Board, which is responsible for the payments system policy of the Reserve Bank of Australia (RBA), noted that in 2017–18, Australians made on average 480 electronic transactions per person (compared with an average of 215 transactions per person ten years earlier). Debit and credit cards combined were the most frequently used payment method in Australia with domestic personal and business cardholders making around 8.7 billion card payments worth $591 billion (an increase of around 13% for credit cards and 7% for debit cards from the previous year).

Note: Data on credit and charge cards published by the RBA shows a gradual decline in the number of these accounts from January 2018 to December 2018. While data on debit cards shows a reduction in the number of accounts when comparing figures for January 2018 and December 2018, the number and value of purchases using debit cards had increased for these months. For links to these statistics, see RBA, Payments data.

(b) *Declining use of cash and cheques*—There has been a corresponding decline in the use of cash and cheques. For example, the RBA has observed a sharp decline in the number and value of cash withdrawals from ATMs. A decade ago, Australians went to the ATM on average about 40 times a year, but today we go to an ATM about 25 times a year and the downward

trend is likely to continue. There has also been a significant reduction in lower-value payments made using cash, facilitated by contactless 'tap-and-go' used by consumers and merchants at the point of sale. In the mid-1990s, Australians made, on average, 45 cheque payments a year per person, whereas today we make about three per person.

(c) *Rapid adoption of contactless payments*—The RBA has also observed that new payment technologies continue to be developed, which will encourage the shift to electronic payments, and that the rapid adoption of contactless payments in Australia shows that Australian customers change how they pay quite quickly when new functionality is offered. For example, the number of transactions through the New Payments Platform is steadily increasing.

Note: For more information on these statistics and observations, see RBA, Payments System Board, Annual report 2018, pp. 23 and 27. See also speech by RBA Governor Philip Lowe, 'A journey towards a near cashless payments system', 2018 Australian Payment Summit, Sydney, 26 November 2018.

19 The New Payments Platform, which has been gradually rolling out since early 2018, facilitates real-time, data-rich payments between accounts at participating financial institutions with the use of a unique identifier—a 'PayID' (such as a mobile telephone number)—in place of bank/state/branch (BSB) and account numbers. This platform is set up to allow for the design of innovative 'overlay services' (i.e. tailored payments services or processes that make use of its infrastructure to offer unique customer experiences).

20 New technologies have to an extent involved a change in the features that we would typically see in the technologies that existed when the Code was initially drafted. The introduction of the New Payments Platform also presents new, but manageable, challenges for financial institutions in identifying and blocking unauthorised transactions.

21 Mobile payment technologies generally do not require the presence of a physical card (e.g. credit or debit card) or the existence, visibility or entering of an 'identifier' (such as an account number, serial number or credit/debit card number). With increased use of mobile payments and mobile banking technology, customers also often have the option of authenticating their identity or transactions biometrically.

22 Biometric authentication, in the context of electronic payments, involves using the unique biological features of an individual to confirm that they are the authorised user of a facility (e.g. when making a payment or securely logging into their account). Examples include (but are not limited to) fingerprints, voice and facial recognition. We note that there may also be a role in the future for *behavioural* biometrics, by which patterns in a person's actions (as opposed to their physical characteristics) could be measured to produce outcomes. The design and functionality of these technologies were not anticipated when the Code was drafted.

23 There has also been a shift in the way many merchants issue transaction receipts to their customers. Previously, a paper receipt would be issued for any payment transaction (whether made by cash or electronically). Many merchants now issue recepts via email or mobile phone text message.

Proposal

B1 We propose to assess whether the Code, as currently worded, has successfully adapted to today's payments environment and is sufficiently adaptable to respond to emerging and future developments in financial technological innovation and changing customer behaviours.

Your feedback

B1Q1 Are you aware of any specific examples where the Code is not adequately catering for these things?

B1Q2 How could our assessment of these things be done in a simple and consumer-focused way?

Rationale

24 It has become increasingly evident that aspects of the Code may not be sufficiently adaptable to respond to recent and future developments in electronic payments. This is demonstrated by the examples set out below.

25 Given the rapid nature of technological developments in the payments market, and that we cannot always anticipate what developments might emerge and how they may or may not fit neatly within the Code's provisions, it is unlikely that completely future proofing the Code will be possible. ASIC's role in regularly reviewing the Code will be important in this regard.

New Payments Platform

26 The Code contains a framework for customers to report 'mistaken internet payments' to their financial institution. Such payments occur where a customer transfers money through an internet banking facility to the wrong recipient due to the customer mistakenly entering the wrong BSB and/or account number. The Code requires the customer's financial institution to contact the mistaken recipient's financial institution about returning the payment.

27 The Code also contains a framework for customers to get assistance from their financial institution in switching to a different bank, credit union or building society by asking their institution to provide a 'listing service', which is a list of all the customer's direct debit/credit arrangements and periodical payments, and other information, over a specified period.

28 However, the commitments in the Code that set out these frameworks refer to payments processed through 'direct entry'. Direct entry means a direct debit or direct credit as defined in the Bulk Electronic Clearing System (BECS) Procedures, administered by the Australian Payments Network (AusPayNet), which is facilitated by entering BSB and account numbers for the payment recipient.

29 The New Payments Platform is not based on the BECS Procedures, which require a BSB and account number; instead, customers can transfer money by using a recipient's 'PayID'. The New Payments Platform is governed by its own rules and regulatory framework administered by NPP Australia Limited.

30 We understand that the regulatory framework for the New Payments Platform has comparable protections to the Code's frameworks for mistaken payments and switching to a different provider. However, we note that the current version of the Code has not been able to adapt to the New Payments Platform and consider that it will not be adaptable, as currently worded, to any other future payment platforms that may emerge.

Mobile and other non-device-based payments

31 The Code does not anticipate electronic payments made without the presence of a physical 'device' (e.g. an ATM card, debit/credit card, token that generates a pass code, or contactless device that has been supplied to the customer by their financial institution) or an 'identifier' (e.g. a bank account number or a credit/debit card number). These concepts (i.e. 'device' and 'identifier') form the basis of several provisions in the Code.

32 However, some electronic payment transactions no longer require the presence of a physical device or identifier. For example, with applications downloaded onto a customer's mobile telephone, tablet or wrist watch, there is no clearly identifiable physical device that the financial institution has given to the customer. If customers store their card details on a website or in a mobile application, they do not need the physical device for future transactions using that website or application. An 'identifier' is also not present in tokenisation (which is the substitution of an identifier with a 'token' to add a layer of security to a payment transaction).

Biometric authentication

33 The Code does not address the use of biometric authentication methods.

34 Under the current requirements, a customer must not voluntarily disclose their 'pass code' to anyone, including a family member or friend. A pass code is a password or code that the customer must keep secret and is used to authenticate a transaction or customer, such as a personal identification number (PIN), internet banking password or code generated by a security

token. The customer also generally must not keep a record of their pass code. If a customer breaches these pass code security requirements, they may be liable for any subsequent unauthorised transactions on their account.

35 The concepts of 'pass code' and the 'recording' of pass codes assume that a customer will have an alphabetical and or numerical password. These security requirements cannot practically be applied if the customer has verified their identity or authenticated a transaction using biometrics (e.g. a fingerprint or voice recognition). This is because a customer cannot practicably keep their relevant biological characteristics secret.

36 Warnings to customers about the importance of pass code security requirements as required under the Code have little relevance where biometric authentication methods are used instead of traditional pass codes. We are also aware of findings in other jurisdictions about the ineffectiveness of risk warnings in influencing consumer behaviour in other contexts that raise questions about whether the warnings in fact achieve their intended purpose.

> Note: See Dutch Authority for Financial Markets (AFM) *Caution! Borrowing money costs money—A study of the effectiveness of a warning in credit advertisements*, December 2016 (PDF, 1 MB); Financial Conduct Authority (UK), Occasional Paper No. 40 *Time to act: A field experiment on overdraft alerts*, July 2018 and Occasional Paper No. 47 *Blackbird's alarm call or nightingale's lullaby? The effect of tweet risk warnings on attractiveness, search, and understanding*, December 2018.

Transaction receipts

37 The Code requires subscribers generally to take reasonable steps to offer customers a receipt for payment transactions at the time of a transaction. The receipt must include information about the transaction such as the monetary amount, the date of the transaction, transaction type, an indication of the facility being debited or credited, and information to allow the subscriber to identify the customer and the transaction. It must not include information that would increase the risk of unauthorised transactions on the customer's account, such as a complete identifier (e.g. a card number) or expiry date for a device (e.g. a card expiry date).

38 These restrictions on receipt content only apply to *paper* receipts. They do not apply to receipts sent electronically (e.g. by email or text message to a mobile phone or receipts made available through the retailer's website). Because emails and text messages are generally not secure methods of communication, it is important that sensitive information be omitted from all forms of receipts, whether electronic or in paper form.

Complaints handling

39 Chapter F of the Code requires most subscribers to maintain:

(a) internal dispute resolution (IDR) procedures that comply with Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165); and

(b) membership with an external dispute resolution (EDR) scheme, which is now the Australian Financial Complaints Authority (AFCA).

40 A tailored regime in Appendix A of the Code applies to all other subscribers. This includes a subscriber who is:

(a) an 'unlicensed product issuer' (defined in RG 165 as an issuer of a financial product that is not an AFS licensee);

(b) an 'unlicensed secondary seller' (defined in RG 165 as a person who offers the secondary sale of a financial product under s1012C(5), (6) or (8) of the Corporations Act and who is not an AFS licensee); and

(c) a credit licensee or credit representative.

41 The key difference between the two regimes is that subscribers who are subject to Chapter F must have IDR procedures that comply with RG 165, while subscribers that are subject to Appendix A do not.

42 However, Appendix A of the Code includes several provisions designed to address this issue (e.g. subscribers must explain the procedure for making complaints in the terms and conditions of their payment facilities, in their general documentation and on request).

Proposal

B2 We propose to assess the clarity and appropriateness of the current policy positions in the Code's complaints handling provisions.

Your feedback

B2Q1 Is there justification for maintaining two complaints handling regimes in the Code (i.e. Chapter F and Appendix A)?

B2Q2 Would there be any benefits in more closely aligning the complaints handling provisions in the Code with RG 165?

Rationale

43 Most current subscribers to the Code are ADIs, who are AFS licensees and credit licensees and already subject to the requirements in RG 165. On this basis, it seems sensible to have a single complaints handling regime in the Code that is aligned as closely as possible with the requirements in RG 165.

44 We do not see a clear justification for a tailored regime to apply to some subscribers and a full regime to others. A consistent approach to complaints handling would give all customers the same access to dispute resolution, regardless of the subscriber they are dealing with.

45 We note that the requirements in RG 165 are scalable—that is, certain principles may apply to a greater or lesser extent depending on the size and nature of the business.

46 We are preparing to undertake a comprehensive review of RG 165 in early 2019 and encourage subscribers to the Code to be involved in that process.

Unauthorised transactions

47 Provisions for allocating liability for losses arising from unauthorised transactions are set out in Chapter C of the Code. These provisions do not apply to transactions performed by the customer (i.e. the account holder), or by anyone else with the knowledge and consent of the customer, including transactions initiated by the customer as a result of falling victim to a scammer or fraudster.

48 Generally, a customer is not liable for losses arising from an unauthorised transaction where the customer has not contributed to the losses. However, the customer may be liable for losses if the subscriber can show that the customer contributed through their actions to the fraud or breached the 'pass code security requirements': see paragraph 34.

49 Subscribers are required by the Code to provide a clear, prominent and self-contained notice to customers summarising the pass code security requirements. This notice must be included with transaction statements at least annually.

'Account aggregators'

50 Over the past decade, ASIC has observed the emergence of financial technology ('fintech') entities, whose operations rely on access to banking customers' transaction data. These fintechs, commonly known as 'account aggregators', can provide a range of services including:

(a) personal financial management tools, which can give consumers a comprehensive view of their financial position and allow them to manage their finances more effectively;

(b) bank statement retrieval/scraping or income and expenses analytics services that help commercial organisations understand prospective clients (e.g. prospective borrowers); and

(c) services that rely on access to consumers' account information to allow functionality beyond 'read only' access (e.g. investment platforms).

Note: See Consultation Paper 20 *Account aggregation in the financial services sector* (CP 20).

51 Account aggregators generally access a customer's bank account by asking the customer to enter their internet banking credentials (i.e. login and password) into a portal of the account aggregator's website, for example. In many cases, the aggregator's access is 'read only', but in some cases, there may be 'write access' (i.e. the aggregator can perform transactions on the customer's account, such as putting customer funds towards financial investments).

Limitation period for lodging complaints

52 There is currently a six-year limitation period during which a subscriber must accept a complaint from a customer: see Chapter F and Appendix A of the Code. This limitation period applies to complaints of all kinds under the Code, including claims relating to unauthorised transactions.

53 If an unauthorised transaction occurs on a credit card or debit card, the relevant rules for the card (e.g. MasterCard, Visa) will include processes—called 'chargeback rights'—that the card issuer can use to claim an equivalent dollar amount for the benefit of the customer who has suffered the loss. This process is an alternative option to the institution having to reimburse the customer under the provisions in Chapter C of the Code.

54 The card's rules generally impose a shorter limitation period (e.g. 120 days) than the six years specified under Code during which a customer may report an unauthorised transaction. If the limitation period has expired under the card's rules for a particular unauthorised transaction, the customer generally still has the right to have the unauthorised transaction considered by their financial institution under the Code if the financial institution is a subscriber.

Proposal

B3 We propose to consider whether the current settings in the Code for unauthorised transactions are appropriate and sufficiently clear.

Your feedback

B3Q1 What are the benefits and challenges of the Code's current settings for unauthorised transactions?

B3Q2 What role, if any, could the Code play in preventing or reducing the risk of customers falling victim to financial scams, or helping customers who have lost money through scams?

Rationale

Practical limitations of the pass code security requirements

55 In practice, the requirement for customers not to record or disclose their pass code may present practical difficulties or limit their ability to access potentially useful third-party services such as 'account aggregators'.

56 Customers will usually have several different logins and passwords or other types of pass codes for accessing various portals such as internet or telephone banking, ATMs, email, work logins, and subscription accounts. They are generally encouraged to use different passwords for each portal, to use passwords that are not readily able to be deciphered and to change them at regular intervals. They are generally discouraged from sharing those passwords or writing them down.

57 People have finite cognitive resources, and there are questions about whether it is feasible for consumers to remember pass codes and reasonable to expect them to. We are anecdotally aware that it is not uncommon for customers to share these details with others or to record them in some form (e.g. by writing them down or using digital 'password managers'). While biometrics present potentially useful solutions to having a large number of logins and passwords, it seems that many portals still require use only of a password, while others that use biometrics still require a password as a back-up.

58 Disclosing internet banking credentials to a third-party service provider such as an account aggregator may be a breach of the pass code security requirements in the Code and, accordingly, a breach of the customer's terms and conditions with their financial institution. This may affect the customer's liability for any subsequent unauthorised transaction on their account.

59 One of the findings of the Review into Open Banking in December 2017 was that, because handing over login credentials goes against the usual security advice to customers about not giving out their passwords, fintechs report that a significant number of potential customers withdraw from the sign-up process when asked to provide these credentials. Despite this, millions of Australian customers have elected to sign up to these businesses as a way to share their banking data to access the services they desire. The review recommended that Open Banking should not prohibit or endorse 'screenscraping' but should aim to make this practice redundant by facilitating a more efficient data transfer mechanism.

> Note: See Treasury, *Review of Open Banking: Giving customers choice, convenience and confidence* (final report), December 2017, p. 72.

60 We anticipate that, even with the commencement of Open Banking, the services of account aggregators may remain relevant for some time and coexist with Open Banking as a potentially valuable tool for consumers and

commercial organisations. This is particularly so, given the planned phased approach for implementing Open Banking with 'read only' access initially.

61 ASIC encourages the development of innovative tools that offer potential benefits to both industry and consumers, while maintaining important consumer protections. Access by customers to their own financial data in an aggregated, easy-to-understand format can help them manage their finances more effectively. Account aggregator services are also attractive to lenders because they can help the lender to obtain reliable data about a prospective borrower's income and expenses and meet their responsible lending obligations under the National Credit Act. For example, some lenders are required by law to consider a consumer's bank account statements for the preceding 90 days, before deciding to provide a loan.

> Note: See s130(1A) of the National Credit Act and Report 426 *Payday lenders and the new small amount lending laws* (REP 426).

62 Fingerprint access to mobile banking on smartphones is a separate concern. Such access is generally linked to the fingerprint(s) registered on the phone. However, a customer who shares access to their phone with family members (e.g. by allowing them to register their own fingerprints on the phone) risks liability for unauthorised transactions on their account. While this issue is not specifically addressed in the Code, we have observed that, under the terms and conditions of some ADIs, a customer must not allow other people to have biometric access to their smartphone if such access is enabled.

63 Given these practical issues, we recognise that there is a need to strike a balance in the Code between:

(a) providing useful outcomes that take into account customer behaviours (noting that the Code is a consumer protection code); and

(b) allowing ADIs to expect reasonable protective behaviours by their customers to guard against financial losses.

Increasing incidence of scams

64 According to the most recent report on scam activity by the Australian Competition and Consumer Commission (ACCC), Australians lost more money to scammers in 2017 than in any other year since the ACCC began reporting on this activity. More than 200,000 scam reports were submitted to the ACCC, the Australian Cybercrime Online Reporting Network and other federal and state-based government agencies in 2017. Total losses reported were $340 million, a $40 million increase compared to 2016. The ACCC also observed that scammers are very sophisticated and hard to identify.

> Note: See ACCC, *Targeting scams: Report of the ACCC on scam activity 2017*, 21 May 2018.

65 We encourage ADIs and other financial institutions to continue to engage and educate customers on cyber safety. However, we think these efforts should be balanced with effective mitigation practices and responses by the institutions to combat such losses, given the growing sophistication of scammers and how difficult it can be for consumers to detect these scams. The Code may be an appropriate mechanism for introducing some consistent minimum standards to achieve this.

66 While we do not consider the risks of unauthorised transactions or the prevalence of scams would increase purely due to implementation of the New Payments Platform, we do note that the window of opportunity to halt a transaction is reduced due to the instantaneous nature of transactions.

Limitation periods under card rules

67 We have observed potential confusion among some ADI subscribers about how the limitation periods under a card's rules coexist with the provisions for unauthorised transactions in Chapter C of the Code (including the six-year limitation period), in cases where a customer reports an unauthorised transaction on a credit card or debit card. We have seen instances where subscribers have initially failed to comply with the Code for unauthorised transactions where the limitation period under card's rules has elapsed.

68 This potential confusion was recently addressed in an ASIC media release where an ADI had incorrectly informed customers who had missed the 120-day limitation period to report an unauthorised transaction on their credit or debit card under the card's rules, that the bank was no longer obliged to investigate the reports. In fact, those customers still had a right to have their reports considered under the Code.

> Note: See Media release 17-376MR *Citibank refunds $1 million following misleading statements made to customers about their rights under the ePayments Code*, 9 November 2017.

69 We have received some stakeholder feedback that the six-year limitation period for the unauthorised transactions regime in Chapter C of the Code should be shortened. A shorter limitation period under the Code may, for example, address the confusion noted above and may also make the task of investigating the circumstances of an unauthorised transaction easier.

70 However, it is also important to recognise the importance of allowing a longer period for customers. Customers need time to discover the problem (i.e. a potential unauthorised transaction) and then to decide whether it is something to raise with their financial institution. The fact that sizeable remediations have been necessary in recent times suggests that many customers do not currently report unauthorised transactions within 120 days.

Data reporting

71 The Code requires every subscriber to report to ASIC annually on the incidence of unauthorised transactions: see clause 44.1.

72 In consultation with stakeholders, we created a data reporting questionnaire to collect data from subscribers on unauthorised transactions made through:

(a) debit or credit cards;

(b) internet or telephone banking; and

(c) cards other than debit or credit cards.

73 In each category, we asked for data on the circumstances of the transaction (e.g. the card was lost or stolen, counterfeit or skimming, fraudulent application, card not present, malware, phishing, ID takeover, phone porting, and system or equipment malfunction) and measured the number of unauthorised transactions against the total number of transactions processed by the subscriber.

74 We also asked for data about the number of complaints the subscriber received about their handling of claims relating to unauthorised transactions.

75 Data on unauthorised transactions was collected using the questionnaire for the 2015, 2016 and 2017 calendar years. In August 2018, we wrote to subscribers informing them of a temporary pause on reporting this data for the 2018 and 2019 calendar years, noting that we intended to assess the continued benefit of this requirement as part of our review of the Code.

76 Based on the data collected in 2015–17, 'card not present' transactions were the most common type of unauthorised transaction, accounting for over 50% of unauthorised transactions in each year. The number and dollar value of unauthorised transactions due to lost or stolen cards increased during this period, although we observed a decline in the average monetary value.

> Note: We intend to provide further details about our findings from this data in the second consultation paper on our review of the Code.

77 After consultation with stakeholders, we also required ADI subscribers to submit data on the incidence of mistaken payments by their customers and the reasons for such mistakes for a one-off three-month period between September and November 2015. This was done through our targeted compliance monitoring under clause 44.2 of the Code.

78 From the data received, we observed that most mistaken payments during this period were caused by the customer entering incorrect account details (83%) compared to 'customer selected wrong payee' (17%). Approximately 74% of the monetary value of mistaken payments reported to ADI subscribers was recovered for the customer.

Proposal

B4 We propose to review the data reporting requirements in the Code and assess the most valuable and efficient approach.

Your feedback

B4Q1 Would it be helpful (for consumers or subscribers or both) for ASIC to collect and publish data about particular matters under the Code? If so, what matters, and why?

Rationale

79 While ASIC is responsible for administering the Code, we generally cannot enforce compliance by imposing penalties or other sanctions unless a breach of the Code also amounts to a breach of other financial services laws to which such penalty or sanction attaches. The consequences of a breach of a Code are contractual in nature, as between the subscriber and their customer.

80 For that reason, our monitoring activity is mainly focused on gathering information to determine whether the Code's provisions remain effective and to address any identified deficiencies in consultation with subscribers and other key stakeholders. We still monitor compliance with the Code and expect subscribers to fully comply. We also expect any failures in meeting Code provisions to be promptly remediated.

81 In our 2010 review, we noted that the most important information ASIC can collect about Code compliance is regular statistical data about the number and type of unauthorised transactions and how subscribers resolve disputes about unauthorised transactions. We also noted that it may be appropriate to focus on other specific consumer protection issues from time to time.

Note: See Consultation Paper 90 *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC proposals* (CP 90) and Report 218 *Electronic Funds Transfer Code of Conduct review: Feedback on CP 90 and final positions* (REP 218).

82 In Information Sheet 195 *ePayments Code: Reporting data on unauthorised transactions* (INFO 195), we stated that data on unauthorised transactions would help us monitor the incidence of unauthorised transactions and the effectiveness of the Code's provisions for allocating liability.

83 In practice, while the data has been useful in demonstrating the extent of the problem and indicating which types of electronic payment facilities present the greatest risk for unauthorised transactions, it has not informed us about the effectiveness of the Code's provisions for allocating liability. For example, the data does not tell us whether it is appropriate to allocate liability based on the current Code provisions, nor does it tell us whether subscribers are correctly receiving and investigating reports by their customers in individual instances of unauthorised transactions.

84 For many subscribers, particularly smaller ADIs, completing and lodging the data reporting questionnaire is resource intensive and time consuming. We have also observed a lack of consistency in how subscribers categorise individual types of unauthorised transactions in their recording systems.

85 The Australian Payments Network (AusPayNet) publishes aggregated payments fraud statistics, provided by Australia's financial institutions and card schemes, twice a year. While the annual data that ASIC has been collecting covers some categories that AusPayNet's data collection does not (e.g. non-card related fraud such as 'Pay Anyone' internet banking transactions), there is an overlap. There may not be benefit in ASIC collecting data that is routinely collected by industry associations.

> Note: AusPayNet is the industry association and self-regulatory body for the Australian payments industry. According to its website, the purpose of their data collection and reporting is to assist financial institutions in monitoring trends, developing targeted mitigation strategies and informing businesses and consumers about fraud issues.

86 Our one-off data collection in 2015 on the causes of mistaken payments found that most mistaken payments made by customers of ADI subscribers were due to an incorrect BSB and/or account number being entered. While we think the use of PayIDs under the New Payments Platform will help to address this risk, we are inviting feedback on whether there is a role for the Code in setting minimum standards for ADI subscribers to reduce the risk of or prevent these payments: see paragraphs 101–103.

Mistaken internet payments

87 Subscribers to the Code that are ADIs must have an effective and convenient process for users to report mistaken internet payments. If a customer reports a mistaken payment, the 'sending ADI' (i.e. the ADI whose customer made the mistaken payment) must investigate whether such a payment has occurred. If the sending ADI is satisfied that the payment has occurred, it must send the 'receiving ADI' (i.e. the ADI whose customer is the unintended recipient of the payment) a request for the return of the funds.

> Note: See Clauses 26.1 and 27.1 of the Code.

88 Once the sending ADI is satisfied that a mistaken payment has occurred, the subsequent actions of the sending and receiving ADIs and the customer's likelihood of having their funds returned depend on how much time has passed since the payment was made and whether there are sufficient funds in the mistaken recipient's account to cover it.

Proposal

B5 We propose to consider whether the provisions in the Code for mistaken payments are simple and accessible enough, and whether ADI subscribers should have any role in mitigating or preventing such payments.

Your feedback

B5Q1 Is the process for seeking return of mistaken internet payments sufficiently simple for customers?

B5Q2 What other provisions could be included in the Code for ADI subscribers to reduce the risk of or prevent mistaken payments?

B5Q3 To what extent do you think the mistaken payments procedures in the Code will remain relevant as more customers begin using the New Payments Platform?

Rationale

Simplifying the process for mistaken payments

89 The process for reporting and retrieving a mistaken payment is worded in a relatively complex way in the Code and differs depending on the time the customer has taken to report the mistake to their institution. We are anecdotally aware that, in some cases, frontline staff of ADI subscribers may not fully understand the customer's right to see the process through and that it should be free of charge to the customer.

90 Stakeholders have raised several concerns with ASIC about the current settings in the Code for these payments, including the following:

(a) There is no time limit within which a sending ADI must determine that a mistaken payment has been made. This is potentially problematic, as this finding is the trigger for retrieval of the payment (and its associated timeframes) to commence.

(b) The customer who has made the mistaken payment cannot complain to the receiving ADI or lodge a complaint with the EDR scheme about the receiving ADI's conduct. The intended recipient who did not receive the payment cannot seek return of the payment through the sending or receiving ADI or complain through internal or external processes.

(c) It is unclear what information the sending ADI must give the customer about what was done to retrieve a mistaken payment. The customer may benefit from knowing what steps the sending ADI took and how long the process took. This may also make the sending and receiving ADIs more accountable.

91 More generally, we are aware that some stakeholders are keen to ensure that the mistaken payments process is operating in the ways envisaged when the provisions were designed. After our 2010 review, we proposed a mistaken payments regime comprising the five elements set out below.

Preventative measures

92 We noted in REP 218 that on-screen warnings (about the importance of entering the correct BSB and account number and the risks of mistaken payments), when properly designed and strategically placed, will help remind consumers of the risks of mistaken payments and encourage greater care in entering transaction details. We also thought that product terms and conditions should clearly set out the circumstances in which mistaken payments can be recovered.

93 However, since the 2010 review, we have developed a deeper understanding of the limitations on the effectiveness of warnings and disclosure. Our review of the ePayments Code presents us with an opportunity to more closely consider the effect and relative usefulness of risk warnings and disclosure on customers. In December 2018, the Financial Conduct Authority (FCA) in the United Kingdom published findings which suggested that risk warnings might fail to achieve their objectives for many reasons.

Note: See FCA, *Don't look here: Do risk warnings really work?*, 13 December 2018.

Recovery where funds are available in the recipient's account

94 During our 2010 review, ASIC and stakeholders agreed to a three-part process for the recovery of mistaken payments where there are sufficient funds in the recipient's account. The process would depend on the timing of the claim being brought to the financial institution and whether there are sufficient funds in the recipient's account to reimburse the payer. This recognised that the more time that has passed since the payment the less likely the funds will still be in the recipient's account (meaning the funds will be harder to recover). The agreed approach sought to balance both the rights of the payer and the unintended recipient.

95 It was considered that mistaken payments reported within 12 business days are most likely to be retrieved. We agreed on the second category (i.e. mistaken payments reported between 12 business days and seven months) because six months was at the time the longest statement period in the market, and an additional month would give customers time to check their statements. For reports of mistaken payments after seven months, it was agreed that the BECS Procedures for return requests would apply and the consent of the recipient would have to be obtained before funds could be recovered.

Recovery where funds are not available in the recipient's account

96 We considered that, where there are insufficient funds in the recipient's account, the recipient's consent should be obtained to the funds being returned to the payer and the financial institution should make reasonable endeavours to retrieve the funds.

97 During our 2010 review, stakeholder opinion was divided on whether liability in cases where funds cannot be retrieved ought to rest with the payer or the financial institutions who operate a payment system that allows errors to occur by ignoring account name information and not validating BSB numbers in their entirety. The interim position reached was that it would be up to the payer to privately pursue recovery of funds, noting that ASIC would collect data to monitor the incidence of mistaken payments.

Role for EDR schemes

98 We considered it was important that customers can make complaints to the EDR scheme where a financial institution concludes that a mistaken payment has not occurred and the customer is not satisfied with this outcome. This is because a customer who has made a mistaken payment is unlikely to know the identity of the recipient or in many cases the name of the recipient's financial institution.

99 In our view, it was better for the customer to bring the complaint to their own financial institution and that institution's EDR scheme because of their existing relationship with that financial institution. An investigation would be facilitated by the existing privacy agreement and contractual relationship between the customer and the institution.

Administration of mistaken payment arrangements

100 To facilitate the mistaken payments arrangements, our 2010 review concluded that subscribers should have clear and accessible processes for all customers to report mistaken payments, receiving financial institutions should acknowledge a mistaken payment query within a prescribed time period (five business days) and ASIC would collect data about the incidence of mistaken payments for a specific three-month period to help us monitor the effectiveness of the procedures set out in the Code.

Role for ADI subscribers in mitigating or preventing such payments

101 We consider that, with growth over time in registration and use of PayIDs under the New Payments Platform (replacing the need for a BSB and account number to be entered), the instances of mistaken payments are likely to reduce. When a customer makes a transaction using a recipient's PayID, the payee's name is presented to confirm the transaction and the correct recipient. As noted in paragraphs 77–78, we have observed that incorrect entry of the account number is the primary cause for mistaken payments.

102 However, the risk of mistaken payments cannot be removed entirely, even with the New Payments Platform. We understand that the BECS Procedures (under which a BSB and account number must be entered to make a 'Pay Anyone' transfer) will continue to be relevant while this platform is being rolled out and because customers presently do not have to participate in the New Payments Platform.

103 When processing transactions through BECS, the general position of ADIs is that incorrectly entering a BSB and/or account number will result in the funds not reaching the intended recipient, even if the customer has entered the recipient's correct name. While the Code currently requires ADI subscribers to clearly warn customers about the importance of entering the correct identifier and the risk of mistaken payments, there is no express requirement to warn customers that correctly entering the account name will not fix an incorrect BSB or account number (although, in practice, we have observed that many ADIs do warn their customers of this risk).

Small business access to Code provisions

104 The Code does not apply to transactions by customers through facilities that are designed primarily for use by a business and established primarily for business purposes: see clause 2.1.

105 In our 2010 review, we sought feedback in CP 90 about whether the Code's protections should be extended to small business. At the time, there was insufficient support on this issue in the submissions received. In particular, there was insufficient data on the prevalence of electronic banking problems for small business customers.

Proposal

B6 We propose to explore whether it may be appropriate to extend the Code, or at least some of its protections, to small business.

Your feedback

B6Q1 Do you think that all or any parts of the Code should, or could appropriately, apply to small business?

B6Q2 Are you aware of any data that shows the prevalence of electronic banking problems for small business customers?

B6Q3 How might the Code best define 'small business'?

Rationale

106 Some provisions in the Code could potentially be extended to customers that are small businesses, without any apparent significant additional cost to subscribers. For example, the process for retrieving mistaken payments is

not intended to result in a sending or receiving ADI having to reimburse a customer for funds lost through a mistaken payment (rather, if the funds cannot be retrieved, the customer must wear the loss). We are not aware of a significant burden on ADIs if these provisions were to apply to mistaken payments made by small businesses.

107 Other parts of the Code, such as the provisions for allocating liability for unauthorised transactions, would be valuable to small businesses. In REP 218, we noted that supporters of extending the provisions in the Code to small business argued there is little distinction in practice between the banking needs and activities of small business owners and individual customers. Supporters also argued that no modifications would be needed to apply these protections to small business customers, apart from a possible modification of no-fault liability for unauthorised transactions (e.g. one submission suggested that this liability should be capped if small business was covered).

> Note: In November 2016, for similar reasons, the *Treasury Legislation Amendment (Small Business and Unfair Contract Terms) Act 2015* took effect to expand the reach of the unfair contract terms legislation to small business.

108 Most industry submissions did not support extending the Code's provisions to small business, citing difficulties for institutions in monitoring when a small business consumer is no longer a small business (as this would require including a threshold test of what constitutes small business, which was said to be problematic and may increase subscribers' compliance risk). There was also little agreement on an appropriate definition of small business.

Other aspects of the Code that may need updating

109 Other issues could be addressed as part of ASIC's review of the Code in addition to the topics we have outlined in this section.

110 Examples of other issues that may be relevant for our review include:

(a) the Code's approach to low-value facilities;

(b) the introduction by APRA of a restricted ADI framework; and

(c) the effect of recent legislative developments for gift card expiry dates.

Proposal

B7 We propose to consider any other aspects of the Code that may need updating as part of our review.

Your feedback

B7Q1 Are there any other aspects of the Code that should be updated?

Rationale

Low-value facilities

111 Low-value facilities (i.e. facilities with a balance of no more than $500 at any one time) are currently subject to limited requirements under the Code. For example, the requirement for subscribers to provide statements of transactions to holders and the liability provisions for unauthorised transactions do not apply to these facilities.

112 After our 2010 review, we agreed with submissions to CP 90 emphasising a need for a 'light touch' approach to low-risk products with low-value holdings. We considered that less onerous requirements should be available to simple, low-value electronic payment products and that customers using higher-value and more complex products should have the full protections.

113 Respondents who advocated a higher cut-off point of $1,000 cited the need for consistency with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML Act) and AFS licensing exemptions (see *ASIC Corporations (Non-cash Payment Facilities Instrument) 2016/211*).

114 In formulating our proposed parameters in 2010, we reviewed the regulatory treatment of new and innovative electronic payment products in various overseas jurisdictions. We noted, for example, that the United Kingdom and the European Union had adopted approaches allowing regulators to apply a light touch regime to disclosure and liability allocation for low-value facilities.

115 We took the view that, as the monetary limit (i.e. the maximum value that can be held on a certain product at any one time) would be the sole criterion for the limited requirements, this limit should be set at a level that balanced consumer and industry interests.

116 We noted that the threshold of $1,000 in the AML Act was used to determine the types of entities that must comply with obligations to verify customers' identities and report suspicious transactions to the Australian Transaction Reports and Analysis Centre (AUSTRAC). We did not consider those obligations overlapped with the Code requirements or that the two thresholds needed to be identical. We remain of that view.

117 The limited requirements would be available to products with a maximum value of $500 at any one time, capturing many products available at that time, particularly simple products that posed limited risks to consumers. Products holding more than $500 would be subject to the full requirements, as typically they would be more complex, have features similar to banking products and be riskier for the average consumer (in terms of potential for fraud or unauthorised transactions). We considered that $1,000 was a significant amount for the average consumer and users of facilities over $500 should feel confident knowing that they had full protection under the Code.

118 While we noted in our 2010 review that there was a higher limit of $1,000 for our licensing and disclosure relief for AFS licensees for non-cash payment facilities, we considered that a lower limit was appropriate for the Code because its protections were quite different to those covered by our relief and should be provided for a wide range of products.

APRA's restricted ADI framework

119 In May 2018, the Australian Prudential Regulation Authority (APRA) introduced a restricted ADI framework as an alternative route to becoming an ADI. This framework gives eligible applicants a restricted licence for a maximum of two years before they must apply the prudential framework in full, allowing them to conduct limited banking business while developing their capabilities and resources.

Note: See APRA, *ADI licensing: Restricted ADI framework*, 4 May 2018.

120 Start-up businesses pursuing this option may choose, for example, to adopt a payment card as the first product under their restricted ADI licence and market it as a transaction facility, which would be relevant for the Code.

121 We are not aware of any circumstances where it would be appropriate to tailor the Code requirements for holders of a restricted ADI licence. We have not applied a tailored regime for entities using ASIC's 'regulatory sandbox', which is available for eligible fintech businesses to test certain services for a limited period without needing to hold an AFS licence or credit licence.

Gift card expiry dates

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

123 In September 2018, the Assistant Treasurer introduced legislation to create a national regime for the regulation of gift cards, with the intention that the Australian Consumer Law would be amended to require a minimum three-year expiry period on gift cards (with some exceptions) and display of expiry dates, among other things. Most recently, Treasury has undertaken a public consultation on exposure draft regulations to support the Competition and Consumer Amendment (Gift Cards) Bill 2018 (Bill).

124 To the extent that a facility under the Code is a gift card, as defined in the Bill, the 12-month minimum expiry period prescribed in the Code would be inconsistent with the legislative amendments.

C Regulatory and financial impact

125 In developing the proposals in this paper, we have carefully considered their regulatory and financial impact. On the information currently available to us we think they will strike an appropriate balance between ensuring our review of the ePayments Code takes into account important consumer protection needs, while keeping in mind the regulatory burden any amendments to the Code may have on subscribers.

126 Before settling on a final policy, we will comply with the Australian Government's regulatory impact analysis requirements by:

(a) considering all feasible options, including examining the likely impacts of the range of alternative options which could meet our policy objectives;

(b) if regulatory options are under consideration, notifying the Office of Best Practice Regulation (OBPR); and

(c) if our proposed option has more than minor or machinery impact on business or the not-for-profit sector, preparing a Regulation Impact Statement (RIS).

127 All RISs are submitted to the OBPR for approval before we make any final decision. Without an approved RIS, ASIC is unable to give relief or make any other form of regulation, including issuing a regulatory guide that contains regulation.

128 To ensure that we are in a position to properly complete any required RIS, please give us as much information as you can about our proposals or any alternative approaches, including:

(a) the likely compliance costs;

(b) the likely effect on competition; and

(c) other impacts, costs and benefits.

See 'The consultation process', p. 3.

Appendix: Further background

Development and governance of the Code

129 The ePayments Code has been in force since 2011. Its predecessor, the Electronic Funds Transfer Code of Conduct (EFT Code), which came into force in 1989, was initially developed in a climate of community and government concern about how to allocate liability between account holders and their financial institutions in the event of loss or theft of the account holder's transaction card or personal identification number (PIN).

130 On 1 July 1998, after recommendations from the Wallis Financial System Inquiry, ASIC became responsible for administering the EFT Code. A review of the EFT Code in 1999–2001 resulted in considerable expansion to its coverage. In particular, a broader technologically neutral definition of 'EFT transactions' replaced an earlier more limited definition and a new regulatory regime for 'stored value facilities and transactions' was introduced.

131 A further review of the EFT Code was completed in December 2010, after which the ePayments Code replaced the EFT Code: see REP 218.

132 In 2014, the final report of the Financial System Inquiry recommended:

(a) clarifying thresholds for regulation of retail payments by ASIC and APRA;

(b) strengthening consumer protection by mandating the ePayments Code; and

(c) introducing a separate prudential regime with two tiers for purchased payment facilities.

Note: See FSI final report, recommendation 16.

133 The Government supported this recommendation.

Timing of ASIC's review

134 The ePayments Code requires ASIC (or its agent) to commence a review of the Code within five years of the conclusion of each preceding review: see clause 44 of the Code.

135 Several factors have delayed the timing of this review since our previous review of the EFT Code in December 2010, including discussions about the implementation of recommendation 16 of the FSI final report and recommendations from other inquiries and reviews.

136 Although it is yet to be determined how recommendation 16 of the FSI final report will be implemented, work is currently underway by the Council of Financial Regulators (CFR) to review the regulatory framework for stored value facilities and aspects of the regulation of retail payments service providers.

137 In an issues paper exploring options for appropriate levels of consumer protection for retail payments products, the CFR sought stakeholder comments on the role the Code could play: see CFR, *Review of retail payments regulation: Stored-value facilities*, September 2018. Several submissions to the issues paper supported making the Code mandatory.

138 The Productivity Commission, in its recent inquiry into competition in the Australian financial system, recommended that ASIC should:

(a) review and update the Code by end-2019 to:

(i) reflect changes in technology, innovative business models and developments in Open Banking; and

(ii) more clearly define the liability provisions for unauthorised transactions when third parties are involved, including participation in financial dispute resolution schemes; and

(b) commit to three-yearly reviews thereafter: see recommendation 17.6.

139 Although the Government is yet to formally responded to the Productivity Commission's recommendations, ASIC supports these recommendations.

140 In December 2017, the ASIC Enforcement Review Taskforce (Taskforce) recommended that ASIC approval be required for relevant financial sector industry codes: see recommendation 18 of the Taskforce report. The Government agreed to this recommendation in principle but deferred implementation to take into account any findings of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.

141 While the Taskforce noted ASIC's submission that the Code should be differentiated from other codes and mandated through a legislative rule-making power, it considered that the approval regime should also be available for the Code.

Key terms

Term	Meaning in this document
2010 review	ASIC's previous comprehensive review of the EFT Code, which was completed in 2010
ACCC	Australian Competition and Consumer Commission
ADI	Authorised deposit taking institution
ADI subscriber	A subscriber to the Code that is an ADI
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ASIC Act	*Australian Securities and Investments Commission Act 2001*
ATM	Automatic teller machine
AusPayNet	The Australian Payments Network, which administers the BECS Procedures
BECS	Bulk Electronic Clearing System
BSB	The number that identifies the bank/state/branch for an account
CFR	Council of Financial Regulators
Code	The ePayments Code, a voluntary code of practice that regulates electronic payments in Australia, including ATM transactions, online payments, BPAY, EFTPOS transactions, credit/debit card transactions (e.g. through contactless and wearable technologies and other emerging payment methods linked to debit and credit cards) and internet and mobile banking
EFT Code	The Electronic Funds Transfer Code of Conduct, which came into force in 1989 and was replaced by the ePayments Code in 2011
FCA	Financial Conduct Authority (UK)
FSI final report	The final report of the 2014 Financial System Inquiry
mistaken internet payment	A payment where a customer transfers money through an internet banking facility to the wrong recipient due to the customer mistakenly entering the wrong BSB and/or account number
mistaken payment	See 'mistaken internet payment'
National Credit Act	*National Consumer Credit Protection Act 2009*

Term	Meaning in this document
National Credit Code	National Credit Code at Sch 1 to the National Credit Act
New Payments Platform	A platform administered by NPP Australia Limited that facilitates real-time, data-rich payments between accounts at participating financial institutions with the use of a 'PayID;
OBPR	Office of Best Practice Regulation
PayID	A unique identifier (such as a mobile telephone number) used by the New Payments Platform in place of BSB and account numbers for the purposes of electronic payments
PIN	Personal identification number
REP 218 (for example)	An ASIC report (in this example numbered 218)
RIS	Regulatory impact statement
s130(1A) (for example)	A section of the National Credit Act (in this example numbered s130(1A))
subscriber	A subscriber to the Code
Taskforce	ASIC Enforcement Review Taskforce

List of proposals and questions

Proposal		Your feedback	
B1	We propose to assess whether the Code, as currently worded, has successfully adapted to today's payments environment and is sufficiently adaptable to respond to emerging and future developments in financial technological innovation and changing customer behaviours.	B1Q1	Are you aware of any specific examples where the Code is not adequately catering for these things?
		B1Q2	How could our assessment of these things be done in a simple and consumer-focused way?
B2	We propose to assess the clarity and appropriateness of the current policy positions in the Code's complaints handling provisions.	B2Q1	Is there justification for maintaining two complaints handling regimes in the Code (i.e. Chapter F and Appendix A)?
		B2Q2	Would there be any benefits in more closely aligning the complaints handling provisions in the Code with RG 165?
B3	We propose to consider whether the current settings in the Code for unauthorised transactions are appropriate and sufficiently clear.	B3Q1	What are the benefits and challenges of the Code's current settings for unauthorised transactions?
		B3Q2	What role, if any, could the Code play in preventing or reducing the risk of customers falling victim to financial scams, or helping customers who have lost money through scams?
B4	We propose to review the data reporting requirements in the Code and assess the most valuable and efficient approach.	B4Q1	Would it be helpful (for consumers or subscribers or both) for ASIC to collect and publish data about particular matters under the Code? If so, what matters, and why?
B5	We propose to consider whether the provisions in the Code for mistaken payments are simple and accessible enough, and whether ADI subscribers should have any role in mitigating or preventing such payments.	B5Q1	Is the process for seeking return of mistaken internet payments sufficiently simple for customers?
		B5Q2	What other provisions could be included in the Code for ADI subscribers to reduce the risk of or prevent mistaken payments?
		B5Q3	To what extent do you think the mistaken payments procedures in the Code will remain relevant as more customers begin using the New Payments Platform?
B6	We propose to explore whether it may be appropriate to extend the Code, or at least some of its protections, to small business.	B6Q1	Do you think that all or any parts of the Code should, or could appropriately, apply to small business?
		B6Q2	Are you aware of any data that shows the prevalence of electronic banking problems for small business customers?
		B6Q3	How might the Code best define 'small business'?
B7	We propose to consider any other aspects of the Code that may need updating as part of our review.	B7Q1	Are there any other aspects of the Code that should be updated?