ASIC
Australian Securities & Investments Commission

REPORT 218

Electronic Funds Transfer Code of Conduct review: Feedback on CP 90 and final positions

December 2010

About this report

This report details the final outcomes of the Electronic Funds Transfer Code of Conduct (EFT Code) review. It follows on from Consultation Paper 90 *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC proposals* (CP 90) and subsequent working group meetings.

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 applicable laws apply to you, as it is your responsibility to determine your obligations.

Contents

Executive summary

1 This report summarises ASIC's final positions on the review of the Electronic Funds Transfer Code of Conduct (EFT Code). The review aims to revise the Code to deal with recent consumer issues and developments in the electronic payment industry. Our positions are guided by the submissions we received to our two consultation papers—Consultation Paper 78 *Reviewing the EFT Code* (CP 78) and Consultation Paper 90 *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC proposals* (CP 90)—as well as the information and assistance provided by our working group members. In many instances we have had to make a judgement about the appropriate balance between competing stakeholder interests.

2 A number of significant changes will be made to the EFT Code as a result of this review. The Code will adopt a one-part structure with lighter requirements for low value electronic transactions. The coverage of the Code will be clarified to include all transactions initiated electronically. The Code will be redrafted in plain English and adopt a principles-based approach as far as possible.

3 The revised Code will deal with the issue of mistaken internet payments and include procedures for recovering funds mistakenly paid to a third party. The positions reached on mistaken payments were based on a compromise that includes industry collecting data on mistaken internet payments, assisted by the Australian Payments Clearing Association (APCA) and external dispute resolution (EDR) schemes. The data will enable us to assess the extent of mistaken payments in the online banking market and the effectiveness of the procedures set out in the Code.

4 Electronic communications is an area that is increasingly important as businesses and consumers make the switch from paper to electronic communication. This report addresses the requirements relating to receipts, notification of changes to fees and the provision of regular statements. Central to the formulation of our positions on electronic communications is the issue of consumer consent to receiving communications electronically.

5 The Code will be reviewed five years following the conclusion of each preceding review. ASIC or its delegate will monitor data on subscribers' unauthorised transactions and compliance with specific Code requirements. Lastly, under the revised Code, we will have the general power to modify the application of the Code to particular products or classes of product to provide ongoing flexibility.

A About the EFT Code review

Background

6 The EFT Code is a voluntary industry code of practice that provides a range of protections for consumer electronic transactions. As administrator of the EFT Code, we are required to periodically review the Code.[1] Since the last review in 2001, there have been significant developments in the electronic payment industry and its regulation.

The review process

7 The current review of the EFT Code started in 2007 with the release of CP 78. The paper raised over 70 issues and attracted over 40 public submissions from consumers and consumer bodies, financial service providers, industry bodies, dispute resolution bodies, academics and government agencies. A working group was formed to help the review process.

8 A second consultation paper was released in October 2008. CP 90 contained proposals in relation to, among others things:

(a) the structure, scope and interpretation of the EFT Code;

(b) disclosure and complaints handling requirements;

(c) liability allocation for unauthorised transactions;

(d) electronic communication; and

(e) our power to modify and obligation to periodically review the Code.

9 We received 20 public submissions to CP 90 (see Appendix 1), as well as some confidential submissions. Two working groups were formed to address the issues surrounding the overall review of the EFT Code and mistaken payments, respectively. Appendix 2 lists the members of the EFT Code Working Group and the Mistaken Internet Payments Working Group. We also consulted a number of stakeholders involved in the innovative electronic payment products industry to discuss issues relating to their industry.

10 This review has taken longer to complete than initially anticipated, due to the complex nature of some of the issues considered as well as resource constraints. The consensus-based nature of the Code called for extensive stakeholder consultation to help us arrive at our final positions.

11 Previous reviews of the Code have centred on the issue of liability for unauthorised transactions. In this review, however, respondents were generally happy with this aspect of the current regime.

[1] EFT Code, cl 24.1(a).

Purpose and scope

12 This report sets out our final positions on the issues raised in this review of the EFT Code. It focuses on the issues discussed in CP 90 and sets out the original proposal, the feedback received, our final position and the rationale.

13 We anticipate that more issues will surface with the further development of innovative electronic payment products. These will be addressed in future reviews as they arise, or between reviews if the matter is urgent.

What's next?

14 We will revise the EFT Code to incorporate our final policy positions. In consultation with stakeholders, we will rewrite the Code in plain English and a principles-based manner, as far as possible, to make it simpler and more accessible to consumers of electronic payment services and products.

15 We expect to release the revised EFT Code in mid-2011. We will discuss an appropriate transition period with stakeholders.

B Structure, scope and membership of the EFT Code

Key points

The revised EFT Code will:

- cover all transactions initiated electronically;
- include lists of examples of transactions covered and not covered that may be modified in consultation with stakeholders;
- be drafted in plain English and principles-based as far as possible;
- include a statement of objectives;
- have a one-part structure with tailored requirements for low value electronic payment products; and
- remain a voluntary industry code of practice.

Statement of objectives

16 The EFT Code does not currently have a statement of objectives. ASIC Regulatory Guide 183 *Approval of financial services sector codes of conduct* (RG 183) states that a code should clearly set out its objectives.[2] For similar reasons, we thought the EFT Code would benefit from a clearly stated set of objectives.

Proposal in CP 90

17 CP 90 proposed to include the following objectives in the revised EFT Code:

(a) providing adequate consumer protection measures for electronic payments;

(b) promoting consumer confidence in electronic banking and payment systems;

(c) promoting better informed consumer decisions about electronic funds transfer services by providing effective disclosure of information;

(d) providing clear and fair rules for allocating liability for unauthorised transactions that reflect longstanding banking law principles and build community trust in online funds transfers;

(e) promoting effective procedures for resolving consumer complaints; and

(f) having all businesses that offer electronic funds transfer transactions subscribe to the EFT Code (proposal B1).

[2] RG 183.57.

Final position

18 The revised Code will include a statement that the Code aims to provide:

(a) a quality consumer protection regime for consumers who use electronic payment products and services;

(b) a framework to promote consumer confidence in electronic banking and payment systems;

(c) effective disclosure of information to enable consumers to make informed decisions about electronic payment services and products;

(d) clear and fair rules allocating liability for unauthorised transactions;

(e) effective procedures for resolving consumer complaints; and

(f) a regime that is flexible and accommodates providers of new electronic payment products and services.

Rationale

19 The inclusion of a statement of objectives in the EFT Code will help readers understand the context and the objectives the Code is designed to meet.

20 Submissions received were unanimous in their support for the inclusion of a statement of objectives in the EFT Code. The original proposal has been simplified and original objective (f) is no longer included as it is a means of achieving the Code's objectives, rather than an objective. We have included a new objective (f) as it is important that an industry Code has the flexibility to accommodate technology development in the payment industry.

One-part structure

21 The current EFT Code has a two-part structure. Part A governs the relationship between account institutions and their clients. Part B applies to stored value products.

Proposal in CP 90

22 CP 90 proposed replacing the current two-part structure of the EFT Code with a one-part structure, incorporating requirements tailored to different products: proposal B2.

Final position

23 The revised Code will replace the current two-part structure of the EFT Code with a one-part structure, tailored so that some requirements of the Code do not apply to some types of electronic payment products.

Rationale

24 Part B of the current EFT Code structure was added to establish a 'light-touch regime' for what were then newer electronic payment products, especially prepaid stored value products. In practice, due to a number of limitations (e.g. some products rely on remote authorisation, which is not covered by the definitions of 'stored value transactions' and 'stored value facilities'), Part B has not been widely used.

25 The rapidly changing nature of the electronic payment industry means that new products are constantly entering the market. Often these products will combine a wide spectrum of features, which makes them difficult to categorise under the current two-part structure.

26 Most submissions supported the proposal to adopt a one-part structure for the Code.[3] Some submissions also emphasised the need to have a light-touch approach for low risk products with low value holdings.[4] We agree with this view and aim to avoid over-regulation of simpler, low risk products.

27 Those who disagreed with this proposal argued that the EFT Code needs to recognise the significant differences in the features and purpose of various payment instruments.[5] We believe this concern can be addressed by tailoring some requirements of the Code to recognise the difference in features and the level of risks among electronic payment instruments, as well as having the general power to modify the EFT Code as it applies to a product or class of products.

28 Our proposals for tailored requirements for certain electronic payment products are discussed in Section C. The proposal for a general power to modify the application of the EFT Code to a product or class of products is discussed in Section H.

Coverage of the EFT Code

29 The scope of the EFT Code is currently defined in a complex way. Part A of the Code applies to 'EFT transactions', which are defined using various terms including 'funds transfers', 'electronic equipment', 'access method', 'account institution' and 'EFT account'. These terms are in turn defined using other terms. We propose to simplify the definition and clarify the coverage of the EFT Code.

[3] Australian Bankers' Association, *Submission* (21 December 2008), p. 1; ANZ, *Submission* (19 December 2008), p. 1; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 6; Financial Ombudsman Service, *Submission* (9 December 2008), p. 3; Law Council of Australia, *Submission* (24 December 2008), p. 2; PIF Australia, *Submission* (12 December 2008), p. 9.
[4] Abacus Australian Mutuals, *Submission* (24 December 2008), p. 3; Australian Payments Clearing Association, *Submission* (5 December 2008), p. 3.
[5] See, for example, Coles, *Submission* (8 December 2008), p. 2.

Proposal in CP 90

30 CP 90 proposed that the EFT Code:

(a) be redrafted to cover all electronic funds transfer transactions initiated electronically;

(b) include a non-exhaustive list of examples of the transactions the EFT Code covers; and

(c) include a non-exhaustive list of examples of the transactions the EFT Code does not cover, including:

(i) cheque transactions; and

(ii) card transactions, where the payment instrument is intended to be authenticated by comparing the consumer's manual signature with a specimen signature (proposal B3).

Final position

31 The revised EFT Code will:

(a) be redrafted to cover all consumer electronic funds transfer transactions initiated electronically;

(b) include a non-exhaustive list of examples of the transactions the EFT Code covers, including:

(i) ATM, EFTPOS and debit card transactions;

(ii) credit card transactions that are not intended to be authenticated by comparing the consumer's manual signature with a specimen signature;

(iii) direct debits;

(iv) telephone banking and bill payment transactions;

(v) internet banking, including 'Pay Anyone' funds transfer, and online bill payment facilities;

(vi) transactions using electronic prepaid cards, whether reloadable or not;

(vii) transactions using electronic toll devices; and

(viii) transactions using mobile phone payment services; and

(c) include a non-exhaustive list of examples of the transactions the EFT Code does not cover, including:

(i) cheque transactions; and

(ii) credit card transactions that are intended to be authenticated by comparing the consumer's manual signature with a specimen signature.

Note: Of course, subscribers can choose to adopt the Code for all card transactions.

32 These lists of examples of transactions covered and not covered by the EFT Code will be modified as needed, subject to a requirement to consult stakeholders.

BPay transactions and biller accounts

33 The revised Code will clarify that BPay transactions are covered by the Code (other than the mistaken payment provisions discussed in Section G).

34 We will also clarify that certain biller accounts are excluded from the EFT Code. A biller account is a consumer account held by a business that records the amounts owing and paid by the consumer for goods and services provided by that business only.

Rationale

35 This proposal was supported by almost all submissions that addressed this issue. Many submissions also emphasised the importance of ASIC being able to modify the lists of examples where appropriate.[6] We agree with this approach. This is consistent with proposal G1 in CP 90.

Direct debits

36 By 2009, direct debit use had more than doubled since the year 2000 (averaging 45.4 million transactions per month, to the value of $349.2 million).[7] Direct debit arrangements can be initiated various ways—by a consumer giving their authority in writing on paper, orally via telephone or by electronic communication (e.g. over the internet). Direct debits are increasingly being initiated and authorised electronically.

37 CP 90 included direct debit as a transaction covered by the new definition of 'electronic funds transfer'.

38 A number of submissions argued that as most direct debits are authorised using a written signature, they should not be covered by the Code.[8]

39 In our view, it is preferable from a consumer protection perspective that all direct debit transactions are included in the EFT Code, given their widespread use in Australia. From the perspective of regulatory simplicity, it is more logical and practical to have one set of Code provisions to apply to all direct debit transactions regardless of how authorisations are obtained.

40 Unlike credit card or charge card transactions, direct debit transactions do not have a set of rules comparable to those set by Visa or MasterCard. Direct

[6] See, for example, Australian Bankers' Association, *Submission* (21 December 2008), p. 2; Financial Ombudsman Service, *Submission* (9 December 2008), p. 4; PIF Australia, *Submission* (12 December 2008), p. 10.
[7] www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/Stats_DETrans_monthly.
[8] Australian Payments Clearing Association, *Submission* (5 December 2008), p. 4; Australian Payments Clearing Association *Supplementary submission on direct debits (31 March 2009).*

debit transactions are governed by Bulk Electronic Clearing System (BECS) Regulations and Procedures, which contain provisions about the responsibilities of businesses who are debit users and their sponsoring financial institutions, but do not cover issues such as liability allocation in the event of unauthorised transactions.

41 Further, while an authorisation for a direct debit arrangement is generally given by a consumer using a manual signature, both this and the individual transactions themselves are not intended to be authenticated by comparing the consumer's manual signature with a specimen signature. Each actual payment transaction is generated and processed electronically.

Expanding the membership of the EFT Code

42 Membership of the EFT Code has been generally limited to traditional financial services providers such as banks, credit unions and building societies. Providers of innovative electronic payment products have not yet subscribed to the Code, despite playing a greater part in the electronic payment industry today. A key issue raised by existing subscribers at the start of this review was the need for a level playing field, as new products issued by non-subscribers are competing in the market with existing products that comply with the EFT Code.

Proposal in CP 90

43 CP 90 proposed that if businesses offering electronic funds transfer payment products do not voluntarily subscribe to the EFT Code, the government give consideration as to whether:

(a) membership of the EFT Code should be made mandatory; or

(b) consumer protection in this area should be dealt with through regulation (proposal B5).

Final position

44 The issue of whether or not membership of the EFT Code should be mandatory for all businesses offering electronic funds transfer payment products is a matter for the government to decide. We will work towards improving the Code membership beyond the traditional financial services providers.

45 We will work with industry representatives and EDR schemes to monitor any problems relating to providers not subscribing to the EFT Code. We will monitor the development in the market and Code membership during the

first 18 months of the revised EFT Code. We will recommend law reform if it appears necessary.

Rationale

46 Submissions were divided on the question of whether the EFT Code should be made mandatory or whether consumer protection in this area should be dealt with through regulation.

47 Whether or not the EFT Code should be made mandatory is an issue for the government. We acknowledge that before the government can reasonably consider legislating or mandating subscription to the EFT Code, the Code needs to be promoted more vigorously, in order to improve consumer awareness of the benefits of dealing with a Code subscriber. We will continue to work with industry and consumer groups to promote the benefits of subscription to the Code.

48 The monitoring of take up rates and any problems relating to providers not subscribing to the Code will inform us about the effectiveness of the current regime and enable us to provide information to the government and, if necessary, a recommendation for law reform.

Principles-based, plain English code

49 As part of this review, we asked what changes should be made to make the EFT Code more user friendly.

Proposal in CP 90

50 CP 90 proposed that the EFT Code be redrafted as a principles-based code in plain English and that we would undertake this work as a separate process after we had finalised and publicly released our final recommendations for substantive changes to the EFT Code (i.e. this report): proposal B6.

Final position

51 We will redraft the EFT Code in plain English. We will adopt a principles-based approach without compromising clarity, certainty and essential consumer protection measures.

Rationale

52 There is universal support for the EFT Code to be redrafted in plain English. There is less support, even among industry stakeholders, for a principles-based code.

53 Most stakeholders stressed that some level of prescription is necessary to give subscribers clarity and certainty on issues such as liability for unauthorised transactions.[9] It was also noted that principles should not be so high level that they water down consumer protection[10] or render the Code incapable of application in any specific case.[11] We agree that some specificity is needed for effective operation of the Code.

Extension to small businesses

54 The EFT Code does not currently cover small business consumers. The question of whether the Code should extend its coverage to protect small business consumers was raised in the last review and again in the current review.

Feedback sought in CP 90

55 CP 90 asked whether the EFT Code should be extended to protect small business consumers. In particular, we asked for a definition of 'small business' to be used in the Code, whether any of the Code provisions need to be modified for application to small business consumers and for an estimate of the compliance costs of extending the Code coverage to small businesses: proposal B7.

Final position

56 The revised Code will not extend the coverage of the EFT Code to small business consumers.

Rationale

57 Submissions that addressed this issue were split in their views. On balance, however, there is insufficient support for the extension of the Code coverage to small business consumers. In particular, there was insufficient data to determine the prevalence of electronic banking problems for small business consumers. We will be working with industry participants and associations to collect data on small business complaints in this sector. Subscribers may also choose to voluntarily extend the protection of the Code to its small business consumers.

[9] Australian Bankers' Association, *Submission* (21 December 2008), p. 10; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 5; Legal Aid Queensland, *Submission* (12 December 2008), p. 11; Financial Ombudsman Service, *Submission* (9 December 2008), p. 6; Law Council of Australia, *Submission* (24 December 2008), p. 3.
[10] Legal Aid Queensland, *Submission* (12 December 2008), p. 5.
[11] Law Council of Australia, *Submission* (24 December 2008), p. 3.

58 The proposal to include small business consumers under the EFT Code was supported by small business associations[12] and some other stakeholders.[13] Those in support argued that there is little distinction in practice between the banking needs and activities of small business owners and individual consumers.[14] Supporters also argued that no modification is needed to apply the EFT Code to small business consumers, apart from the possible modification of no-fault liability for unauthorised transactions.[15] For example, Abacus suggested that if small business was included in the Code, no-fault liability should be set at the greater of $150 or 5% of the amount in dispute.[16]

59 Most financial industry submissions did not support the proposal to extend the coverage of the EFT Code to small business consumers.[17] Submissions cited the difficulty for institutions to monitor when a small business consumer is no longer a small business,[18] as this would require inclusion in the EFT Code of a threshold test of what constituted a small business, which was said to be problematic, and ultimately increase subscribers' compliance risks.[19]

60 There was also little agreement as to what definition of 'small business' the EFT Code should adopt if small business was to be covered.

[12] National Independent Retailers Association, *Submission* (19 December 2008), pp. 2–3; Small Business Development Corporation, *Submission* (11 December 2008), p. 1.
[13] Coles, *Submission* (8 December 2008), p. 4; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), pp. 8–9; Financial Ombudsman Service, *Submission* (9 December 2008), p. 7; Law Council of Australia, *Submission* (24 December 2008), p. 3. PIF Australia had 'no objection' to the EFT Code being extended to cover small business consumers, *Submission* (12 December 2008), p. 15.
[14] National Independent Retailers Association, *Submission* (19 December 2008), p. 3; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), pp. 8–9; Financial Ombudsman Service, *Submission* (9 December 2008), p. 7.
[15] National Independent Retailers Association, *Submission* (19 December 2008), p. 3; Small Business Development Corporation, *Submission* (11 December 2008), p. 2; Financial Ombudsman Service, *Submission* (9 December 2008), p. 7.
[16] Abacus Australian Mutuals, *Submission* (24 December 2008), p. 4.
[17] Australian Bankers' Association, *Submission* (21 December 2008), p. 12; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 4; Australian Payments Clearing Association, *Submission* (5 December 2008), p. 5; ANZ, *Submission* (19 December 2008), p. 4.
[18] Australian Bankers' Association, *Submission* (21 December 2008), p. 12.
[19] Australian Payments Clearing Association, *Submission* (5 December 2008), p. 5.

C Tailored requirements for certain types of electronic transactions

Key points

The revised EFT Code will provide light-touch requirements for electronic payment products capable of holding no more than $500 at any one time.

61 In order to improve the flexibility of the EFT Code, we consider it appropriate that less onerous requirements be available to simple, low value electronic payment products.

Proposal in CP 90

62 CP 90 proposed to tailor the requirements for transactions performed using newer electronic payment products with the following features:

(a) the product issuer is not able to cancel the product if it is lost or stolen;

(b) there is no electronic authentication mechanism to safeguard consumers against unauthorised transactions (e.g. a PIN or electronic signature is not required); and

(c) the maximum value that can be held on the product at one time is $100 (proposal B4).

Final position

63 The revised Code will tailor the requirements for transactions performed using electronic payment products where the maximum value that can be held on the product at any one time is $500.

64 For these products, the general EFT Code requirements apply subject to the modified requirements listed in Table 1.

Table 1: Tailored requirements for low value electronic payment products ($500 or less at any one time)

Area	Tailored requirement
Terms and conditions (current EFT Code cls 2, 3)	Subscribers must: • where practicable, give consumers a copy of terms and conditions for the product before they use it; or • give consumers notice of how they can obtain the full terms and conditions (e.g. refer them to a website) and highlight any key terms (e.g. expiry date). Subscribers must also: • give consumers a copy of terms and conditions on request; and • give advance notice of changes to terms and conditions: – directly to the consumer if the subscriber knows the identity and contact details of the consumer; – by publicising the changes at physical kiosks and ATMs where the product is used; or – by publicising the changes through the mechanism used by consumers to check their available balance (see below). Subscribers must not apply any such changes to terms and conditions to existing clients where they have not notified the client using one of the methods above.
Periodic statements (cl 4)	Subscribers are not required to provide consumers with periodic statements.
Receipts/ checking balances (cl 4.1)	Subscribers must provide consumers with a mechanism to check the available balance on these products. Subscribers must: • provide consumers with a receipt or reference enabling identification of a transaction, the transaction amount and any charges relating to the transaction; or • provide consumers with a mechanism to check their transaction history.
Liability for unauthorised transactions (cl 5)	If subscribers do not provide consumers with the ability to cancel or suspend the products and obtain a refund of the remaining balance, prominent warning about this must be given to consumers at point of sale or prior to their first use of the products.
Dispute resolution (cl 10)	Subscribers must comply with dispute resolution obligations set out in the EFT Code to the extent it is relevant and using appropriate communication channels.

Rationale

Issues with current arrangements under the EFT Code

65 Part B of the current EFT Code provides a light-touch regime for stored value products. Part B was intended to provide some basic consumer protection mechanisms for these products without hindering product innovation. At the time it was drafted, we expected that this would facilitate providers of these products subscribing to the Code and in doing so reassure consumers that their products met the key consumer protection standard in this industry.

66 In practice Part B has been underused. Many newer electronic payment products are operated using remote authorisation, which is not covered by the definition of 'stored value facility' under Part B. While these products could be covered by Part A of the Code, most providers of newer electronic payment products have not subscribed to the Code.

67 Arguably the diversity of products available in the market today does not allow for a single set of rules that can apply to all products in the same way and remain simple to implement. There is also little consensus either overseas or among stakeholders in Australia as to how these products can or should be regulated. Our view is that certain requirements in the Code should be tailored for low value products, based on a synthesis of consumer and industry feedback received and an analysis of the approaches taken overseas.

Consumer issues

68 New and innovative payment products are constantly being introduced into the market. Many have increasingly complex features and relatively high monetary value, and are accepted by a wide range of merchants, effectively allowing these products to compete with traditional banking products.

69 Some of these products are not subject to any industry code or regulations. These factors combined significantly increase the risks and potential losses for consumers should things go wrong. Consumer protection measures offered by product issuers vary greatly.

Industry issues

70 Some industry submissions were concerned that some current EFT Code requirements could not be applied to many emerging payment products. For example:

(a) as some products can be used anonymously, the requirement to provide regular statements to the users may be unworkable; and

(b) as some products are designed to be used exclusively online and are purchased by users largely for that reason, the EFT Code's reliance on paper-based communication imposes additional cost on issuers and is inconsistent with their business models.

71 While most industry submissions welcomed the idea of a light-touch regime for certain types of electronic transactions, there was little consensus on what that light-touch regime should involve or what products it should cover.

72 The proposal in CP 90 was based on the premise that less onerous requirements should only apply to simple, low value products, as these products would pose lower risks to consumers. Consumers using higher value and more complex products should have the normal EFT Code protections.

73 Almost all submissions that addressed this issue disagreed with the criteria proposed to define the scope of the tailored requirements. While the reasons varied, most submissions disagreed with criterion (a) (product issuer unable to cancel the product if it is lost or stolen) and (b) (product does not have electronic authentication mechanism to safeguard consumers against unauthorised transactions) because they might result in products being deliberately designed with fewer consumer safeguards, to fall under the light-touch regime.[20]

74 Similarly, almost all submissions that addressed this issue were of the view that a $100 cut-off point for a light-touch regime was too low. Alternatives submitted ranged from $250–$500[21] to $1000.[22] Those who advocated a cut-off point of $1000 cited the need for consistency with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML Act) and Class Order [CO 05/736] *Low value non-cash payment facilities*.

Overseas experience

75 In formulating our proposals we have reviewed the regulatory treatment of new and innovative electronic payment products in various overseas jurisdictions.

76 Overseas approaches to the regulation of new electronic payment products vary greatly. Relevantly, the UK and European Union have each adopted approaches that allow issuers of low value payment instruments to apply a light-touch regime in relation to disclosure and liability allocation.

77 A summary of relevant overseas approaches is set out in Appendix 3.

[20] ANZ, *Submission* (19 December 2008), p. 2; PIF Australia, *Submission* (12 December 2008), pp. 10–11; Universal Gift Cards, *Submission* (19 December 2008), p. 2; Westfield, *Submission* (5 December 2008), pp. 5–6; Legal Aid Queensland to an extent, *Submission* (12 December 2008), p. 3; Australian Bankers' Association to an extent, *Submission* (21 December 2008), p. 6; Abacus Australian Mutuals to an extent, *Submission* (24 December 2008), p. 3.
[21] Abacus Australian Mutuals to an extent, *Submission* (24 December 2008), p. 3.
[22] Australian Bankers' Association, *Submission* (21 December 2008), p. 7; Coles, *Submission* (8 December 2008), p. 3; PIF Australia, *Submission* (12 December 2008), p. 11; Universal Gift Cards, *Submission* (19 December 2008), p. 2; Westfield, *Submission* (5 December 2008), p. 6.

Coverage of tailored requirements

78 We agree with the submissions that the first two criteria proposed in CP 90 (that the issuer is not able to cancel the product if it is lost or stolen, and that the product does not have an electronic authentication mechanism to safeguard consumers against unauthorised transactions) risk giving firms an incentive to design products that do not incorporate adequate consumer protection measures, to bring those products within the light-touch EFT Code requirements.

79 The revised Code will simply apply the tailored requirements to low value electronic payment products. In this respect the proposed approach is most similar to the approaches taken in the European Union and the UK.

Monetary limit

80 As the monetary limit (i.e. the maximum value that can be held on a certain product at any one time) is now the sole criterion that will attract the light-touch EFT Code requirements, it is our view that the monetary limit ought to be set at a level that balances consumer and industry interests.

81 As noted previously, some submissions argued the need for consistency with the AML Act. However, the threshold of $1000 is used in the AML Act to determine the type of entities that must comply with obligations to verify consumers' identities and report suspicious activities to the Australian Transaction Reports and Analysis Centre (AUSTRAC). We do not consider these obligations overlap with the requirements of the EFT Code or that the two thresholds need be identical.

82 In the UK the light-touch regime prescribed by the Payment Services Regulations 2009 applies to low value payment instruments that store funds not exceeding €500. This cut-off point is lower than the threshold in the UK's Money Laundering Regulations 2007 which set lighter due diligence requirements for providers of electronic money that store no more than €2500 per calendar year (if the device can be recharged).

83 Class Order [CO 05/736] gives licensing and disclosure relief to providers of payment facilities where the total amount available under all facilities of the same class held by any one consumer does not exceed $1000 at any one time. We have granted conditional relief to providers of low value non-cash payment facilities on the basis that the products are generally simple, easy-to-use and well understood by consumers.

84 In our view a light-touch regime under the EFT Code ought to be available only to products with a maximum value of $500 at any one time. This threshold will capture many products currently available, in particular, simple products that pose limited risks to consumers.

85 Payment products capable of holding over $500 should be subject to the general EFT Code provisions, as they will typically be more complex, have features more akin to banking products and be more risky for the average consumer, in terms of potential fraud and unauthorised transactions. In our view, $1000 is a significant sum for the average consumer, and users of products that can hold over $500 should feel confident knowing that they are afforded the full protection of the EFT Code.

86 A lower monetary limit is appropriate for the EFT Code because the Code covers protections (e.g. for unauthorised transactions and lost/stolen cards) that are quite different to those covered in [CO 05/736] and should be provided for a wide range of products. The tailored requirements of the Code should also make it less expensive for industry participants to comply with the Code but should only apply to very low value products.

Liability for loss, theft or unauthorised transactions

87 Ideally all consumers should be able to notify product providers of the loss, theft or unauthorised use of their product, and receive either a refund or a replacement product with the remaining value. However, we acknowledge that there may be circumstances where it is not operationally or economically viable for very low value product providers to provide their customers with the ability to do so.

88 Having considered submissions received to CP 90 and the development in payment products, we believe that products that are capable of holding more than $500 should provide customers with the means to notify the subscriber of the loss, theft or unauthorised use of the products and provide the customers with a refund or a replacement product containing the remaining value. This is because the detriment to consumers of losing any amount greater than $500 is sufficiently significant to warrant subscribers investing resources to enable their customers to report the loss, theft or unauthorised transactions of the products and to prevent further transactions.

89 For products not capable of holding more than $500, if subscribers are not able to provide customers with the ability to cancel or suspend the products or provide a refund upon notification, a prominent warning must be given to consumers at point of sale or prior to the first use of the products, that they should treat the products like cash.

90 Subscribers should also comply with dispute resolution obligations set out in the EFT Code using communication channels that are appropriate for low value product providers and users of these products. What is appropriate will vary for different products and users (e.g. electronic communication may not be appropriate for customers who choose to lodge their complaints via the telephone because they do not have internet connection). We are not going to prescribe what we think constitutes appropriate communication channels in the revised Code.

Expiry period and refund of expired value

Feedback sought in CP 90

91 CP 90 asked if EFT Code subscribers who offer newer electronic payment products should be required not to use an expiry period, or be required to include a minimum expiry period of 12 months combined with a right to refund of expired value for a further 12 months: question B4Q3.

Final position

92 If an electronic payment product has an expiry period, subscribers must:

(a) provide a minimum expiry period of 12 months for the product from either the date of activation (if the product is non-reloadable), or the date when the funds were last loaded (if the product is reloadable);

(b) not unilaterally reduce the expiry period;

(c) give consumers a method of checking the expiry date of the product;

(d) include information about product expiry in their disclosure to consumers; and

(e) the expiry date must be prominently set out on the device (or if no relevant device, in a prominent way) in a way that is clear that it is an expiry date.

93 These requirements will apply to all products that impose expiry periods, not just low value products.

Rationale

94 While the revised EFT Code will not prohibit the use of expiry period, in our view it is best practice for EFT Code subscribers not to attach expiry period to their products. Products such as prepaid cards act as substitutes for cash, which does not typically expire.

95 Prepaid cards are widely used in Australia and so issues of expiry periods and refunds are relevant.

96 Almost all submissions agreed with a minimum expiry period of 12 months.[23] Similarly, almost all submissions rejected the proposal of a further 12-month period in which a consumer could claim refunds for any expired value.[24] The submissions argued that a requirement of no expiry period or

[23] Australian Bankers' Association, *Submission* (21 December 2008), p. 9; ANZ, *Submission* (19 December 2008), p. 3; Financial Ombudsman Service, *Submission* (9 December 2008), p. 5, Universal Gift Cards, *Submission* (19 December 2008), p. 2. Legal Aid Queensland suggested a minimum expiry period of six months, *Submission* (12 December 2008), p. 3; Law Council of Australia suggested an expiry period of two years, *Submission* (24 December 2008), p. 3.

[24] Australian Bankers' Association, *Submission* (21 December 2008), p. 9; PIF Australia, *Submission* (12 December 2008), p. 21; Universal Gift Cards, *Submission* (19 December 2008), p. 2; Westfield, *Submission* (5 December 2008), p. 6.

the additional 12-month period for refunds of expired value will impose an unreasonable commercial and regulatory burden on some businesses.

97 The minimum expiry period requirements in paragraph 92 should apply to all payment products that impose an expiry period, not just low value payment products. However, we understand that expiry periods are more common with low value stored value products.

98 A number of payment providers have issued high worth prepaid card products, with some offering as much as $10,000 of prepaid value. The proposal to introduce a minimum 12-month expiry period will provide consumers with a clearly disclosed minimum amount of time in which they can use their prepaid value. As most prepaid product issuers already offer 12–24 month expiry periods for their products, we do not envisage this proposal will significantly increase subscribers' compliance costs.

D Disclosure requirements

Key points

The revised Code will:

- allow both 'opt-in' and 'opt-out' receipt systems;
- require ATM owners to disclose charges for using an ATM before a person performs a transaction, and give the opportunity to cancel the transaction at no cost;
- retain the current requirements for notifying changes to fees and charges, while clarifying that individual notification can be delivered electronically where a customer has given consent; and
- provide that subscribers need not provide regular statements for accounts with both a zero balance and no transactions during the statement period.

Receipts

99 Clause 4.1(a) of the current EFT Code requires a subscriber to give a consumer a receipt unless the consumer specifically elects otherwise (opt-out). However, both opt-in (where consumers must positively choose to receive a receipt) and opt-out receipt systems are currently used by subscribers.

Proposal in CP 90

100 CP 90 proposed amending the EFT Code to:

(a) clarify that opt-in receipt systems comply with the EFT Code;

(b) clarify that a subscriber must take reasonable steps to provide a receipt and need not provide a receipt where it is not reasonably practicable to do so; and

(c) permit a receipt for a voice transaction to specify a number rather than the merchant's name, where the invoice from the merchant to the consumer includes their name and the number (proposal C1).

Final position

101 The revised Code will:

(a) state that both opt-in and opt-out receipt systems comply with the EFT Code;

(b) clarify that a subscriber must take reasonable steps to provide a receipt (and need not provide a receipt where it is not reasonably practicable to do so); and

(c) permit a receipt for a voice transaction to specify a reference number rather than the merchant's name, where the invoice from the merchant to the consumer includes their name and the number.

102 The revised EFT Code will state that disclosing the merchant's name in receipts is considered best practice.

Rationale

103 Almost all submissions that responded to this proposal agreed with points (a) and (b) in proposal C1 of CP 90 as they reflect common industry practice[25] without diminishing consumer amenity.[26]

104 We will therefore confirm that both opt-in and opt-out receipt systems comply with EFT Code requirements.

Surcharges charged by ATM owners

105 The ATM system in Australia has recently gone through RBA-led reforms to promote competition by making the cost of cash withdrawals more transparent to cardholders, and to remove barriers to entry for new ATM operators. Traditionally many financial institutions charge their customers a 'foreign fee' when they use an ATM belonging to another financial institution.

106 ASIC and the Reserve Bank of Australia (RBA) believe that ATM owners should be required to disclose to a person belonging to another financial institution the charges for using their ATM before that person performs a transaction, and give that person the opportunity to cancel the transaction at no cost.[27]

107 Clause 4.6 of the EFT Code requires Code subscribers to include in agreements with ATM owners the requirement that the ATM owner disclose any fee or surcharge they charge consumers.

Proposal in CP 90

108 CP 90 proposed that the EFT Code should be redrafted to make it clearer that:

[25] Australian Payments Clearing Association, *Submission* (5 December 2008), p. 5.
[26] Financial Ombudsman Service, *Submission* (9 December 2008), pp. 8–9.
[27] Reserve Bank of Australia, *Submission on CP 78* (30 April 2007), p. 1.

(a) subscribers should provide in their agreements with independent ATM owners that they must disclose charges for using an ATM before a person performs a transaction; and

(b) subscribers need not disclose specific surcharges charged by independent ATM owners to consumers in statements if they do not know the precise amount of these surcharges (proposal C2).

Final position

109 The revised Code will make it clearer that:

(a) subscribers who are ATM owners must disclose charges for using an ATM before a person belonging to another financial institution performs a transaction and the person must be able to cancel the transaction at no cost;

(b) when a Code subscriber and an ATM owner are party to an agreement, the agreement should specify that the ATM owner must disclose charges for using an ATM before a person performs a transaction and the person must be able to cancel the transaction at no cost; and

(c) it is best practice for subscribers to provide in statements information (where possible) about any surcharges charged for the use of ATMs that are not theirs (i.e. charged by the ATM owner). If subscribers do not know the precise amount of those surcharges they need not disclose the specific amounts in statements.

Rationale

110 Under the Direct Charging Regime, each time an ATM cardholder uses an ATM that does not belong to their financial institution a message appears on the ATM screen disclosing the amount that the ATM owner will directly charge the cardholder for using their service. The cardholder is given the option of either accepting the fee to continue using the ATM, or cancelling the transaction (in which case no fee will be deducted from the cardholder's account). The regime replaces the previous arrangements involving bilateral ATM interchange agreements whereby interchange fees were paid to ATM owners/operators by card issuers whenever their cardholders used other institutions' ATMs.[28]

111 The Direct Charging Regime is facilitated by the operation of the ATM Access Code and the Consumer Electronic Clearing System (CECS) Manual. While monetary penalties apply for breaches of the ATM Access Code, it is not mandatory. We understand that all independent ATM owners are currently sponsored into the Direct Charging Regime.

[28] For more information on ATM fee reforms, go to www.rba.gov.au/PaymentsSystem/Reforms/ATMFeeReforms/index.html and www.apca.com.au/afr/whatschanging.html.

112 In CP 90 we asked whether, after these ATM reforms, EFT Code subscribers would always have agreements with independent ATM owners. Most submissions did not address this question.

113 We will therefore clarify in the EFT Code that:

(a) ATM owners who are subscribers to the Code must disclose any charges before a cardholder belonging to another financial institution performs a transaction on the ATM, and that the cardholder must be able to cancel the transaction at no cost; and

(b) when a subscriber is party to an agreement with an ATM owner the agreement must require the owner to disclose any charges before a cardholder performs a transaction on the ATM, and that the cardholder must be able to cancel the transaction at no cost.

This position was supported by most submissions[29] and is in our view consistent with the intention of the ATM reforms.

Notifying changes to fees

114 Clause 3 of the current EFT Code requires subscribers to give consumers written notice at least 20 calendar days (or, where applicable legislation requires a longer notice period, that longer period) before:

(a) imposing or increasing charges for the use of an access method (e.g. a debit card);

(b) increasing an account holder's liability for losses; or

(c) imposing, removing or adjusting a daily or other transaction limit.

115 A number of industry representatives have voiced their concerns about the compliance costs of this requirement.[30]

Feedback sought in CP 90

116 CP 90 sought feedback on different approaches to notifying consumers of changes to fees and charges. In particular, we asked whether the current Code requirements should be retained or the use of media advertisements should be allowed, and sought feedback on the cost implications of both options: proposal C3.

[29] Abacus Australian Mutuals, qualified support, *Submission* (24 December 2008), p. 5; ANZ, *Submission* (19 December 2008), p. 5; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 10; Financial Ombudsman Service, *Submission* (9 December 2008), p. 9; Law Council of Australia, *Submission* (24 December 2008), p. 3.

[30] ANZ, *Submission on CP 78* (2 May 2007), p. 2; Abacus, *Submission on CP 78* (25 June 2007), p. 12; Australian Bankers' Association, *Submission on CP 78* (6 June 2007), p. 16; Suncorp, *Submission on CP 78* (1 May 2007), p. 3; PIF Australia, *Submission* (12 December 2008), pp. 16–17.

Final position

117 The revised Code will retain the current requirements for notifying changes to fees and charges. The Code is based on the requirements under the law and common industry practice.

118 Individual notification can be delivered using a variety of methods, including electronic communication where the customer has given consent to receive information this way: see Section E.

Rationale

119 Many stakeholders supported the retention of the current EFT Code requirements for notifying changes to existing fees and charges.[31] Others recommended aligning the Code with other industry codes of practice.[32] Relevant requirements in industry codes and legislations are summarised in Appendix 4.

120 In our view a minimum of 20 calendar days advance notice (or, where the applicable legislation requires a longer notice period, that longer period) is important for changes to fees and charges. The 20-day advance notice is consistent with the Mutual Banking Code of Practice and the *National Consumer Credit Protection Act 2009* (National Credit Act). The Code of Banking Practice and *Corporations Act 2001* (Corporations Act) generally require at least 30 calendar days notice. The revised EFT Code will therefore reflect the current legislation (where applicable).

121 As the EFT Code currently stands, where legislation and the EFT Code require different notification periods for changes to terms and conditions:

(a) the Code subscriber must provide notice at the earliest time as is required under the legislation or the EFT Code; and

(b) the provision of notice under the legislation at or earlier than the time required by the EFT Code, will satisfy the Code's requirements for notice.

122 Code subscribers should comply with the earliest disclosure obligation and thus satisfy the timing of all relevant disclosure obligations.

123 The Code requirement to provide at least 20 calendar days notice prior to changing transaction limits and liability for losses is important to enable consumers to control their exposure to the risk of losses from unauthorised transactions. This is an important issue not fully dealt with by the other Codes and legislation discussed earlier.

[31] Australian Bankers' Association, *Submission* (21 December 2008), p. 17; Financial Ombudsman Service, *Submission* (9 December 2008), p. 9.
[32] Coles, *Submission* (8 December 2008), p. 5; Australian Payments Clearing Association, *Submission* (5 December 2008), p. 6; ANZ, *Submission* (19 December 2008), p. 5; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 11.

124 We accept that the cost to business of mailing written notices is significant. There are increasing numbers of products whose features are entirely online, and whose customers prefer to conduct their communication electronically. Thus we propose that subscribers to the EFT Code be allowed to use electronic communication to meet their disclosure obligations under the Code, subject to some conditions: see Section E.

125 In our view the use of media advertisements on their own to notify customers of significant changes is of limited effectiveness.[33] Media advertisements can be used to disclose changes to existing fees and charges in conjunction with individual notification.

Periodic statements

126 Clause 4 of the EFT Code requires subscribers to provide statements every six months. Other industry codes qualify this by providing that statements need *not* be provided for dormant accounts.

Feedback sought in CP 90

127 In CP 90 we asked whether the EFT Code should be modified so that subscribers need not give statements for accounts with both a zero balance and no transactions during the statement period: proposal C4.

Final position

128 The revised Code will provide that subscribers are not required to provide statements for accounts with a zero balance where there were no transactions during the statement period.

Rationale

129 The feedback sought in proposal C4 of CP 90 only dealt with zero-balance statements. However, broader and more fundamental issues arose in this review in relation to statements, in particular, that of paper versus electronic communication.

130 The issues in relation to statements are covered in more detail in Section E.

Statements and zero-balance accounts

131 The EFT Code currently requires subscribers to give a statement every six months to account holders as a record of account activity, with the exception

[33] See Australian Competition and Consumer Commission, *Review of the Australian product safety recalls system: ACCC research report* (January 2010) at 3.6. Report available at www.accc.gov.au/content/item.phtml?itemId=930113&nodeId=ea13de4b0902a0365ae124a43ddb5123.

of passbook accounts.[34] Account holders are also to be offered the option of receiving periodic statements more frequently. The Code also specifies the information to be provided in a statement, including details of the transaction and any charges relating to the use of an access method.[35]

132 Various legislation and industry codes also require customer statements every six months, or more frequently if customers request it.[36]

133 The National Credit Code provides that statements need not be given for accounts with a zero balance where there were no transactions during the statement period.[37] Both the Code of Banking Practice and the Mutual Banking Code of Practice go further and state that no statements are needed for accounts that are dormant.[38]

134 The Corporations Act is silent on this issue.

135 In our view, industry codes ought to do more than restate the law; they should promote a higher standard of conduct consistent with best practice.[39]

136 Retaining the requirement for EFT Code subscribers to provide a statement every six months, but amending the Code to allow subscribers not to provide regular statements for accounts with a zero balance and where there were no transactions during the reporting period, brings the EFT Code into alignment with the more recent national consumer credit legislation and other industry codes of practice.

137 In our view, subscribers should provide regular statements for accounts that had no activity during the reporting period if there are funds in the account. For consumers who have funds put away for long periods, having regular statements allows them to monitor their finances, even if they choose not to use the funds.

[34] EFT Code, cl 4.2.
[35] EFT Code, cl 4.3.
[36] *Corporations Act 2001*, s1017D(3); National Credit Code, s33.
[37] National Credit Code, s33(3).
[38] Code of Banking Practice, cl 24; Mutual Banking Code of Practice, s16.
[39] RG 183.28–183.29.

E Electronic communications and privacy

Key points

The revised Code will provide that:

- subscribers can meet their disclosure obligations under the Code electronically if the consumer consents to receiving information this way (opt-in);
- for products designed for exclusively electronic use, consumer consent can be obtained at the point of acquisition as long as this is made clear;
- the use of hyperlinks to deliver disclosure required under the EFT Code is discouraged; and
- receipts for non-internet payments initiated by credit card or debit card must not include a non-truncated version of account number and not include an expiry date.

Consent to electronic communication

138 In CP 90 we proposed that subscribers could electronically deliver information that must be disclosed under the EFT Code. In this section we provide further clarification on some elements of electronic communication including consumer consent, the difference between exclusively electronic products and hybrid products, and discuss the risks and challenges posed by the use of electronic communication.

139 In this section we also discuss how our broader work on online financial disclosure relates to EFT Code requirements.

Proposal in CP 90

140 CP 90 proposed to amend the EFT Code so that subscribers can meet their disclosure obligations under the Code electronically by using emails to notify consumers that information that must be disclosed is available from a website, on the following conditions:

(a) the consumer must positively consent to receive the information this way;

(b) the email notice must clearly describe the information so consumers can make an informed decision whether to get the information this way;

(c) the information must be easy for the consumer to find;

(d) the information must be easy to retrieve, read, print and, as far as practicable, to save electronically for six years—or the consumer must

be able to request a paper copy of the information for up to six years, and must be told this;

(e) the information must be available on a website for a reasonable period (we consider 18 months or two years to be the minimum reasonable period, especially given the need for people to find old receipts and statements when doing their tax); and

(f) subscribers must have a user-friendly process for consumers to update their email address (proposal F1).

Final position

141 The revised Code will provide that subscribers can meet their disclosure obligations under the Code electronically by using electronic communication to notify consumers that information that must be disclosed is available from a website, on the conditions below:

(a) the consumer must consent (i.e. opt-in) to receive the information this way;

(b) the information must be easy for consumers to retrieve, read, print and save electronically;

(c) the information must be available at an electronic location for a reasonable period;

(d) the consumer must be able to request a paper copy of the information for up to seven years; and

(e) subscribers must have a user-friendly process for consumers to update their electronic contact details.

142 For products designed exclusively for electronic use, the condition that the customer has the right to obtain a paper copy will not apply.

Rationale

143 In considering issues relating to electronic communication we have differentiated between new products that are wholly managed online and those that combine online and non-online features. We will take a different approach to consent for these products.

144 We recognise the importance of electronic communication and the convenience it offers business and consumers, and seek to promote the responsible use of electronic communication.

145 It was submitted during consultation that the EFT Code should aim to be technologically neutral[40] in order to accommodate technology innovation in the market. We have replaced ‘emails’ in paragraph (a) of proposal F1 of

[40] BPay, *Submission* (25 November 2008), p. 5.

CP 90 with 'electronic communication', and 'website' in paragraph (b) of proposal F1 with 'electronic address', so as not to mandate the use of any particular means of electronic delivery and accommodate technological innovation. This will also provide greater flexibility for consumers to determine what kind of electronic communication suits them best.

146 We have simplified the conditions proposed under paragraph (b) of proposal F1 (CP 90). We maintain that the consumer's consent to receiving information electronically is important. Subscribers should ensure that the information is available at their electronic address such that consumers can find and read it with ease. Consumers should be able to print the information or save it electronically, should they choose to do this.

147 The information should remain available at an electronic address for a reasonable period so that consumers who might not have the opportunity to access the information immediately can do so later. In our view, 18 months is the minimum period in which a piece of information should continue to be available at an electronic address.[41] We expect that industry will maintain sound business practices so as to attract and retain consumer loyalty, and we will monitor this.

148 Subscribers will be required to provide consumers with paper copies of information for up to seven years. Businesses are already required to retain copies of their records for seven years under the Corporations Act.[42] In our view this requirement is reasonable given the overall greater flexibility in the revised Code relating to use of electronic communication and disclosure.

149 Consumers' ability to update their electronic contact details with ease is essential for effective communication.

150 For EFT Code purposes we will not prescribe the ways in which consumers can update their electronic contact details, so as to offer greater flexibility for both consumers and industry. The requirement for subscribers to have a user-friendly process for consumers to update their details will address issues such as bounced emails. We understand that some subscribers already have additional procedures in place to address the problem of successive failed deliveries of electronic communication.

Consumer consent to electronic communication and disclosure

151 Some submissions said that express consumer consent is unnecessary for some notifications,[43] or for products designed to be operated wholly online.[44]

[41] This view is broadly consistent with ASIC Consultation Paper 121 *Facilitating online financial services disclosures* (CP 121), item 4 of proposed good practice guidance, p. 15.
[42] Corporations Act, s286; Financial Ombudsman Service, *Submission* (9 December 2008), p. 16; Law Council of Australia, *Submission* (24 December 2008), p. 7.
[43] ANZ, *Submission* (19 December 2008), p. 10.
[44] Australian Bankers' Association, *Submission* (21 December 2008), p. 27.

152 In our view, unless the law provides otherwise, generally a subscriber should obtain customer consent prior to electronic delivery of mandatory disclosures. This view is consistent with our approach in Consultation Paper 121, *Facilitating online financial services disclosures* (CP 121).

New accounts and products

153 For products designed exclusively for electronic use, consumer consent can generally be assumed at the point of acquisition, provided that it is made clear to the client that the primary method of communication for the product will be electronic.

154 Consumers who purchase wholly electronic products will be made aware that all communications are electronic, so subscribers need not provide the option of paper-based communication and disclosure.

155 For products not designed for exclusively electronic use, electronic communication and disclosure can be used when a consumer consents to receiving electronic communication and disclosure (opt-in). Such consent can be requested and obtained at point of sale provided that the request is clear and the process requires a specific positive action by the consumer (e.g. ticking a box) to give their consent.

Existing accounts

156 In our view a subscriber to the EFT Code should not use electronic communication and disclosure for existing customers or account holders without first having obtained their consent. To do so would be inconsistent with the customer having choice about how they communicate with their financial institution. We believe that the Code should keep paper-based disclosure as the default unless the customer decides otherwise. That is, existing customers or account holders must opt in for the use of electronic communication and disclosure by Code subscribers. This approach is broadly consistent with the proposals in CP 121.

Hyperlinks

157 Clause 22 of the current EFT Code allows a subscriber to provide information electronically by providing the consumer with the ability to readily retrieve the information by electronic communication. The examples given include the provision of an electronic link (hyperlink) to the information at the subscriber's website.

158 The use of hyperlinks is linked to the risk of 'phishing' and other internet scams, in which consumers follow hyperlinks in emails purporting to be from their financial service provider.

159 ASIC, the Australasian Consumer Fraud Taskforce and the banking industry have encouraged consumers not to follow hyperlinks, to reduce the risk of consumers falling into a scam. However, hyperlinks are increasingly common and it provides a convenient way to deliver information.

Feedback sought in CP 90

160 CP 90 sought views on using hyperlinks to deliver EFT Code disclosures. In particular, it asked whether the EFT Code should prohibit the use of hyperlinks to deliver information, or the use of hyperlinks should be limited in any way. CP 90 also invited feedback on any potential cost savings from the use of hyperlinks: proposal F3.

Final position

161 The revised Code will discourage (as a matter of best practice) the use of hyperlinks to deliver the disclosures required under the EFT Code.

Rationale

162 Submissions were divided on whether the EFT Code should prohibit the use of hyperlinks, with the majority supporting the prohibition of hyperlinks for delivery of Code disclosures.

163 Both industry[45] and consumer representatives[46] voiced concerns that to allow hyperlinks would be inconsistent with best industry practice and would dilute the industry's message to consumers about the risks associated with responding to hyperlinks, such as potential exposure to phishing and scams.

164 Other submissions, however, argued that the EFT Code should not be so prescriptive as to prohibit hyperlinks, and that the decision about use of hyperlinks should be left to the discretion of the subscriber.[47]

165 Still others proposed a middle ground: that hyperlinks should be allowed only if they lead to general information.[48]

166 No submission addressed the question of potential cost savings for subscribers if the use of hyperlinks was permitted.

167 In CP 121, we invited comments on the proposal to give relief to enable providers to deliver Product Disclosure Statements, Financial Services Guides and Statements of Advice via hyperlinks and references to website

[45] Australian Bankers' Association, *Submission* (21 December 2008), p. 31; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 8.
[46] *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 17.
[47] See, for example, Financial Ombudsman Service, *Submission* (9 December 2008), p. 17.
[48] Coles, *Submission* (8 December 2008), p. 7.

addresses. CP 121 also stated our preference for using a reference to a website rather than a hyperlink.

168 While there may be circumstances where hyperlinks are appropriate, in our view hyperlinks should not be used by EFT Code subscribers to deliver mandatory disclosures, particularly those containing personalised information where the customer is asked to enter security details (e.g. username and password) to access the disclosures. Use of hyperlinks is contrary to best industry practice and to industry and consumer messages about the risks associated with responding through hyperlinks. Industry and consumer advocates do an important job in raising awareness of the risks associated with the use of hyperlinks, and it is important that a consistent message is conveyed by regulators, financial institutions and consumer organisations. The risk of fraud through the use of hyperlinks is also particularly high in the banking industry, the majority of whose members are subscribers to the Code.

169 We therefore discourage the use of hyperlinks by EFT Code subscribers for disclosures required under the Code. We encourage instead the practice of providing consumers with a reference to a website where the relevant disclosure information is available, rather than a hyperlink, and continued consumer education about the risks involved in the use of different types of electronic communication.[49]

Phishing

170 CP 121 sought comments on the suggestion that disclosure documents should be delivered in a way that does not unreasonably expose customers to security risks such as phishing.[50] 'Phishing' is a type of scam in which fraud perpetrators use deceptive electronic messages that appear to come from legitimate businesses, to coax individuals into revealing personal information such as banking details.

171 In our view the use of hyperlinks significantly increases an account holder's exposure to the risk of phishing, particularly for banking products. We believe discouraging hyperlinks for delivery of financial disclosures under the EFT Code, particularly those containing personal information, will help reduce the risk of phishing, along with consumer education on how to better protect their interests when using electronic payment transactions. This position is supported by most stakeholder submissions received.

[49] We will omit the examples using hyperlinks in the current version of the Code.
[50] CP 121, item 7 of proposed good practice guidance, p. 16.

Privacy issues with receipts

172 Clause 4.1 of the current EFT Code prescribes some information that must be provided by subscribers when issuing receipts, including:

(a) transaction amount;

(b) time and date of transaction;

(c) an indication of the account(s) involved; and

(d) data that would enable a subscriber to identify the customer and the transaction.

173 The issue discussed in CP 90 was whether the provision of this information on receipts could potentially compromise the privacy or security of a consumer's financial information.

Proposal in CP 90

174 CP 90 proposed that receipts:

(a) must include a truncated version of any account number; and

(b) must not include an expiry date or any other extraneous information (proposal F2).

Final position

175 The revised Code will retain the current requirements relating to receipts and provide that receipts for non-internet payments initiated by credit card or debit card:

(a) must not include a non-truncated version of the account number; and

(b) must not include an expiry date.

Rationale

176 Most submissions supported proposal F2 in CP 90,[51] but there were reservations expressed about its application to all electronic payment transactions.[52] For example, non-truncated account details on a receipt may be required to establish that a payment has been made to a particular Bank State Branch (BSB) number and account number for an internet banking transaction or in-branch transaction. This is in contrast to EFTPOS and ATM receipts, which are rarely used for reconciliation purposes. The possibility of a stranger obtaining a receipt is also lower for internet banking than for

[51] Coles, *Submission* (8 December 2008), p. 7; Australian Bankers' Association, *Submission* (21 December 2008), p. 30; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 8; ANZ, *Submission* (19 December 2008), p. 10; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 16; Financial Ombudsman Service, *Submission* (9 December 2008), p. 17; Law Council of Australia, *Submission* (24 December 2008), p. 7.

[52] Australian Payments Clearing Association, *Submission* (5 December 2008), p. 7.

ATM and EFTPOS receipts, which are often printed and discarded in public places.[53]

177 We accept 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. 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.

178 While some stakeholders felt the requirement to omit the expiry date from receipts was not justified as the card expiry date is of little use without full card number details,[54] we agree with those who submitted that knowledge of a card number and expiry date is often the only information required to process a transaction. The requirement to omit the expiry date from receipts will in our view reduce the amount of information that can be used to perpetrate a card fraud.

179 Some merchants include the customer's name and address (and sometimes phone number) on receipts when the customer is part of the merchant's loyalty scheme. As a general rule we do not think that receipts should contain any extraneous information.

180 We acknowledge that sometimes extraneous information may benefit consumers even when not needed for transaction confirmation purposes, such as where an ATM receipt shows the account balance after a withdrawal.[55] In our view receipts should not contain extraneous personal information about a customer. However, because what is useful for consumers will differ from product to product, the revised EFT Code will not contain a general prohibition on printing of extraneous information on receipts.

[53] Australian Payments Clearing Association, *Submission* (5 December 2008), p. 7.
[54] Australian Payments Clearing Association, *Submission* (5 December 2008), p. 7.
[55] Example given in Australian Payments Clearing Association, *Submission* (5 December 2008), p. 7.

F Complaints handling

Key points

The revised Code will:

- use the definition of 'complaint' in AS ISO 10002-2006 *Customer satisfaction—Guidelines for complaints handling in organizations*;
- require subscribers to maintain internal dispute resolution procedures that comply with AS ISO 10002-2006 consistent with Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165);
- allow subscribers a short time period to investigate a complaint and to resolve it to the customer's complete satisfaction before the requirement to give written information about the dispute resolution process is activated. The time period will be consistent with the time period specified in RG 165; and
- require subscribers to respond within 30 calendar days to requests for information from other subscribers, unless there are exceptional circumstances.

Australian standard on complaints handling

181 Clause 10.1 of the current EFT Code requires subscribers to establish internal dispute resolution procedures that comply with Australian Standard AS 4269-1995 *Complaints handling*. A new Australian standard on complaints handling has since been introduced: AS ISO 10002-2006 *Customer satisfaction—Guidelines for complaints handling in organizations*.

Proposal in CP 90

182 CP 90 proposed amending the EFT Code to:

(a) include a definition of 'complaint' using the definition in AS ISO 10002-2006; and

(b) require subscribers to establish internal dispute resolution procedures that comply with the new standard (proposal D1).

Final position

183 The revised Code will:

(a) include a definition of 'complaint' using the definition in AS ISO 10002-2006; and

(b) require subscribers to maintain internal dispute resolution procedures that comply with AS ISO 10002-2006 to the extent required by

Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165).

Rationale

184 All submissions but one agreed in principle with this proposal. Some suggested a distinction between a complaint and a query,[56] such that dispute resolution procedures need not apply during a query handling process.

185 AS ISO 10002-2006 defines 'complaint' as:

> An expression of dissatisfaction made to an organisation, related to its products and services, or the complaints handling process itself, where a response or resolution is explicitly or implicitly expected.[57]

186 In our view, based on the ordinary meaning of the words as defined in a general dictionary, a query is different to an 'expression of dissatisfaction'. A query will not be captured by this definition of complaint unless the nature of a customer's expression has changed from that of a question to that of dissatisfaction.

187 This approach is consistent with that taken in RG 165, which adopts the AS ISO 10002-2006's definition of 'complaint'. We expect subscribers to use their internal dispute resolution procedures to deal effectively with and monitor their customer inquiries as well as complaints (consistent with RG 165.73).

188 We expect subscribers to maintain internal dispute resolution procedures that:

(a) satisfy the Guiding Principles at Section 4 of AS ISO 10002-2006, and follow Section 5.1—Commitment, Section 6.4—Resources, Section 8.1—Collection of Information, and Section 8.2—Analysis and evaluation of complaints in AS ISO 10002-2006; and

(b) have a system for informing complainants or disputants about the availability and accessibility of the relevant EDR scheme (see RG 165.65).

Complaints that are not immediately settled

189 Clause 10.3 of the current EFT Code provides that when a complaint is not immediately resolved, a subscriber needs to provide the customer with written information about its complaints handling procedures.

[56] Australian Bankers' Association, *Submission* (21 December 2008), p. 19; Australasian Compliance Institute, *Submission* (4 December 2008), p. 3; Financial Ombudsman Service, *Submission* (9 December 2008), p. 10.
[57] AS ISO 10002-2006 *Customer satisfaction—Guidelines for complaints handling in organizations*, at 2.

Proposal in CP 90

190 CP 90 proposed amending this to provide that a subscriber can investigate a complaint for one business day before giving the customer written information about how it resolves complaints: proposal D2.

Final position

191 The revised Code will provide that a subscriber will have a short time period to investigate a complaint and resolve it to the customer's complete satisfaction before the requirement to give written information about the dispute resolution process is activated. The time period will be consistent with the time period specified in RG 165.

Rationale

192 Several submissions suggested that five business days is a preferable timeframe.[58] Sometimes subscribers require more than one business day to successfully contact the other entity involved in a complaint.

193 RG 165 currently provides that a financial service provider or product issuer is not required to apply the full internal dispute resolution process (in terms of capturing and recording a complaint) if the complaint is resolved to the customer's satisfaction by the end of the next business day.[59] This requirement is currently under review.

194 Many of the EFT Code subscribers are also subject to the requirements of RG 165. To reduce the compliance burden, we will align the EFT Code with the requirement in RG 165.

Complaints involving two or more subscribers

195 Some stakeholders argued that the timeframe for resolving complaints needs to accommodate situations where one of the parties involved in the electronic funds transfer transaction is a non-Code subscriber (e.g. an independent ATM owner).[60]

196 As the EFT Code remains a voluntary industry code, the provisions of the Code will only bind subscribers to the Code. Our proposal related to the introduction of a timeframe for the exchange of information between two Code subscribers where one of them is the subject of a complaint.

[58] Australian Bankers' Association, *Submission* (21 December 2008), p. 21; Australasian Compliance Institute, *Submission* (4 December 2008), p. 4; ANZ, *Submission* (19 December 2008), p. 7.
[59] RG 165.82.
[60] Australian Bankers' Association, *Submission* (6 June 2007), p. 21.

Proposal in CP 90

197 CP 90 proposed introducing a requirement for a subscriber to respond to requests for information from another subscriber within 30 days, unless there are exceptional circumstances: proposal D3.

Final position

198 The revised Code will introduce a requirement for a subscriber to respond to requests for information from another subscriber within 30 calendar days, unless there are exceptional circumstances.

Rationale

199 Most submissions that addressed this issue agreed with this proposal.[61] Better resolution of complaints involving multiple subscribers is an important issue on which we have received a large number of complaints over many years.

200 In setting the 30-day timeframe for EFT Code subscribers, we reiterate our view that the standard set out in the EFT Code is a threshold to be met by industry but should not limit its ability to provide better service, in this case, timely complaints handling procedures and faster dispute resolution.

201 We believe the timeframe for response to requests for information from other subscribers should be 30 calendar days, not business days. This is consistent with RG 165 and industry codes.[62] Allowing 30 business days would essentially result in complaints taking around 40 calendar days to finalise, and even longer in exceptional circumstances. This may put consumers at risk of financial distress and place the work of entities such as EDR schemes on hold for longer. We also believe that the sooner a complaint is resolved, the more likely it is that a subscriber will repair their relationship with the customer.

Providing information to EDR schemes

202 EDR schemes sometimes experience difficulty obtaining information from the parties involved in a dispute. In such situations, EDR schemes are entitled to resolve factual issues based on the available information. The EFT Code is currently silent on this matter.

[61] Australian Bankers' Association, *Submission* (21 December 2008), p. 21; Coles, *Submission* (8 December 2008), p. 6; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 6; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 13; Financial Ombudsman Service, *Submission* (9 December 2008), p. 12; Law Council of Australia, *Submission* (24 December 2008), p. 4.
[62] Mutual Banking Code of Practice.

Proposal in CP 90

203 CP 90 proposed amending the EFT Code so that where an EDR scheme asks for information from a subscriber and they do not provide it:

(a) the scheme must give the subscriber an opportunity to explain why they cannot supply the information; and

(b) if the subscriber does not provide a satisfactory explanation, the scheme can resolve the factual issue the information relates to on the basis of the information available to it (proposal D4).

Final position

204 The revised Code will provide that where an EDR scheme asks for information from a subscriber and they do not provide it:

(a) the scheme must give the subscriber an opportunity to explain why they cannot supply the information; and

(b) if the subscriber does not provide a satisfactory explanation, the scheme can resolve the factual issue the information relates to on the basis of the information available to it.

Rationale

205 Almost all submissions that addressed this issue agreed with proposal D4 of CP 90. It is also consistent with existing procedures of EDR schemes.[63]

206 A number of submissions suggested that this issue would be best addressed through our review of dispute resolution procedures.[64] Regulatory Guide 139 *Approval and oversight of external dispute resolution schemes* (RG 139) currently does not address this issue. However, in our view, there is merit in amending the EFT Code to reflect this practice so as to promote awareness among Code subscribers and consumers.

Limitations period for complaints

207 Clause 4.4 of the current EFT Code prohibits subscribers from imposing a time limit on complaints about erroneous or unauthorised transactions.

[63] ANZ, *Submission* (19 December 2008), p. 7; Financial Ombudsman Service, *Submission* (9 December 2008), p. 12. See, for example, rule 27 of the Credit Ombudsman Service Rules (7th ed).
[64] Abacus Australian Mutuals, *Submission* (24 December 2008), p. 6; Australian Payments Clearing Association, *Submission* (5 December 2008), p. 6.

Proposal in CP 90

208 CP 90 proposed amending the EFT Code to introduce a six-year time limit for consumers to bring their complaints to a Code subscriber. The limit would run from the time that the complainant first became aware, or should reasonably have become aware, of the event that the complaint is about: proposal D5.

Final position

209 The revised Code will introduce a six-year time limit for complaints to be brought to a Code subscriber for determination in accordance with the EFT Code. The limit would run from the time that the complainant first became aware, or should reasonably have become aware, of the event that the complaint is about. Consumers may also bring the complaint to an EDR scheme within two years of a financial service provider providing a 'final response' at internal dispute resolution, or within six years from the date the consumer became aware (or should reasonably have become aware) of the loss where no 'final response' has been provided.

Rationale

210 While all submissions supported the introduction of a time limit for complaints to be determined in accordance with the EFT Code, they were divided on what the time limit should be. Some agreed with a six-year time limit, however, the majority preferred a shorter time, for various reasons.[65]

211 We agree that too long a time limit might detract from the message that consumers should review their statements in a timely manner,[66] and that delays can contribute to future losses or disputes,[67] which can be costly to both consumers and business. The average consumer will take less than six years to become aware of a problem in relation to transactions covered by the EFT Code. This is supported by the Financial Ombudsman Service's (FOS) experience, in that most of the disputes received by FOS involve transactions that were made less than six years prior to the consumer bringing the dispute to the account institution.[68]

212 RG 139 provides that the time limit for bringing a complaint to an EDR scheme is the earlier of six years from the date that the consumer first becomes aware (or should reasonably have become aware) of the loss; or two years from when the financial service provider provides a 'final

[65] Coles, *Submission* (8 December 2008), p. 6; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 13.
[66] Australian Bankers' Association, *Submission* (21 December 2008), p. 24; Law Council of Australia, *Submission* (24 December 2008), p. 4.
[67] Australian Payments Clearing Association, *Submission* (5 December 2008), p. 6.
[68] Financial Ombudsman Service, *Submission* (9 December 2008), p. 13.

response' at internal dispute resolution.[69] Exceptions can be made where the EDR scheme considers that exceptional circumstances apply and/or the financial service provider agrees to the EDR scheme having jurisdiction.[70]

213 In our view a six-year time limit for complaints is appropriate as it provides adequate consumer protection and is consistent with the statutory limitation period, EDR schemes' practice and RG 139.

214 As most consumers already lodge their complaints within six years of the disputed transactions, the proposal for a six-year time limit will not significantly change the number of disputes already received by institutions, or dispute resolution costs to institutions. Similarly, the imposition of the time limit will not reduce consumer amenity as most disputes are dealt with within six years of the event that gives rise to the complaint.

[69] RG 139.201.
[70] RG 139.202.

G Liability for unauthorised transactions and mistaken payments

Key points

The revised EFT Code will:

- provide that a consumer is liable for unauthorised transactions when they leave a card in an active ATM;
- require subscribers to prohibit merchants from taking consumers' PINs as part of book up arrangements; and
- specify funds recovery procedures for mistaken internet payments.

Liability for losses caused by a person leaving their card in an ATM

215 The EFT Code does not specifically address liability allocation for situations where unauthorised transactions occur as a result of a person leaving a card in an ATM.

Proposal in CP 90

216 CP 90 proposed amending the EFT Code so that a consumer is liable for unauthorised transactions that occur because they leave a card in an active ATM, where the ATM automatically shuts down within 40 seconds: proposal E1.

Final position

217 The revised Code will provide that, under normal circumstances, a consumer is liable for unauthorised transactions that occur because the consumer leaves a card in an active ATM, where the ATM satisfies adequate safety standards aimed at mitigating the risk of the consumer leaving their card behind.

Rationale

218 We accept that ATM operators employ differing safety mechanisms to help protect consumers. In particular we note that most ATMs do not shut down when a consumer leaves a card in an active ATM. Instead, when no activity occurs within a certain period, many ATMs retract and deposit the card into an internal card bin.[71]

[71] Australian Bankers' Association, *Submission* (21 December 2008), p. 25; ANZ, *Submission* (19 December 2008), p. 8.

219 Other ATMs use 'dip' card readers, which prompt the user to insert and withdraw their card immediately before proceeding with the transaction. This helps reduce the incidence of consumers leaving their cards behind and is just one example of a safe alternative to automatic shut-down procedures.

220 In our view it is important that ATM operators employ adequate safety mechanisms for users, but we accept that flexibility is warranted for the particular methods employed. In the revised EFT Code a consumer will be liable for unauthorised transactions that occur because the consumer leaves a card in an active ATM, where the ATM satisfies adequate safety standards aimed at mitigating the risk of cards being left behind. This provision will apply in conjunction with the current liability allocation provisions in the EFT Code.

Book up

221 Book up is a common practice in remote Australian communities. It allows consumers to buy goods (usually groceries) on credit. Book up usually involves some form of security being left with the merchant until payment is made, such as consumers' bank cards. The practice has been abused by some merchants in the past, and it continues to be a concern today.

Proposal in CP 90

222 CP 90 proposed requiring subscribers to prohibit merchants in merchant agreements from taking consumers' PINs as part of book up practices: proposal E2.

Final position

223 The revised Code will require subscribers to prohibit merchants in merchant agreements from obtaining consumers' PINs, including as part of book up practices.

Rationale

224 Book up is credit offered by stores and other traders for the purchase of goods or services, and is commonly used in regional and remote areas of Australia. Most traders who offer book up hold the consumer's bank debit card as security, often with their PIN as well.

225 While we note that book up practices may be operated honestly and successfully in some communities, there is a high risk of abuse by merchants and this risk should be minimised.

226 The Ministerial Council on Consumer Affairs has made book up one of its national priority points for its 2010–2013 action plan. The Council's view is that the merchants should not hold consumer cards and PINs.[72]

227 All submissions that addressed this issue supported the proposal, although some argued that liability for any resulting unauthorised transactions should be placed on the merchants.[73] Clause 8.2 of the current EFT Code provides that a subscriber may not avoid liability by relying on the fact that they are party to a shared electronic funds transfer system and that another party (e.g. a merchant) has caused the liability. We do not propose to change this provision, and believe the matter can be addressed by subscribers through their merchant agreements.

Mistaken payments

228 Internet banking services allow consumers to use online banking to transfer funds between individuals ('Pay Anyone' transactions). Sometimes consumers transfer funds to the wrong person because they enter the wrong payment details or because they have been given the wrong account information. Recovery of mistakenly paid funds from the unintended recipients has been difficult.

229 The issue of how mistaken internet banking payments might be dealt with in the EFT Code has proven to be one of the most difficult to resolve in the current review.

230 Stakeholder feedback revealed concerns that were difficult to reconcile, in particular given that very little industry data is available on the extent and nature of mistaken payments. This lack of data about the size of the problem made it difficult to judge the real costs to industry of implementing system changes, as well as the real impact on consumers of not having a mistaken payments regime as one of the protections in the EFT Code. For example, there were dramatically different views on the issue of funds recovery and liability where there are insufficient funds in a recipient's account, but in the absence of data we were not able to accurately assess the true cost impact of allocating liability to either consumers or industry.

231 The proposals in this report represent significant compromises by all Mistaken Internet Payments Working Group members to accommodate each other's concerns and achieve a workable outcome for consumers and industry.

[72] Ministerial Council on Consumer Affairs, *Taking Action, Gaining Trust: A National Indigenous Consumer Strategy—Action Plan 2010–2013*, at 5.
[73] See, for example, Law Council of Australia, *Submission* (24 December 2008), p. 5.

Proposal in CP 90

232 CP 90 proposed that the EFT Code deal with the issue of mistaken payments, but did not contain a detailed proposal: proposal E3.

Final position

233 The revised EFT Code will deal with mistaken payments, in particular the obligations of Code subscribers in relation to recovery of funds and liability for mistaken payments.

234 We will monitor the effectiveness of the mistaken payment provisions in the EFT Code by collecting and analysing data about these payments with the help of industry stakeholders and EDR schemes.

235 There are five elements to our proposed regime for mistaken payments, being:

1 preventative measures;

2 recovery where there are sufficient funds;

3 recovery where there are *not* sufficient funds;

4 role of EDR schemes; and

5 administration of mistaken payments arrangements.

These elements are set out below, together with the rationale for each.

236 Where funds are still available in the unintended recipient's account, three funds recovery procedures can be applied by financial institutions depending on when a payer reports the mistaken payment to their financial institution. Where there are *insufficient* funds in the unintended recipient's account, financial institutions must employ reasonable endeavours in order to assist the fund recovery process. The procedures below reflect the compromise positions agreed to by stakeholders.

Definition and scope

237 A mistaken payment will be defined for EFT Code purposes as:

> a payment made by a consumer through a 'Pay Anyone' facility and processed by financial institutions through direct entry processes where funds are paid into the account of an unintended recipient because the consumer enters or selects a BSB number and/or account number that does not belong to the named and/or intended recipient as a result of:
>
> (a) the consumer's error; or
>
> (b) the consumers being advised of the wrong BSB number and/or account number.

238 Transactions performed using BPay will be exempt from the mistaken payments provisions of the EFT Code, as BPay currently has its own liability

allocation rules for losses caused by mistaken BPay payments. The BPay system uses a biller code and customer reference number, and when the biller code is entered the name of the linked biller is brought to the screen automatically, reducing the possibility of payment to the wrong entity. Where a consumer is not satisfied with the handling of a complaint about a BPay transaction they can go to an EDR scheme to have their complaint resolved.

1 Preventative measures

On-screen warnings

239 The revised Code will require prominent on-screen warnings about the risks associated with mistaken payments, namely that:

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

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

Warnings are to be delivered when the consumer is performing a transaction and before the transaction is finally confirmed.

Rationale

240 On-screen warnings, when properly designed and strategically placed, will help remind consumers of the risks of mistaken payments and encourage greater care in entering transaction details. These warnings should be explicit and should be delivered before the transaction is finally confirmed by the consumer.

Terms and conditions

241 Under the revised Code, terms and conditions for relevant electronic payment services should contain disclosure about mistaken payments and the processes prescribed in the Code. In particular, terms and conditions should clearly state the circumstances in which the financial institution will try to recover funds from an unintended recipient and the circumstances in which an account holder will be liable to bear the losses arising from mistaken payments.

Rationale

242 Product terms and conditions should state that mistaken payments will be resolved in accordance with EFT Code provisions. They should also clearly state the circumstances in which the financial institution will try to recover funds from an unintended recipient and the circumstances in which an account holder will be liable to bear the losses from mistaken payments.

BSB validation

243 We understand from submissions received that a small number of mistaken payments are caused by the use of incorrect BSB numbers. We are also aware of some instances where financial institutions only refer to account numbers and not BSB numbers when processing payments.

244 Financial institutions are currently only required to validate the first two digits of BSB numbers.

245 The Mistaken Internet Payments Working Group considered the possibility of a system whereby the financial institution would check all six digits of the BSB number entered by the consumer before processing the transaction and alert the consumer when the BSB number entered was invalid. The working group also considered requiring institutions to display the name of the bank and branch that corresponded to a valid BSB number, so that consumers could confirm these details before proceeding with a transaction.

246 The Mistaken Internet Payments Working Group discussions noted that six-digit BSB validation could potentially stop a payment with invalid BSB details (i.e. a non-existent bank branch), but would not stop a payment where an incorrect but otherwise valid BSB number was used. It was also suggested that BSB details of the branch at which a consumer initially opened their account might not be known to those making payments into that account.

247 Industry also stressed that significant system changes would be required for financial institutions to perform six-digit BSB validations against APCA's directory list.

248 In our view, requiring six-digit BSB validation is not currently justified given the potential expense of the system changes required, the lack of comprehensive data about the extent of the problem and uncertainty about the extent to which it would actually prevent mistaken payments. We will ask APCA to collect data about mistaken payments caused by incorrect BSB numbers.

2 Recovery where funds are available in the account

249 Stakeholders have agreed to a three-part process for the recovery of mistaken payments where there *are* sufficient funds in the recipient's account.

250 Based on discussions with the Mistaken Internet Payments Working Group, we accept that different recovery procedures are required to address the various circumstances in which a mistaken payment claim is brought to a financial institution, both in terms of timing of the claim and whether there are sufficient funds available in the recipient's account to reimburse the payer.

251 The paragraphs below summarise the policy positions for the recovery of funds in three general circumstances, following a determination by the financial institution that a mistaken payment has occurred. The procedures for each recovery process are detailed in Appendix 5.

Transactions reported within 12 business days

252 Under the revised Code, where the payer notifies their financial institution of a mistaken payment within 12 business days, the financial institutions[74] will assess whether there has been a mistaken payment and, if there *are* funds in the recipient's account, the mistaken payment will be repaid in full.

Rationale

253 When a mistake is reported within 12 days of the transaction of the mistaken payment being made, it is more likely that funds will still be in the recipient's account and will thus be easier to recover.

Transactions reported between 12 business days and seven months

254 Under the revised Code, where the payer reports a mistaken payment between 12 business days and seven months, the financial institutions will assess whether there has been a mistaken payment, the disputed monies will be placed on hold and the recipient will be given 10 business days to prove they are entitled to the payment. If they cannot do so, the funds will be returned to the payer.

Rationale

255 We believe this approach adequately addresses the rights of both the sender and unintended recipient, particularly where the financial institutions' investigations already suggest a mistaken payment has occurred. We understand that a number of financial institutions have already adopted a similar approach and we support this.

256 The seven-month period is based on the longest statement period in the market—currently six months—plus one month for consumers to check their statements. While there will always be outliers, in our view most mistakes will be identified within this period.

Transactions reported later than seven months

257 If the payer reports the mistake after the seven-month period, the existing BECS return request procedures will apply and the consent of the unintended recipient would have to be obtained before the funds can be recovered.[75]

[74] Both sending and receiving financial institutions will make an assessment of whether there has been a mistaken payment.
[75] We understand the BECS return request procedures will be made publicly available.

Interaction with Code of Operation for Centrelink Direct Credit Payment

258 Where the Code of Operation for Centrelink Direct Credit Payment[76] applies, the mistaken payment amount will be recovered in accordance with that Code.

Rationale

259 There may be circumstances where it is not appropriate to process a request for the return of funds even if there are funds in the account. For example, where an unintended recipient relies on social security benefits as their only source of income, having a large amount of money taken out of their account in one transaction might put them into financial difficulty.

260 Where such a situation is identified by the receiving financial institution, mistaken payment amounts should be recovered in accordance with the procedures set out in the Code of Operation for Centrelink Direct Credit Payment, which stipulates that financial institutions will use only 10% of each regular Centrelink payment to repay the money owed by the unintended recipient, unless the unintended recipient agrees to pay more.

3 Recovery where funds *are not* available in the account

261 Under the revised Code, where there are insufficient funds in the account to enable full return of the mistakenly paid funds:

(a) the receiving financial institution must use its reasonable endeavours to retrieve the funds for return to the payer (e.g. by facilitating repayment by instalments); and

(b) where the funds cannot be recovered despite the sending and receiving financial institutions' reasonable endeavours, it will be up to the payer to privately pursue recovery of the funds.

Rationale

262 In our view, where there is insufficient money in the unintended recipient's account, the recipient's consent should be obtained to the funds being returned and the receiving financial institution should use its reasonable endeavours to retrieve the funds for return to the payer.

263 The receiving financial institution has the responsibility for making the arrangements to return the funds to the payer because it has an existing contractual relationship with the unintended recipient, making it the party with the best chance of retrieving the mistakenly paid funds.

[76] Available at www.centrelink.gov.au.

264 The receiving financial institution should have some flexibility about how they can facilitate such return—for example, through use of instalment payments.

265 The question of liability in cases where funds *cannot* be recovered has been central to our consultation on mistaken payments. Opinion is divided on whether liability ought to rest with:

(a) the payer, as the party who made the mistake; or

(b) 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.

266 For the subset of cases where there are insufficient funds in the recipient's account to enable repayment and the reasonable endeavours of the financial institutions are not able to recover the funds, the working group was unable to reach consensus on the issue of liability. For the time being, in these cases it will be up to the payer to privately pursue recovery of the funds.

267 We will monitor the appropriateness of this liability arrangement through collection of data on the incidence of mistaken payments and the effectiveness of funds recovery procedures.

4 Role of EDR schemes

268 Where a financial institution concludes that a mistaken payment has not occurred, it is not required to treat the situation as a mistaken payment. If the consumer is not satisfied with this outcome, they can complain to the sending financial institution's EDR scheme.

269 The EDR scheme may hear a case brought by a payer in circumstances where there is no direct relationship between the payer and the receiving financial institution, provided that the receiving financial institution consents.

270 EDR schemes will issue guidance to clarify that a financial institution can reverse a mistaken payment without the consent of an unintended recipient.

Rationale

271 A consumer who has made a mistaken payment is unlikely to know the identity of the person who receives the funds, or in many cases the name of the receiving financial institution where the recipient holds an account.

272 It is preferable that, where a payer has a complaint, they bring it to their own financial institution and, if necessary, that institution's EDR scheme. Because the payer has an existing relationship with this financial institution, any investigation conducted in relation to the mistaken payment will be

facilitated by virtue of the existing privacy agreement between the payer and the institution.

273 This approach will assist the receiving financial institution in that it will enable enquiries to be streamlined using established channels of communication between financial institutions, rather than requiring the receiving financial institution to deal with individuals with whom it will typically have no contractual relationship.

274 In our view, when a transaction is proved to be mistaken and the unintended recipient fails to substantiate their entitlement to the payment, a financial institution should be able to reverse the transaction without the account holder's consent, to restore the sender's rights to the payment. Members of the Mistaken Internet Payments Working Group supported this view. We expect EDR schemes to make necessary arrangements to implement this approach.

5 Administration of mistaken payment arrangements

Notification

275 Subscribers should have a clear and accessible process for all consumers to report mistaken payments. The process will not be prescribed in the Code. The benefits of a clear and accessible process for consumers to report mistaken payments are self-evident.

Time for response by receiving financial institution

276 Receiving financial institutions should at least acknowledge a mistaken payment query within five business days.

277 In our view, five business days is a reasonable time for a receiving financial institution to acknowledge a return request by a sending financial institution and, depending on the circumstances of the case, to advise the sending financial institution of the attempt(s) made to contact the unintended recipient.

Data collection

278 Mistaken payments data will be collected within two years of the implementation of the revised Code for at least a three-month period with the assistance of industry association bodies, APCA and EDR schemes. In our view the data to be collected should include:

(a) number and value of mistaken payments;

(b) causes of mistaken payments, in particular, how many are due to:

(i) a consumer being given the wrong account details;

(ii) a consumer entering the wrong account number;

(iii) a consumer entering the wrong BSB number; or

(iv) a consumer entering a wrong BSB number but a valid account number, which results in the payment being sent to an existing account number at the wrong institution;

(c) time taken by consumers to report mistaken payments;

(d) number and value of mistaken payments recovered:

(i) using mistaken payment return request procedures when the transactions are reported within 12 business days;

(ii) using mistaken payment return request procedures when the transactions are reported between 12 business days and seven months;

(iii) using the existing return request procedures; and

(iv) with consent of unintended recipients where there are insufficient funds in the account;

(e) number and value of mistaken payments not recovered;

(f) number of mistaken payments claims involving a Centrelink account (either as sender or recipient); and

(g) number and value of fees and/or charges applied by financial institution for processing mistaken payments claims.

279 We will work with stakeholders to determine the details of data to be collected and the feasibility of such collection.

280 One of the challenges in analysing issues relating to mistaken payments has been a lack of comprehensive data on the extent of the problem, the causes of mistaken payments and the effectiveness of current channels used to recover them.

281 Having reliable data will help us monitor the effectiveness of the procedures set out in the Code and make amendments as required.

Transition period

282 We will consult stakeholders to negotiate a reasonable and realistic timeframe for implementation of these proposals, as well as monitor the progress of their implementation.

283 We are aware that our positions on mistaken payments will require subscribers to the Code to undertake some systems changes, which may take longer to implement than other changes coming from this review.

H Administration and review

Key points

The revised EFT Code will:

- give ASIC a general power to modify the application of the Code to a product or class of products, subject to the principles of procedural fairness;
- provide that the Code must be reviewed every five years;
- require subscribers to provide ASIC or its delegate with data on unauthorised transactions; and
- require ASIC or its delegate to monitor compliance with specific EFT Code requirements.

Modifying the EFT Code

284 The EFT Code currently gives us limited powers to modify the application of specific provisions of the Code.[77] We think a general power to modify the application of the EFT Code as it applies to particular products or classes of products would enhance the flexibility and responsiveness of the EFT Code to industry developments.

Proposal in CP 90

285 CP 90 proposed that we should have a general power to modify the EFT Code as it applies to a product or class of products, subject to the principles of procedural fairness: proposal G1.

Final position

286 Under the revised Code, we will have a general power to modify the EFT Code as it applies to a product or class of products. This general power could be exercised either upon application by stakeholders or on our own initiative. We will apply the principles of procedural fairness and publish any modifications made to the Code. Subscribers to the Code are bound to comply with the Code as modified by ASIC from time to time.

[77] EFT Code, cl 23.3

Rationale

287 This proposal was supported by almost all submissions that addressed the issue,[78] although some qualified their support by adding that any modifications must be subject to prior consultation with stakeholders. In our view the principles of procedural fairness, in particular the fair hearing and no bias principles, already require stakeholder consultation before any modification can be made to the Code. We will clarify in the revised Code the requirement that we consult with our stakeholders before any modifications can be made to the Code.[79] We will balance the need to consult and publicise modifications with any stakeholder confidentiality concerns.

Periodic reviews of the Code

288 Currently we are required to undertake periodic review of the EFT Code: cl 24.1. We consider it appropriate that the frequency of the Code reviews be specified.

Proposal in CP 90

289 CP 90 proposed that the EFT Code be reviewed every five years: proposal G2.

Final position

290 The revised Code will provide that the Code must be reviewed five years following the conclusion of each preceding review.

Rationale

291 A number of submissions disagreed with the proposed timeframe, submitting, in particular, that five yearly reviews were not sufficiently frequent and that, for example, three years was more appropriate.[80] Others submitted that the quality of overall consultation between ASIC and industry stakeholders was more important than the timeframe, and suggested using an independent reviewer as an alternative to ASIC.[81] However, most

[78] Australian Bankers' Association, *Submission* (21 December 2008), p. 31; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 8; Australian Payments Clearing Association, *Submission* (5 December 2008), p. 8; Law Council of Australia, *Submission* (24 December 2008), p. 7; Legal Aid Queensland, *Submission* (12 December 2008), p. 9; ANZ, *Submission* (19 December 2008), p. 11; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 18; Financial Ombudsman Service, *Submission* (9 December 2008), p. 18. PIF Australia, *Submission* (12 December 2008), p. 21.
[79] We will also apply the principles of best-practice regulation and regulatory assessment requirements, which include the assessment of risk analysis, cost-benefit analysis, assessments of compliance costs and competition effects, and consultation.
[80] Law Council of Australia, *Submission* (24 December 2008), p. 8.
[81] See, for example, Australian Payments Clearing Association, *Submission* (5 December 2008), p. 8.

submissions[82] supported a review every five years, some noting that three yearly reviews do not allow sufficient time and are impractical and costly.[83]

292 We agree with the majority that five yearly reviews are appropriate. Should a particular issue need to be addressed in the Code during the period between reviews, we will use our general power to modify the Code, subject to procedural fairness principles: see paragraphs 284–287.

Monitoring compliance

293 In the past, Code subscribers were required to fill out self-assessment surveys to report on their compliance with every clause of the EFT Code, and to report on aggregated transaction and complaints data.

294 The exercise imposed a significant compliance burden on subscribers and the data collected was difficult to analyse as subscribers have different system capabilities to extract and report transactions and complaints data.

295 It would be a better use of subscribers' resources if compliance monitoring were focused on specific areas. From our perspective the most important information we can collect for EFT Code compliance purposes is regular statistical data on unauthorised transactions. Additional specific compliance monitoring activities will be determined in consultation with subscribers and other stakeholders as the need arises.

Unauthorised transactions

Proposal in CP 90

296 CP 90 proposed that subscribers be required to give us the following information about unauthorised transactions:

(a) the number of unauthorised transactions;

(b) information about the channels used to perform unauthorised transactions; and

(c) data about how disputes about unauthorised transactions were resolved.

297 Subscribers should be required to provide this data annually: proposal G3.

[82] Coles, *Submission* (8 December 2008), p. 8; Australian Bankers' Association, *Submission* (21 December 2008), p. 32; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 8; ANZ, *Submission* (19 December 2008), p. 10; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 18; Financial Ombudsman Service, *Submission* (9 December 2008), p. 18; PIF Australia, *Submission* (12 December 2008), p. 22.
[83] Australian Bankers' Association, *Submission* (21 December 2008), p. 32; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 8.

Final position

298 Under the revised Code, subscribers will be required to give ASIC or its delegate the following information about unauthorised transactions:

(a) the number and value of unauthorised transactions;

(b) information about the channels used to perform unauthorised transactions; and

(c) data about how disputes about unauthorised transactions were resolved, outcomes and average timeframes for these resolutions.

Subscribers should be required to provide this data annually.

Rationale

299 Few submissions addressed this proposal.

300 A number of submissions raised the difficulties for effective compliance reporting caused by the different interpretations of 'unauthorised transactions' currently used by EFT Code subscribers.[84] This lack of consistency risks the data captured being of little value for comparison. Clause 5.1 of the current EFT Code defines unauthorised transactions as transactions which are not authorised by the user, but does not apply to transactions carried out by the user or by anyone performing a transaction with the user's knowledge and consent.

301 We will work with Code subscribers, industry representatives and EDR schemes to examine the interpretations currently used to capture unauthorised transactions data and, if needed, issue guidance to clarify and improve comparability of that data.

Ongoing compliance monitoring

Proposal in CP 90

302 CP 90 proposed that we monitor compliance with specific EFT Code requirements. This would replace the current arrangements, which require subscribers to self-report on compliance with every obligation under the EFT Code. The focus of this compliance monitoring would be targeted and might change over time. Subscribers might be required to report information about other specific requirements as part of this targeted compliance monitoring. We might also use other monitoring mechanisms such as shadow shopping exercises: proposal G4.

[84] Australian Bankers' Association, *Submission* (21 December 2008), p. 32; ANZ, *Submission* (19 December 2008), p. 11.

Final position

303 Under the revised Code, ASIC or its delegate will monitor compliance with specific EFT Code requirements. This will replace the current arrangements, which require subscribers to self-report on compliance with every obligation under the EFT Code. The focus of this compliance monitoring will be targeted and may change over time. Subscribers may be required to report information about other specific requirements as part of this targeted compliance monitoring.

Rationale

304 There was universal support among all submissions that addressed this issue for a targeted approach to compliance monitoring.[85] Supplementary suggestions included the use of an issues-based survey with qualitative responses where necessary, improved communication by ASIC to Code subscribers about any proposed monitoring focus throughout the year,[86] the collection and analysis of consumer case studies from casework agencies[87]and the use of complaints data collected by EDR schemes.[88]

305 We are exploring the possibility of improving our Code monitoring function by engaging an appropriate delegate to take on the monitoring and review role.

[85] Coles, *Submission* (8 December 2008), p. 8; Legal Aid Queensland, *Submission* (12 December 2008), p. 9; Australian Bankers' Association, *Submission* (21 December 2008), p. 32; Abacus Australian Mutuals, *Submission* (24 December 2008), p. 9; Australian Compliance Institute, *Submission* (4 December 2008), p. 8; ANZ *Submission*, p. 11; *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 19; Financial Ombudsman Service, *Submission* (9 December 2008), p. 19; Law Council of Australia, *Submission* (24 December 2008), p. 8.
[86] Abacus Australian Mutuals, *Submission* (24 December 2008), p. 9.
[87] *Joint submission* by CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia (24 December 2008), p. 19.
[88] Abacus Australian Mutuals, *Submission* (24 December 2008), p. 9.

Appendix 1: List of non-confidential submissions to CP 90

Table 2: List of non-confidential submissions

Submission	Date Received
Abacus Australian Mutuals	24 December 2008
ANZ	19 December 2008
Australasian Compliance Institute	4 December 2008
Australian Bankers' Association	21 December 2008
Australian Payments Clearing Association	5 December 2008
Australian Payments Clearing Association—supplementary submission	31 March 2009
BPay	25 November 2008
CHOICE, Consumer Action Law Centre and Consumers' Federation of Australia	24 December 2008
Coles	8 December 2008
Financial Ombudsman Service	9 December 2008
HSBC Bank Australia	5 December 2008
Kirsten Livermore MP (Member for Capricornia)	7 April 2009
Law Council of Australia	24 December 2008
Legal Aid Queensland	12 December 2008
National Independent Retailers Association	9 December 2008
PIF Australia	12 December 2008
Small Business Development Corporation	11 December 2008
Universal Gift Cards	19 December 2008
Westfield	5 December 2008
Woolworths Limited	25 May 2009

Appendix 2: Working groups

Members of the EFT Code Working Group

- ASIC (chair)
- Abacus Australian Mutuals
- Australian Bankers' Association
- Australian Finance Conference
- Australian Mobile Telecommunication Association
- Australian Payments Clearing Association
- Centre for Credit and Consumer Law
- Consumer Action Law Centre
- Department of Communications, Information Technology and the Arts
- Financial Ombudsman Service
- Galexia (on behalf of CHOICE and Consumers' Federation of Australia)
- Telecommunications Industry Ombudsman
- Treasury

Members of the Mistaken Internet Payments Working Group

- ASIC (chair)
- Abacus Australian Mutuals
- Australian Bankers' Association
- Australian Finance Conference
- Australian Payments Clearing Association
- Consumer Action Law Centre
- Financial Ombudsman Service
- Galexia (on behalf of CHOICE and Consumers' Federation of Australia)
- Law Council of Australia, e-Commerce Committee

Appendix 3: Overseas treatment of emerging electronic payment products

Table 3: Overseas treatment of emerging electronic payment products

Country	Instrument	Scope and related requirements
Canada	EFT Code of Practice (due to be released)	Not available yet. The development of the EFT Code of Practice is now on hold due to competing priorities. The new code will replace the Canadian Debit Card Code and cover all types of electronic payment methods.
European Union	E-Money Directive (Directive 2009/110/EC)[89]	The E-Money Directive defines 'electronic money' as monetary value stored electronically (including magnetically) for making payment transactions, which is accepted by third parties.
	Payment Services Directive (Directive 2007/64/EC)[90]	Electronic money products and issuers are regulated by the Payment Services Directive. This directive provides a light-touch regime for 'low-value payment instruments and electronic money' or products that store no more than €150 so that the issuers: • only need to provide information about the main characteristics of the payment service; • give only a reference to enable identification of payment transaction, the transaction amount and any charges; • have options of not providing consumers with the means to notify the loss, theft or misappropriation of product, or the ability to block further use; and • may let the user bear financial loss resulting from any loss, theft or misappropriation of the product if the issuer does not have the ability to block its further use.
United Kingdom	*Financial Services and Markets Act 2000* (FSMA)	The FSMA defines electronic money as monetary value that is stored on an electronic device, issued on funds receipts, and accepted as payment means by persons other than the issuer as a surrogate for coins and banknotes.

[89] Available at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0110:EN:NOT
[90] Available at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:en:HTML

Country	Instrument	Scope and related requirements
	Payment Services Regulations 2009 (No. 209) (PSR)[91]	The PSR imposes business conduct requirements on all payment service providers, but applies lighter requirements for 'low-value payment instruments'. For products that store no more than €500: • issuers only need provide consumers with information about the payment service's main characteristics; • issuers may provide consumers with simplified references to identify the transaction, the amount and any charges relating to the transaction; and • for anonymous products, issuers must give consumers the means to check the amount of funds stored.
United States	Electronic Funds Transfer (Regulation E)[92]	Regulation E defines electronic fund transfer as any transfer initiated through an electronic terminal, telephone, computer or magnetic tape. It applies to point of sale transfers, ATM transfers, direct deposit or fund withdrawals, telephone transfers and debit card transactions. In November 2009, the US Federal Reserve Board proposed amending Regulation E to implement gift card provisions of the *Credit Card Accountability Responsibility and Disclosure Act 2009* to gift certificates, store gift cards and general use prepaid cards. The proposals provide that: • the use of dormancy fees on gift cards, subject to certain conditions, is prohibited; and • the expiry date must be at least 5 years after the date of card issuance, or 5 years after the date when funds were last loaded.
Hong Kong	Hong Kong Code of Banking Practice (HK Banking Code)[93]	The HK Banking Code contains requirements for disclosure, notification of changes to terms and conditions, and fees and charges, receipts and transaction history, for stored value cards issued by banking institutions. General Banking Code requirements also apply where relevant, e.g. where a stored value card can be used as an ATM card.
	Banking Ordinance[94]	Non-bank card issuers of multi-purpose stored value cards are subject to the licensing requirements under the Banking Ordinance and the supervision of the Hong Kong Monetary Authority (HKMA). The HKMA encourages the industry to adopt a self-regulatory regime.
	Code of Practice for Multi-purpose Stored Value Card Operation[95]	The Code of Practice for Multi-purpose Stored Value Card Operation was issued by Octopus Cards Limited, the system operator of Octopus cards. It is a voluntary industry code that employs a very high level principles-based approach to regulating multi-purpose stored value cards.

[91] Available at www.hm-treasury.gov.uk/d/si_payment_services_regulations100209.
[92] Available at www.federalreserve.gov/bankinforeg/reglisting.htm#E.
[93] Available at www.hkab.org.hk/DisplayArticleAction.do?sid=5&ss=3.
[94] Available at www.legislation.gov.hk/blis_ind.nsf/WebView?OpenAgent&vwpg=CurAllEngDoc*155*0*155#155.
[95] Available at www.info.gov.hk/hkma/eng/bank/value_cards/code_of_practice_OCL_.pdf.

Appendix 4: Notification requirements in industry codes and legislations

Table 4: Comparison of requirements of Code of Banking Practice and Mutual Banking Code of Practice

	Code of Banking Practice	Mutual Banking Code of Practice
1. Changes to certain terms and conditions	Changes to: (a) introduce a fee or charge (excludes government charges); (b) vary the minimum balance to which an account keeping fee applies; (c) vary the method by which interest is calculated; (d) vary the balance ranges within which interest rates apply to a deposit account; or (e) vary the frequency with which interest is debited or credited.	Changes to: (a) introduce a new fee or charge; (b) increase a fee or charge; (c) reduce the number of fee-free transactions permitted on an account; (d) vary the minimum balance to which an account keeping fee applies; (e) vary the method by which interest on an account is calculated; or (f) vary the circumstances when interest is credited or debited from an account.
Notification period	Notification of changes must be provided 30 days before the changes take effect.	Notification of changes must be provided 20 days before the changes take effect.
Notification methods	By written notice.	Notification may be provided on or with a customer's account statement, by letter, subscribers' newsletter or website, or advertisement in the media.[96]
2. Changes to the interest rate	Notification must be made no later than the day on which the variation takes effect. It can be made by advertisement in the national or local media or in writing.	Notification must be provided no later than the day on which the change takes effect. It may be provided on or with a customer's account statement, by letter, subscribers' newsletter or website, or advertisement in the media.
3. Other changes to terms and conditions	Notification must be made available by advertisement in the national or local media or in writing, no later than the day on which the variation takes effect.	Notification will be made at the next communication with the customer.

[96] Mutual Banking Code of Practice, s17.

Table 5: Comparison of notification requirements under legislation

Corporations Act	Issuers must notify retail clients of material changes to regulated products, in writing, electronically or by other means specified in the regulations. Thirty days advance notice is required for a change that is an increase in a fee or charge.[97]
National Credit Code[98]	Notification in writing of a change to the amount, frequency or time for payment of a credit fee or charge (including a new credit fee or charge) must be given no later than 20 days before the change takes effect.[99]

[97] Section 1017B(5) of the Corporations Act.
[98] Schedule 1 of the National Credit Act.
[99] National Credit Code, s64–68.

Appendix 5: Recovery procedures where funds are available in the account

Table 6: Recovery procedures where funds are available in the account

Reporting period	Procedures
Mistaken payments reported within 12 business day of the transaction (see paragraphs 252–253)	The revised Code will provide that: • the sending financial institution will investigate and determine whether a claim is a mistaken payment; • once satisfied a mistaken payment has occurred, the sending financial institution will send a request for the return of the funds to the receiving financial institution; • the receiving financial institution will determine whether the request is a mistaken payment; and • the receiving financial institution will recover the funds from its customer's account and return them to the payer via the sending financial institution within 5 business days of receiving the request.
Mistaken payments reported between 12 business days and 7 months of the transaction (see paragraphs 254–256)	The revised Code will provide that: • the sending financial institution will investigate and determine whether a claim is a mistaken payment; • once satisfied that a mistaken payment has occurred, the sending financial institution will send a request for return of the funds to the receiving financial institution; • the receiving financial institution will determine whether the request is a mistaken payment within 10 business days of receiving the request and put a hold on the funds for up to 10 further business days; • the receiving financial institution will notify the unintended recipient that it believes a mistaken payment has been made to their account and that it will reverse the transaction if no substantiated claim to the payment is made within 10 business days; and • if no substantiated claim is received within 10 business days, the receiving financial institution will recover the funds and return them to the payer via the sending financial institution within 2 business days after the 10 business day period when the funds are put on hold.
Mistaken payments reported after 7 months of the transaction (see paragraph 257)	The revised Code will provide that the existing BECS return request procedures will apply and the consent of an unintended recipient would have to be obtained before the funds can be recovered. Where BECS return request procedures are used, the sending financial institution will ask the receiving financial institution to seek the consent of the unintended recipient to return the funds by completing a Request for Return of Item(s) Sent in Error form. This option is also appropriate where an error is not completely clear on the face of the documents, and gives the unintended recipient an opportunity to refuse the return of funds. There is no time limit relating to use of BECS return request procedures.

Key terms

Term	Meaning in this document
AML Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
APCA	Australian Payments Clearing Association
ASIC	Australian Securities and Investments Commission
BECS	Bulk Electronic Clearing System
BSB	A unique number that identifies both the financial institution and the point of representation of a particular account in Australia
[CO 05/736] (for example)	An ASIC class order (in this example numbered 05/736)
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
CP 90 (for example)	An ASIC consultation paper (in this example numbered 90)
EDR scheme (or scheme)	An external dispute resolution scheme approved by ASIC under the Corporations Act (see s912A(2)(b) and 1017G(2)(b)) and/or the National Credit Act (see s11(1)(a)) in accordance with our requirements in RG 139
EFT Code (or the Code)	Electronic Funds Transfer Code of Conduct
FOS	Financial Ombudsman Service—an ASIC-approved EDR scheme
National Credit Act	*National Consumer Credit Protection Act 2009*
National Credit Code	National Credit Code at Schedule 1 of the National Credit Act
RG 183 (for example)	An ASIC regulatory guide (in this example numbered 183)