ASIC
Australian Securities & Investments Commission

CONSULTATION PAPER 90

Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC proposals

October 2008

About this paper

This paper sets out proposals for changes to the Electronic Funds Transfer (EFT) Code of Conduct based on a review of the Code by the Australian Securities and Investments Commission (ASIC).

About ASIC regulatory documents

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

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

Regulatory guides: give guidance to regulated entities by:

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

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

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

Document history

This paper was issued on 3 October 2008 and is based on the Corporations Act as at 31 July 2008.

Disclaimer

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

Contents

The consultation process

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

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

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

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

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

Your comments will help us develop our approach to reviewing the EFT Code. In particular, any information about compliance costs, impacts on competition and other impacts, costs and benefits will be taken into account if we prepare a Business Cost Calculator Report and/or a Regulation Impact Statement: see Section H Regulatory and financial impact.

Making a submission

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

Comments should be sent by 5 December 2008 to:

Delia Rickard
Acting Executive Director, Consumer Protection and International
Australian Securities and Investments Commission
GPO Box 9827
Canberra ACT 2600
email: eftreview@asic.gov.au

What will happen next?

Stage 1	3 October 2008	ASIC consultation paper released
Stage 2	5 December 2008	Comments due on the consultation paper
Stage 3	Early 2009	Final report released
Stage 4	Mid 2009	Revised EFT Code released

A Background to the proposals

Key points

The Electronic Funds Transfer Code of Conduct (EFT Code) is a voluntary industry code of practice that provides a range of protections for consumer electronic payments.

Since the last review of the EFT Code, there have been significant developments in the marketplace for electronic payments, online fraud and the regulation of electronic payments.

This consultation paper contains proposals relating to:

- the structure, scope and interpretation of the EFT Code
- the disclosure and complaints handling requirements
- the rules on liability for unauthorised transactions and mistaken payments
- the treatment of electronic communications, and
- ASIC's power to modify the EFT Code and our obligation to periodically review it.

About the EFT Code

1 The Electronic Funds Transfer Code of Conduct (EFT Code) is a voluntary industry code of practice covering consumer electronic transactions. It covers:

- ATM and EFTPOS transactions;
- credit and debit card transactions including transactions intended to be authorised by entering a PIN or by signing an electronic tablet (but not transactions intended to be authorised by manual signature);
- telephone and online banking, including bill payment and 'pay anyone' facilities;
- stored value cards; and
- digital cash products.

2 The EFT Code provides protection for consumers in the following areas:

- disclosure of terms and conditions, fees, receipts and statements;
- dispute resolution procedures; and
- liability allocation where there is a dispute about an unauthorised transaction.

Table 1 on the next page lists current subscribers to the EFT Code.

Table 1: Current subscribers to the EFT Code[1]

- Almost all banks, building societies and credit unions that offer electronic banking facilities
- ABB Grain Ltd
- American Express International
- Baptist Investments and Finance Ltd
- Bluestone Servicing Pty Limited
- Collins Securities Pty Ltd
- Columbus Capital Pty Limited
- First Data Resources Australia
- GE Capital Finance Australia
- Landmark Operations Limited
- LinkLoan Services Pty Limited
- Money Switch Limited
- Pioneer Mortgage Services
- Prime Mortgage Group Ltd
- RESIMAC Limited
- Rural Finance Corporation of Victoria
- Technocash
- The Territory Insurance Office

The review process

3 ASIC administers the EFT Code and is required to periodically review it: clause 24.1(a). The last review was completed in 2001.

4 In January 2007, ASIC released a consultation paper, *Reviewing the EFT Code* (January Consultation Paper). The January Consultation Paper identified a range of issues. We received over 40 public submissions from consumers and consumer bodies, financial services providers, industry bodies, businesses, lawyers, academics, law enforcement bodies, government agencies and experts in online fraud. Appendix 1 of this consultation paper lists non-confidential submissions. We also received a number of confidential submissions.

5 In August 2007, ASIC convened a working group to help us with the review. This paper was developed in consultation with the working group and contains a number of specific proposals for changes to the EFT Code. ASIC will develop its final recommendations over the coming months with further assistance from the working group, taking into account the submissions received in response to this consultation paper. Table 2 lists the members of the working group.

[1] Until recently, all retail institutions that offered electronic banking services were members of the EFT Code. ASIC is currently doing an audit of membership and has identified a very small number of institutions who are not members of the code. We are presently following this issue up with each of the institutions involved as we believe the protections in the code are part of the fundamental consumer protection framework for electronic banking.

Table 2: 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 • Banking and Financial Services Ombudsman (now Financial Ombudsman Service) • Centre for Credit and Consumer Law • Consumer Action Law Centre	• Department of Communications, Information Technology and the Arts • Telecommunications Industry Ombudsman • Treasury

How has the environment changed?

6 Since the last review of the EFT Code was completed in 2001, there have been significant changes in:

- the marketplace for electronic payments;
- the extent and nature of online fraud; and
- the regulatory environment.

Marketplace developments

7 Since the last review, the use of electronic payments has increased, especially internet banking, online bill payments, direct debit and direct credit. A number of new electronic payment products, offered by organisations that are not traditional financial services providers, have entered the market (e.g. prepaid electronic gift cards and online payments products). Section 2 of the January Consultation Paper discussed these developments.

8 Submissions to the January Consultation Paper also noted the proposed introduction of PIN@POS for credit card transactions. This initiative was launched on 4 June 2008. It involves consumers having the option to use a PIN rather than a manual signature for credit card transactions.

9 As noted in paragraph 1 of this paper, credit card transactions authorised by a manual signature are not covered by the EFT Code.[2] Credit card transactions authorised by a PIN under PIN@POS are covered by the EFT Code.[3] Therefore, PIN@POS will result in a significant expansion of the coverage of the EFT Code.

10 Submissions to the January Consultation Paper also noted the development of non-contact payment mechanisms offered by financial services providers and other organisations, including telecommunications and transit providers.

[2] This is because the EFT Code covers transactions that, among other things, are initiated by an 'access method': clause 1.1(a). Manual signature authorisation is not an 'access method': clause 1.5(c).
[3] This is because authorisation using a PIN is an 'access method': clause 1.5(a) and (b).

Online fraud

11 Since the last review, online fraud has become more common, increasingly sophisticated and constantly evolving in response to counter-fraud security measures. However, the level of online fraud is relatively contained compared to other forms of fraud. Section 3 of the January Consultation Paper discussed these developments.

12 According to submissions, most consumers have a low level of understanding of the risks of online fraud, and poor fraud detection and mitigation skills. There are also significant limitations on the ability of technology to prevent online fraud, which often involves organised crime and is trans-jurisdictional, making it hard to police.[4]

13 Financial institutions have responded to online fraud by introducing a range of anti-fraud measures. Submissions identified a range of measures, including improved authentication technology and fraud detection measures. Several submissions highlighted the need to constantly update technological responses to online fraud.[5] The joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre included a detailed appendix on authentication technologies.[6]

Regulatory developments

14 Since the last review, there have been significant developments in the regulation of electronic transactions. Section 4 of the January Consultation Paper discussed some domestic regulatory developments, including:

- Chapter 7 of the *Corporations Act 2001* (Corporations Act), introduced as part of the financial services reforms in 2002;
- the significant revision of the Code of Banking Practice in 2003 and the commencement of a further review of the Code;[7]
- work on revising the Code of Practice for credit unions and building societies by Abacus[8];

[4] Law Council of Australia, *Submission* (27 April 2007) at 2; P Hobson, *Submission* (1 May 2007) at 2; Australian Competition and Consumer Commission, *Submission* (24 April 2007) at 2–3; Consumers Telecommunications Network, *Submission* (13 April 2007) at 2; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 13–14; Australian Bankers Association, *Submission* (6 June 2007) at 7–8; Suncorp, *Submission* (1 May 2007) at 9; Abacus, *Submission* (25 June 2007) at 9.

[5] AusCERT, *Submission* (30 April 2007) at 8; Bendigo Bank, *Submission* (27 April 2007) at 2; Suncorp, *Submission* (1 May 2007) at 2; ANZ, *Submission* (2 May 2007) at 3; Australian Bankers Association, *Submission* (6 June 2007) at 9–10

[6] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007)), Appendix 1.

[7] The review is being conducted by Jan McClelland and Associates. An Issues Paper was released in May 2008. It is available at www.reviewbankcode2.com.au.

[8] Abacus released a draft revised Code of Practice for public comment in November 2007. The final draft Mutuals Code of Practice was released in April 2008. The Code is expected to be completed in late 2008 and come into effect in June 2009. A copy of the final draft can be accessed at http://www.abacus.org.au/media_centre/code_of_practice/docs/code_of_practice_final_draft_april08.pdf

- payments systems reforms implemented by the Reserve Bank of Australia; and
- regulation of purchased payment facilities by the Australian Prudential Regulatory Authority;
- the release of an ASIC consultation paper on the use of electronic communication to facilitate disclosure of financial services information under Chapter 7 of the Corporations Act.[9]

Appendix 2 of this consultation paper summarises developments in the international regulatory environment since 2007.

15 Submissions to the January Consultation Paper noted a number of other regulatory developments, including:

- the Simpler Regulatory System proposals announced by the Parliamentary Secretary to the Treasurer in November 2006;
- the development of a potential National Electronic Conveyancing System;
- self-regulatory frameworks for mainstream electronic payments channels (e.g. card scheme rules);
- the Australian Law Reform Commission's review of privacy laws; and
- the Productivity Commission review of consumer policy.[10]

Proposals in this paper

16 This consultation paper picks up and expands on some of the proposals in the January Consultation Paper for further feedback: see Table 3. There are some proposals from the January Consultation Paper we are not proposing to follow up. These are discussed in the relevant section under 'Other issues'.

Table 3: Summary of proposals in this paper

Section/Topic	Proposals in this section
Section B: Structure, scope and membership of the EFT Code	ASIC proposes to: • include a statement of objectives in the EFT Code (see proposal B1); • replace the current two-part EFT Code (which has a tailored regime for stored value facilities in Part B) with a one-part structure, with tailored requirements for certain products (see proposals B2 and B4);

[9] See ASIC Consultation Paper 93 *Facilitating online financial services disclosures* (CP 93), issued April 2008 at www.asic.gov.au/CP.
[10] Law Council of Australia, *Submission* (27 April 2007) at 3; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 13; Abacus, *Submission* (25 June 2007) at 10–11; Australian Bankers Association, *Submission* (6 June 2007) at 12–13.

Section/Topic	Proposals in this section
	• introduce a simpler, technology-neutral concept for the transactions the EFT Code covers (see proposal B3); • consider ways to expand the membership of the EFT Code (see proposal B5); and • redraft the EFT Code in plain English (see proposal B6). We would also: • consult further on the possibility of extending the protections under the EFT Code to small business consumers (see proposal B7; and • clarify that the EFT Code covers BPay transactions (see paragraphs 90–93).
Section C: Disclosure requirements	ASIC proposes to modify the EFT Code disclosure obligations to: • refine the requirements for receipts relating to 'opt-in' systems, when a receipt is required and voice transactions (see proposal C1); and • clarify the requirements for disclosure of surcharges charged by third party ATMs (see proposal C2).
Section D: Complaints handling	ASIC proposes to modify the EFT Code to: • reflect the introduction of a new Australian Standard on complaints handling (see proposal D1); • clarify the obligation for subscribers to give consumers written information about how they investigate complaints unless the complaint is immediately settled (see proposal D2); • introduce a requirement for subscribers to respond to requests for information from another subscriber within 30 days (see proposal D3) • deal with the situation where a subscriber does not respond to a request by an external dispute resolution scheme for information (see proposal D4); and • introduce a limitations period for making complaints (see proposal D5).
Section E: Liability for disputed transactions and mistaken payments	ASIC proposes to retain the current approach to allocating liability for unauthorised transactions in clause 5 with proposed amendments to: • provide that a consumer would be liable for unauthorised transactions that occur because they leave a card in an active ATM which has automatic shut down procedures (see proposal E1); • require subscribers to prohibit merchants from taking consumers' PINs as part of 'book up' practices in merchant agreements (see proposal E2); and • deal with mistaken payments (see proposal E3).
Section F: Electronic communications and privacy	ASIC proposes to: • amend the requirements for delivering information electronically (see proposal F1); and • introduce new requirements for what is printed on receipts to protect consumers' privacy (see proposal F2).
Section G: Administration and review of the EFT Code	ASIC proposes that: • we should have a general power to modify the EFT Code (see proposal G1); • the EFT Code should be reviewed every five years (see proposal G2); and • we would monitor compliance with specific requirements of the EFT Code, including a requirement for subscribers provide certain information on unauthorised transactions (see proposal G3).

B The structure, scope and membership of the EFT Code

Key points

ASIC proposes to:

- include a statement of objectives in the EFT Code (see proposal B1);
- replace the current two-part EFT Code (which has a tailored regime for stored value facilities in Part B) with a one-part structure, with tailored requirements for certain products (see proposals B2 and B4);
- introduce a simpler, technology-neutral concept for the transactions the EFT Code covers (see proposal B3);
- consider ways to expand the membership of the EFT Code (see proposal B5); and
- redraft the EFT Code in plain English (see proposal B6).

We would also:

- consult further on the possibility of extending the protections under the EFT Code to small business consumers (see proposal B7); and
- clarify that the EFT Code covers BPay transactions (see paragraphs 90–93).

PROPOSALS

Statement of objectives (proposal B1)

(January Consultation Paper, Q72)

Proposal

B1 We propose to include a statement of objectives in the revised EFT Code reflecting the following objectives:

(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 long standing 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.

Your feedback

B1Q1 Do you agree with these objectives? What other objectives should the statement of objectives include?

Rationale

17 ASIC Regulatory Guide 183 *Approval of financial services codes of conduct* (RG 183) states that a code should clearly set out its objectives: see RG 183.57. The Code of Banking Practice and the General Insurance Code of Practice include a statement of objectives.

18 The joint submission by Choice, Consumer Action Law Centre and the Centre for Credit and Consumer Law, Griffith Law Centre argued that a statement of objectives is not a priority for the EFT Code.[11] However, our view is that including a statement of objectives in the EFT Code would give readers useful context, and provide criteria for measuring the effectiveness of the EFT Code. All other submissions supported this proposal.[12]

19 We have not proposed exact wording for the statement of objectives at this stage of this review because our proposal to redraft the EFT Code in plain English (see proposal B6) may impact on the precise wording of the statement of objectives.

20 For the purposes of the statement of objectives and the EFT Code as a whole, we take 'electronic' transactions to includes transactions conducted using wireless technology as well as transactions conducted using other electronic technology (e.g. transactions using an ATM, EFTPOS or online banking).

[11] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre, (30 May 2007) at 47.
[12] Suncorp, *Submission* (1 May 2007); Law Council of Australia, *Submission* (27 April 2007) at 15; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 38; Abacus, *Submission* (25 June 2007) at 7; Australian Bankers Association, *Submission* (6 June 2007) at 4; Australian Payments Clearing Association, *Submission* (9 May 2007) at 14; P Hobson, *Submission* (1 May 2007) at 22.

One-part structure (proposal B2)

(January Consultation Paper, Q42–Q43)

Proposal

B2 We propose to replace the current two-part structure of the EFT Code with a one-part structure, incorporating tailored requirements for different products.

Your feedback

B2Q1 Do you agree with this proposal? Please give reasons.

Rationale

21 The EFT Code adopts a two-part structure. Part B of the EFT Code was added following the last review to establish a light touch regime for newer electronic payment products, particularly prepaid stored value products. The goal was to provide some basic protections for consumers without unnecessarily inhibiting innovation and product design in this emerging area.

22 However, in practice Part B has had little impact. There are several reasons for this. First, many newer products rely on remote authorisation, which is not covered by the definitions of 'stored value facilities' and 'stored value transactions' under Part B. These products could be covered by the definition of EFT transaction under Part A of the current EFT Code, but providers of electronic payments services outside financial services have not subscribed to the EFT Code.

23 Secondly, some newer products such as gift cards and other prepaid cards issued by retailers are not personalised and so are not covered either by Part A or Part B of the current Code.

24 Submissions were divided on this issue. Some submissions, including submissions by current subscribers and their representative associations, argued that a separate framework for stored value facilities should be retained but the definition of 'stored value facilities' should be modified to cover emerging products.[13] Alan Tyree argued that all EFT transactions not covered by Part A should be covered by Part B, and that ASIC should be given a power to grant exemptions.[14]

25 The joint submission by Choice, Consumer Action Law Centre and the Centre for Credit and Consumer Law at Griffith University supported

[13] Suncorp, *Submission* (1 May 2007) at 7; Law Council of Australia, *Submission* (27 April 2007) at 11; Abacus, *Submission* (25 June 2007) at 1; Australian Bankers Association, *Submission* (6 June 2007); Australian Merchant Payments Forum, *Submission* (2 May 2007).
[14] [14] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 38.

republishing Part B as best practice guidance, rather than regulating these facilities under the EFT Code.[15]

26 Other submissions supported exploring the introduction of a unitary model.[16]

27 Our view is that emerging products that offer electronic transactions are evolving towards holding higher value and being accepted at a wider range of merchants. These products are competing with traditional banking products. Therefore, the starting point should be that they should be regulated in the same way as traditional banking products, unless there is a good reason for tailoring the requirements.

28 We also consider that a one-part structure rather than a two-part structure would be more conceptually coherent for the EFT Code.

29 We accept that it will be necessary to incorporate specific requirements for certain products as part of this structure: see proposal B4.

30 A submission to this review by the Australian Payments Clearing Association (APCA) noted that the traditional electronic funds transfer channels have developed self-regulatory frameworks that overlap with the EFT Code, including the rules administered by APCA and the various card scheme rules. APCA argued that the EFT Code should cease to formally bind subscribers and instead be reformulated as a set of non-binding policy principles applied to these self-regulatory frameworks.[17]

31 ASIC does not agree with this suggested approach. We think the EFT Code should continue to exist as a standalone Code administered by a regulator. We believe that the EFT Code plays an important role as a consumer-facing Code that provides comprehensive information about consumers' rights with electronic funds transfers. Important as the rules administered by APCA are, they are not where consumers look for information relevant to them. We also think it is important that the EFT Code should bind subscribers and that an independent regulator with a consumer protection focus is best placed to administer a code with such broad reach.

32 Finally, we note that the approach suggested by APCA would not cover emerging electronic payments providers. While we acknowledge that the EFT Code has not achieved this to date, this consultation paper considers ways to promote EFT Code membership among emerging providers, as well as alternatives should this prove unsuccessful.

---

[15] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 38.
[16] P Hobson, *Submission* (1 May 2007) at 18 and Australian Settlements Limited, *Submission* (24 April 2007) at 3.
[17] Australian Payments Clearing Association, *Submission* (9 May 2007) at 15–19.

What transactions should the EFT Code cover? (proposal B3)

(January Consultation Paper, Q9, Q42 and Q43)

Proposal

B3 We propose to:

(a) redraft the EFT Code to cover all electronic funds transfer transactions initiated electronically;

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

(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 instruction is intended to be authenticated by comparing the consumer's manual signature with a specimen signature.

Your feedback

B3Q1 Do you agree with this proposal? Please give reasons.

Rationale

33 Part A of the current EFT Code applies to 'EFT transactions'. This term is defined exhaustively using a number of terms including 'funds transfers', 'electronic equipment', 'access method', 'account institution' and 'EFT account'. These terms are then defined using other terms, which are also defined. The result is a complex and somewhat circular definition of the scope of the EFT Code.

34 We propose to simplify this definition. Under our proposal, the EFT Code would cover 'all electronic funds transfer transactions initiated electronically'.

35 For the purposes of coverage, we would take this to include transactions initiated using wireless technology as well as transactions conducted using other electronic technology (e.g. transactions using an ATM, EFTPOS or online banking).

36 We also propose to include the following non-exhaustive list of examples of transactions covered by this definition:

- ATM and EFTPOS transactions
- credit card transactions that are intended to be authenticated by an electronic signature, including by entering a PIN and by signing an electronic tablet;
- direct debits;

- telephone banking and bill payment transactions;
- internet banking including 'pay anyone' funds transfer, and online bill payment facilities;
- transactions using electronic prepaid cards whether re-loadable or not;
- transactions using electronic toll devices;
- transactions using mobile phone payment services.

37 Transactions using mobile phone payment services are generally not covered by any industry code or legislation, unless they are classified as a Mobile Premium Service (MPS). A MPS is an information and content service that can be accessed via mobile phones and mobile internet-enabled devices (e.g. personal digital assistants). MPS is regulated under the Telecommunications Service Provider (Mobile Premium Services) Determination 2005 (No 1) and the Mobile Premium Services Industry Scheme.

38 Because most mobile payment services are not regulated elsewhere, we think it is appropriate that the EFT Code cover them.

39 We also propose to include the following non-exhaustive list of examples of transactions not covered by the definition:

- cheque transactions; and
- card transactions intended to be authenticated by comparing the consumer's manual signature with a specimen signature.

40 We propose that ASIC should have a general power to modify the application of the EFT Code in particular cases or classes of cases, subject to a requirement to consult with stakeholders: see proposal G1. If necessary, we will use this power to add new types of transactions to the list of examples of transactions that the EFT Code covers.

41 Part B of the current EFT Code imposes a lighter-touch regime for stored value facilities. We are proposing to adopt a one-part structure for the EFT Code: see proposal B2 with tailored requirements for certain products: see proposals B2 and B4.

Tailored requirements for certain types of electronic transactions (proposal B4)

(January Consultation Paper, Q42–Q54)

Proposal

B4 We propose 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 or less.

The general requirements under the EFT Code would not apply to transactions using these products. For example, the requirement to give periodic statements and the rules allocating liability for unauthorised transactions would not apply. Table 4 summarises the tailored requirements that would apply under our proposal.

Your feedback

B4Q1 Do you agree with this proposal? Please give reasons.

B4Q2 Is $100 the right cut off point for this lighter-touch regime?

We are interested in feedback from businesses that offer products with these features about the compliance costs of complying with the tailored regime we are proposing.

Table 4: Proposed tailored requirements for certain types of electronic transactions

Area	Tailored requirement	Related general requirement
Terms and conditions	Subscribers must: • if practical, give consumers terms and conditions for the product before they first use it; or • if this is not practical, and the subscriber knows the identify and contact details of the consumer, give a summary and notice about how the consumer can obtain the terms and conditions. Subscribers must also: • publicise the availability of terms and conditions and 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 consumers; or – by publicising the changes.	These requirements modify the general requirements under clause 2 of the current EFT Code.
Checking balances	Subscribers must provide a mechanism for checking the available balance on these products that is reasonably accessible to consumers in line with clause 14 of the current EFT Code.	This requirement would replace the general obligation to provide receipts under clause 4.

Area	Tailored requirement	Related general requirement
Exchange or refund	Subscribers must give consumers the right to obtain an exchange or refund on request and where the product malfunctions in line with clauses 15 of the current EFT Code.	Not applicable.
System or equipment malfunction	Subscribers would be liable for losses caused by system or equipment malfunction in line with clause 17 of the current EFT Code.	This requirement would replace the general liability allocation provisions in clause 5 and 6 of the current EFT Code.
Dispute resolution	Subscribers would be required to comply with the dispute resolution obligations under the EFT Code, in line with clause 19 of the current EFT Code.	This requirement is in line with the requirements for other products under clause 10 of the current EFT Code.
Expiry period	If the product has a minimum expiry period: • subscribers must not unilaterally reduce it; • subscribers must include information about these rights and protections in their disclosure to consumers; and • where possible, consumers must be able to see the expiry date information when using the product (e.g. on any card or as part of any web transaction).	Not applicable.

Rationale

42 The proposed tailored requirements would only cover transactions using products with certain features. For example, the tailored requirements would cover prepaid cards, whether reloadable or not, if:

- the product issuer cannot cancel the card if it is lost or stolen;
- consumers are not required to authenticate transactions using a PIN, electronic signature or other electronic method of authentication; and
- the maximum value that can be held on the card at one time is $100 or less.

43 We propose this approach because in practice, the general requirements under the EFT Code could not apply to transactions using many of these emerging products. In particular, these products can be used anonymously, which renders many of the general requirements unworkable (e.g. the requirement to provide periodic statements).

44 We also think it is necessary to include requirements to reflect the fact that these products often include an expiry date.

45 We propose that these less onerous requirements only apply to low value products because lower value products pose lower risks to consumers. Some

electronic gift vouchers and travel cards can hold thousands of dollars of value. We think these products should be subject to the general rules in the EFT Code, including in particular the rules that allocate liability for unauthorised transactions.

46 Apart from the proposed prohibition on unilaterally reducing the minimum expiry period for these products, our proposed tailored requirements are existing requirements under Part B of the current EFT Code: see clauses 12–19.

47 No submissions addressed whether the requirement that subscribers must provide a mechanism for consumers to check the available balance that is reasonably accessible instead of receipts should be retained.

48 We believe that a mechanism should be available on continuing basis to enable consumers to check the balance of their products initially at the point of sale, whenever they use the products and at any other time afterwards. This enables consumers holding a product with an expiry date to use all the funds held before the product expires.

49 We did not receive any submissions from businesses that offer newer electronic payment products.

50 Under the current EFT Code, subscribers to Part B that provide a way for consumers to report the loss or theft of a product and cancel it must also refund lost or stolen value to consumers if a consumer has reported a loss or theft: see clause 16 of the EFT Code.

51 The Australian Merchant Payments Forum opposed any right to refund of lost or stolen stored value.[18] One financial services provider argued that the right to refund lost or stolen stored value should only apply for products that hold a minimum of $50 while Abacus emphasised the importance of improving consumer rights.[19] No other submissions addressed this issue.

52 Under our proposal, one of the criteria for the tailored requirements is that the provider cannot cancel the product if it is lost or stolen. Therefore, the requirement to refund lost or stolen value would not be relevant.

Transaction records

(January Consultation Paper, Q44–Q45)

53 The January Consultation Paper asked whether subscribers should be required to make a transaction history available on request for products currently covered by Part B of the EFT Code.

[18] Australian Merchant Payments Forum, *Submission* (2 May 2007) at 3–4.
[19] Suncorp, *Submission* (1 May 2008) at 8; Abacus, *Submission* (25 June 2007) at 17.

54 Most submissions that addressed this issue supported a requirement to provide transaction records, although no submissions suggested a specific period or number of transactions that the record should cover.[20] Abacus supported a requirement to provide transaction records but argued that the priority should be reviewing the scope of Part B before expanding the obligations under it.[21]

55 We did not receive any submissions on this issue from businesses that offer newer electronic payment products.

56 The argument in favour of requiring transaction records is that without access to minimum records, it is difficult for consumers to identify unauthorised transactions.

57 On the other hand, requiring subscribers to provide transaction records for these products is likely to involve significant compliance costs and, under our proposal, subscribers would not be liable for unauthorised transactions for these products anyway.

58 On balance, we think that the costs of requiring transaction records for products would outweigh the benefits where the subscriber cannot cancel the product if it is lost or stolen, there is no electronic authentication mechanism to safeguard consumers against unauthorised transactions and the maximum value that can be held on the product at one time is $100 or less.

59 Therefore, we are not proposing to require subscribers providing these products to make a transaction history available on request. For the tailored requirements we are proposing for these products, see proposal B4.

Expiry period

(January Consultation Paper, Q48–Q49)

60 Under Part B of the current EFT Code, subscribers must generally give consumers the right to exchange stored value that has expired for 12 months after expiry: clause 15.2(b). The January Consultation Paper asked whether this should be retained or modified.

61 Most submissions to the January Consultation Paper supported a requirement that newer electronic payment products must have a minimum use time (e.g. 12 months).[22]

62 We did not receive any submissions on this issue from businesses that offer these products.

---

[20] Suncorp, *Submission* (1 May 2007) at 7; P Hobson, *Submission* (1 May 2007) at 18.
[21] Abacus, *Submission* (25 June 2007) at 16.
[22] Suncorp, *Submission* (1 May 2007) at 8; Abacus, *Submission* (25 June 2007) at 17; Australian Bankers Association, *Submission* (6 June 2007) at 28; P Hobson, *Submission* (1 May 2007) at 19.

63 Our ideal position is for electronic payment products not to have an expiry period. However, we acknowledge that this could deter businesses that provide newer electronic payment products from subscribing to the EFT Code.

64 We are interested in receiving further feedback about this, particularly from providers of these products. If it is not feasible not to have an expiry period, we think a minimum expiry period of 12 months should be required.

65 We also think there should be clear and prominent disclosure of the expiry period, including clear and prominent disclosure that a consumer will see when they perform a transaction. For example, for prepaid cards, the expiry date should be printed on the card itself. All submissions supported a disclosure requirement although they did not address how disclosure should be made.[23]

66 One submission pointed out that some products are event-specific.[24] Any requirements would need to accommodate this. We are proposing that ASIC should have a general power to modify the EFT Code, subject to a requirement to consult with stakeholders: see proposal G1. If necessary, we could use this power to modify the expiry period requirements for event-specific products.

67 If a minimum expiry period of 12 months is adopted, we believe it is reasonable for consumers to have a further 12 months after the product has expired to retrieve the expired value. We are interested in receiving further feedback about this before we finalise our proposals on expiry periods.

Your feedback

B4Q3 Should the EFT Code impose a requirement on subscribers that offer newer electronic payment products must not include an expiry period for these products, or a minimum expiry period of 12 months for these products, combined with a right to obtain a refund of expired value for a further 12 months?

B4Q4 What would be the costs of prohibiting expiry periods or imposing a minimum 12-month expiry period and a further 12 months to obtain a refund?

Payment finality

(January Consultation Paper, Q54)

68 The January Consultation Paper asked whether the EFT Code should be amended to provide for payment finality when a consumer performs a transaction using a non-traditional electronic payment product.

[23] Suncorp, *Submission* (1 May 2007) at 8; Abacus, *Submission* (25 June 2007) at 17; Australian Bankers Association, *Submission* (6 June 2007) at 28; P Hobson, *Submission* (1 May 2007) at 19; Australian Merchant Payments Forum, *Submission* (2 May 2007) at 3.
[24] Australian Merchant Payments Forum, *Submission* (2 May 2007) at 3.

69 This proposal was not widely supported. While the Australian Bankers Association and Abacus supported this proposal, two submissions argued that the common law adequately provides for payment finality and that it would be difficult to formulate a workable payment finality rule for the wide range of newer electronic payment products.[25] We do not propose to pursue this proposal.

Expanding the membership of the EFT Code (proposal B5)

(January Consultation Paper, Q68–Q70)

Proposal

B5 If businesses offering electronic funds transfer payment products do not subscribe to the EFT Code voluntarily, we propose that the government give consideration as to whether:

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

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

Your feedback

B5Q1 Do you agree with this proposal? Please give reasons.

B5Q2 What would be the compliance costs of making the EFT Code mandatory for businesses that have not yet subscribed to the EFT Code?

Rationale

70 Membership of the EFT Code has generally been limited to traditional financial services providers including banks, building societies and credit unions and a small number of finance brokers. Providers of newer electronic payment products (e.g. retailers issuing gift cards, mobile phone operators providing third party payments and transit authorities) have not yet subscribed to the EFT Code.

71 Submissions to the January Consultation Paper argued that there is low awareness of the EFT Code among potential subscribers and consumers and little or no incentive for these providers to subscribe.[26]

[25] Suncorp, *Submission* (1 May 2007) at 8; A Tyree, *Submission* 15 February 2007 at 7.

[26] Suncorp, *Submission* (1 May 2007) at 10; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 36–7; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 46; Care Financial Counselling Service, *Submission* (31 May 2007) at 20; Abacus, *Submission* (25 June 2007) at 6–7; Australian Bankers Association, *Submission* (6 June 2007) at 1 and 3–4; Australian Payments Clearing Association (9 May 2007) at 13; P Hobson, *Submission* (1 May 2007) at 22; Law Council of Australia, *Submission* (27 April 2007) at 15; N Murdoch, *Submission* (27 April 2007) at 1; Australian Settlements Limited, *Submission* (24 April 2007) at 4; Family Business Australia, *Submission* (13 April 2007) at 2; J Roth, *Submission* (19 February 2007) at 1.

72 The starting point for the Working Group was to try to encourage these providers to subscribe. Submissions suggested a number of ways to address this, including:

- ASIC promoting the EFT Code (e.g. by introducing a logo signifying that a business subscribes to the EFT Code);
- requiring non-subscribers to report to ASIC their reasons for not subscribing and requiring ASIC to publicly report this information; and
- making the EFT Code mandatory.

73 As part of this review, ASIC will publish the names of every subscriber on our consumer website, FIDO (www.fido.gov.au).

74 We acknowledge the importance of promoting the EFT Code to potential subscribers and consumers, and the ongoing need to do more of this. However, establishing broad awareness of the EFT Code will be challenging. In reality, even where consumers consider EFT Code membership when choosing a provider that offers electronic transactions, it is likely to be only one of a number of competing considerations.

75 For this reason, relying on promoting the EFT Code to consumers is likely to have only minimal impact in generating consumer demand that newer electronic payment providers subscribe to the EFT Code. Behavioural economics research shows that consumers tend to be overoptimistic when choosing providers, in the sense that they discount the likelihood of adverse events such as a dispute with their provider over an unauthorised transaction.

76 If promotion is not effective, it will be necessary to explore other options, including:

- making the EFT Code mandatory for all businesses that provide electronic transactions; or
- dealing with consumer protection in this area through regulation.

77 The Working Group has considered the possibility that the EFT Code should be made mandatory for all providers of electronic payment products.

78 We acknowledge that EFT Code subscribers incur compliance costs, including the costs of complying with disclosure obligations, dispute resolution requirements, the allocation of liability for unauthorised transactions required under the EFT Code and cooperating with compliance monitoring activities undertaken by ASIC.

79 Arguably, businesses that offer newer electronic payment products are in direct competition with subscribers, yet these businesses avoid the compliance costs associated with EFT Code membership. Making the EFT Code mandatory would establish a more level playing field in this market in terms of the costs of doing business.

Design and presentation (proposal B6)

(January Consultation Paper, Q71)

Proposal

B6 We propose to redraft the EFT Code as a principles-based code in plain English. In terms of timing, we propose to undertake this work as a separate process after we have finalised and publicly released our recommendations for substantive changes to the EFT Code.

Your feedback

B6Q1 Do you agree with this proposal? Please give reasons.

Rationale

80 The January Consultation Paper asked what changes could be made to make the EFT Code more user friendly. There was widespread support for redrafting the EFT Code in plain English and adopting a more principles-based, less prescriptive approach.[27] The Australian Bankers Association indicated that it is willing to contribute resources to this work.

81 We propose to undertake this work as a separate process after we have finalised our recommendations for substantive changes to the EFT Code and released our recommendations publicly. We will undertake further consultation with all stakeholders about the redrafting process.

OTHER ISSUES

Protecting small business consumers

(January Consultation Paper, Q11)

82 The question of whether the EFT Code should protect small business consumers was raised at the last review and in the January Consultation Paper.[28]

83 Most submissions to the January Consultation Paper supported extending the EFT Code protections to small business consumers.[29] The Australian Bankers Association, Abacus and Australian Settlements Limited opposed this.[30]

---

[27] Suncorp, *Submission* (1 May 2007) at 10; ANZ, *Submission* (2 May 2007) at 2; Law Council, *Submission* (27 April 2007) at 15; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 9–10; Abacus, *Submission* (25 June 2007) at 7; Australian Bankers Association, *Submission* (6 June 2007) at 4; Australian Payments Clearing Association, *Submission* (9 May 2007) at 13–14.

[28] See paragraphs 5.10–5.19.

[29] Suncorp, *Submission* (1 May 2007) at 3; Law Council of Australia, *Submission* (27 April 2007) at 4; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 8; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 21; P Hobson, *Submission* (1 May 2007) at 7–8; N Murdoch, *Submission* (27 April 2007) at 1; Family Business Australia, *Submission* (13 April 2007) at 2–3; J Roth,

84 The January Consultation Paper asked for data on the extent to which small businesses experience problems with electronic banking and the nature of the problems. Data provided by the Australian Bankers Association, Abacus and the Banking and Financial Services Ombudsman indicated that the number of complaints by small business consumers is relatively low. On the other hand, the Council of Small Business argued that its members do experience problems with electronic banking but that the time and effort involved in making a complaint and seeing it through is often more than they can afford.

85 On 30 April 2008, the Productivity Commission released its final report on Australia's consumer policy framework. The final report noted that the Uniform Consumer Credit Code does not protect small business consumers and noted that:

> *While not having examined this issue in any detail, the Commission observes that such an extension in coverage would at least have the advantage of promoting more consistency in the remit of applicable regulatory instruments in this area.*[31]

86 One possible approach, if the EFT Code were to be extended, would be to modify the way the protections apply to small business consumers. For example, if electronic transactions by small businesses tend to be of higher value than transactions performed by individuals, it may be appropriate to adjust the no-fault liability threshold to an amount greater than $150. It may be appropriate that a no fault liability amount is set at 5% of the amount in dispute for disputes between subscribers and small business consumers.

87 If the EFT Code protections are extended to cover small businesses, it will be necessary to define 'small business'. Section 761G(12) of the Corporations Act defines 'small business' as a business *employing*: [emphasis added]

- less than 100 people, if the business is or includes the manufacture of goods; or
- otherwise, less than 20 people.

88 This is different to the definition of 'small business' under clause 40 of the Code of Banking Practice, which is a business *having*: [emphasis added]

- less than 100 full time (or equivalent) people if the business is or includes the manufacture of goods; or
- in any other case, less than 20 full time (or equivalent) people.

Submission (19 February 2007) at 1; Western Australia Small Business Development Corporation, *Submission* (1 November 2007) at 1; Queensland Retail Traders and Shopkeepers Association, *Submission 1*(29 January 2008) at 1 and *Submission 2* (22 February 2008) at 1.

[30] Australian Bankers Association, *Submission* (6 June 2007) at 14–15; Abacus, *Submission* (25 June 2007) at 11–12; Australian Settlements Limited, *Submission* (24 April 2007) at 2.

[31] Productivity Commission, Review of Australia's Consumer Policy Framework (30 April 2008) at 457–458.

89 The Code of Banking Practice's definition is wider than that of the Corporations Act as it is not restricted to employer-employee relationship.

Small business consumers

B7 We are interested in exploring whether the EFT Code should be extended to protect small business consumers. We plan to discuss this possibility in coming weeks with stakeholders, including financial services providers and small businesses.

Your feedback

B7Q1 Should the EFT Code protect small business consumers?

B7Q2 If so, what, if any protections under the EFT Code should be modified for small business consumers, and why?

B7Q3 Should the no-fault liability amount be set at 5% of the amount in dispute for disputes between subscribes and small business consumers?

B7Q4 What definition of 'small business' should the EFT Code adopt?

B7Q5 What would be the compliance costs of extending the EFT Code protections to small business, if the no-fault liability amount was set at 5% of the amount in dispute for small business disputes?

BPay transactions and biller accounts

(January Consultation Paper, Q10)

90 The January Consultation Paper noted that the use of BPay examples in the Endnotes to the current EFT Code has led to confusion about whether BPay transactions come within the scope of the Code.[32]

91 We consider that the EFT Code does cover BPay transactions and we will amend the EFT Code to clarify this.

92 A biller account is a consumer account held by a business for the purpose of recording the amounts owing and paid by the consumer for goods and services provided by the business. Most EFT transactions involving biller accounts are excluded from the EFT Code under clause 1.4.

93 The January Consultation Paper asked whether biller accounts should continue to be excluded from the EFT Code. Few submissions addressed this issue and those that did generally supported the existing exemption.[33] We will retain the existing exemption but redraft it to make it easier to understand.

[32] See paragraph 5.
[33] Suncorp, *Submission* (1 May 2007) at 3; Law Council, *Submission* (27 April 2007) at 3.

C Disclosure requirements

Key points

ASIC proposes to modify the EFT Code disclosure obligations to:

- refine the requirements for receipts (see proposal C1); and
- clarify the requirements for disclosure of surcharges charged by third party ATMs (see proposal C2).

PROPOSALS

Receipts (proposal C1)

(January Consultation Paper, Q13–Q16)

Proposal

C1 We propose to amend the EFT Code to:

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

(b) clarify that subscribers 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 receipts for voice transactions 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.

Your feedback

C1Q1 Do you agree with this proposal? Please give reasons.

Rationale

Opt-in receipt systems

(January Consultation Paper, Q13)

94 Clause 4.1(a) of the EFT Code requires a subscriber to give a consumer a receipt unless the consumer specifically elects otherwise.

95 Some subscribers operate 'opt-in' receipt systems where consumers must positively choose to receive a receipt for each transaction. Subscribers have expressed concern that the drafting of clause 4.1(a) suggests that only 'opt-out' systems are permitted.

96 Our view is that consumers should be required to consider whether they want a receipt. We consider that systems where consumers must opt-in to receive receipts for each transaction and systems where consumers must opt-out of receiving receipts both achieve this. We propose amending the wording of clause 4.1(a) to clarify this.

97 All the submissions to the January Consultation Paper that addressed this issue supported this approach.[34]

Requiring receipts where reasonably practicable

(January Consultation Paper, Q14)

98 Clause 4.1(a) requires subscribers to ensure a receipt is issued. Several subscribers have raised concerns that this requirement does not recognise that it is not possible to issue receipts if the machine (e.g. an ATM or EFTPOS machine) runs out of paper.

99 We propose to modify clause 4.1(a) to provide that subscribers are required to take reasonable steps to ensure that a receipt is issued and are not required to provide a receipt where it is not reasonably practicable to do so. Where a receipt will not be issued because it is not reasonably practicable, consumers must be notified before they complete the transaction so they can decide whether to proceed with it.

100 Submissions supported this approach.[35]

101 We are aware of a number of proposals to deploy EFTPOS machines in petrol station forecourts. We understand that it may not be technically possible for EFTPOS machines to generate receipts in this physical environment because dust and grime interferes with the printing function of EFTPOS machines.

102 We accept that subscribers should not be required to provide receipts where it is not reasonably practicable to do so because of the physical environment. Again, our view is that in this situation subscribers should be required to notify consumers that they will not receive a receipt before they complete

[34] Bendigo Bank, *Submission* (27 April 2007) at 1; Suncorp, *Submission* (1 May 2007) at 3; Law Council of Australia, *Submission* (27 April 2007) at 4; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 16; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 22; Abacus, *Submission* (25 June 2007) at 12; Australian Bankers Association, *Submission* (6 June 2007) at 16–17; Australian Payments Clearing Association, *Submission* (9 May 2007) at 6; Australian Merchant Payments Forum, *Submission* (2 May 2007) at 2; P Hobson, *Submission* (1 May 2007) at 10.

[35] Bendigo Bank, *Submission* (27 April 2007) at 1; Suncorp, *Submission* (1 May 2007) at 3; Law Council of Australia, *Submission* (27 April 2007) at 4; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 17; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 22; Abacus, *Submission* (25 June 2007) at 12; Australian Bankers Association, *Submission* (6 June 2007) at 17; Australian Payments Clearing Association, *Submission* (9 May 2007) at 6; Australian Merchant Payments Forum, *Submission* (2 May 2007) at 2; P Hobson, *Submission* (1 May 2007) at 10.

the transaction so they can decide whether to proceed with it. Our proposal will address this situation.

Merchant identification on transaction receipts

(January Consultation Paper, Q15)

103 Clauses 4.1(a) and 4.1(b) prescribe information that must be included on receipts. For merchant payments conducted by voice communication (e.g. telephone banking), this includes the merchant's name: see clause 4.1(b)(v). This enables consumers to confirm the identity of the merchant to ensure that the payee is correct.

104 We understand that in practice, many voice communication transaction systems record a unique number for each merchant but do not record their name.

105 We propose to amend the EFT Code so that identifying merchants either by name or a unique number is acceptable. If a receipt for a merchant payment conducted by voice communication uses a number rather than the merchant's name, the invoice provided by the merchant to the consumer must include both their name and the number on the receipt. This will enable the consumer to match the number on the receipt with the name and number on the invoice and check that they have paid the correct merchant.

106 Subscribers would also be required to ensure that their contractual arrangements with merchants addressed this requirement.

107 Most submissions supported this proposal.[36] Three submissions opposed it on the basis that it would confuse consumers and that from a technical perspective, it should be possible to provide the merchant's name for payments conducted by voice communication.[37] However, subscribers have advised us that this is not possible for all software systems. While we agree that it may cause consumer confusion, we think the requirement to include the number with the merchant's name on the consumer invoice and statement addresses this.

108 We believe that disclosing the merchant's name is best practice and we will state this in the EFT Code.

109 Our proposal is consistent with ASIC's approach on this issue in a letter to subscriber industry associations on 18 March 2002.

---

[36] Suncorp, *Submission* (1 May 2007) at 3; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 22; Abacus, *Submission* (25 June 2007) at 12; Australian Bankers Association, *Submission* (6 June 2007) at 17 and B Pay, *Submission* (8 May 2007) at 7.
[37] Bendigo Bank, *Submission* (27 April 2007) at 1; Law Council of Australia, *Submission* (27 April 2007) at 4; and P Hobson, *Submission* (1 May 2007).

Disclosing balance on receipts

(January Consultation Paper, Q16)

110 Clause 4.1(a)(viii) requires subscribers to include on receipts the balance remaining after the transaction when possible and when it is unlikely to compromise the consumer's privacy or security. Endnote 12 adds that 'privacy and security concerns may preclude providing balance information at EFTPOS terminals but not at ATMs'.

111 The January Consultation Paper asked whether the EFT Code should give further guidance about this requirement.

112 The majority of submissions on this issue opposed including further guidance on the grounds that it was not required and that the EFT Code should be expressed as a series of flexible high level principles rather than detailed, prescriptive rules.[38] Only one submission supported this.[39] We will not be pursuing this proposal.

Surcharges charged by independent ATM owners (proposal C2)

Proposal

C2 We propose to redraft the EFT Code to make it clear that:

(a) as specified in their agreement with the subscriber, independent ATM owners must disclose charges for using their ATM before a person performs a transaction (see clause 4.6); and

(b) subscribers need not disclose specific surcharges for using independent ATMs to consumers in statements if they do not know the precise amount of these surcharges.

Your feedback

C2Q1 Do you agree with this proposal? Please give reasons.

C2Q2 After the industry-based reforms of the ATM system, will subscribers always have agreements with independent ATM owners?

Rationale

113 Subscribers must include in agreements with independent ATM owners a requirement that the independent ATM owner disclose any fee or surcharge they charge consumers: clause 4.6. This information must be disclosed at a time that enables the consumer to cancel the transaction without cost.

---

[38] Suncorp, *Submission* (1 May 2007) at 3; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 23; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 17; Abacus, *Submission* (25 June 2007) at 12; Australian Bankers Association, *Submission* (6 June 2007) at 17; Australian Payments Clearing Association, *Submission* (9 May 2007) at 7 and P Hobson, *Submission* (1 May 2007).
[39] BPay, *Submission* (8 May 2007).

114 For a number of years, the Reserve Bank of Australia has been encouraging industry-based reform of Australia's ATM system. One objective of the reform process is to remove barriers to participation in the ATM system. In particular, the Reserve Bank has indicated that there should be no restrictions on ATM owners directly charging consumers for using an ATM.[40]

115 The Reserve Bank's view is that independent ATM owners should be required to disclose charges for using their ATM before a person performs a transaction so that potential users can cancel the transaction at no cost after the disclosure if they choose.[41] ASIC agrees with this approach. We think this is already required under clause 4.6. We will redraft this clause to make this clearer.

116 The Australian Bankers Association and Abacus argued that independent ATM operators should be required to subscribe to the EFT Code because they will have a direct charging relationship with consumers.[42]

117 However, clause 4.6 achieves disclosure of surcharges charged by an independent ATM owner through the agreement between them and the subscriber.

118 The EFT Code also requires subscribers to disclose fees in statements: clause 4.3(b). ASIC accepts that subscribers cannot disclose specific surcharges for using independent ATMs to consumers in statements if they do not know the precise amount of these surcharges. In this situation, we consider that subscribers should be required to disclose that independent ATM owners may charge a surcharge for using their ATMs. We will amend the EFT Code to require this. We note, though, that best practice would be to include surcharges by independent ATM owners on statements if this information is known.

OTHER ISSUES

Notifying changes to fees

(January Consultation Paper, Q12)

119 Clause 3 requires subscribers to give consumers written notice at least 20 days before:

- imposing or increasing charges for an access method (e.g. an internet banking fee);
- increasing the consumer's liability for losses; or
- imposing, removing or adjusting a daily or other transaction limit.

[40] Reserve Bank of Australia, *Submission* (30 April 2007) at 1.
[41] Reserve Bank of Australia, *Submission* (30 April 2007) at 1.
[42] Abacus, *Submission* (25 June 2007) at 10; Australian Bankers Association, *Submission* (6 June 2007) at 5.

120 Several industry representatives have raised concerns about the compliance costs of this requirement.[43] Suncorp, ANZ, Abacus and Australian Bankers Association argued that the EFT Code should be aligned with the Code of Banking Practice. The Code of Banking Practice requires:

- written notice of new fees 30 days in advance; and
- notice of other changes, including changes to existing fees, liability for losses and transaction requirements, using media advertisements on the day the change takes effect.[44]

121 ASIC's view is that media advertisements have limited effectiveness. Submissions by the Law Council, consumer representatives and individual consumers supported this view.[45] Our ideal position is for consumers to be provided with individual disclosure.

122 However, we accept that the costs of mailing separate written notices of these changes to terms and conditions are significant. Our proposal to permit subscribers to meet their EFT Code disclosure obligations electronically, subject to certain conditions addresses this, at least in part: see proposal F1.

123 One alternative approach would be to allow subscribers to use media advertisements to disclose changes to existing fees and charges, and give consumers written notice in their next statement, without giving personal notification to consumers before the change.

124 Another and better compromise would be to require subscribers to notify consumers by email about changes to existing fees and charges where these email details are available as well as using media advertisements to disclose changes to existing fees and charges, and giving consumers written notice in their next statement.

Changes to fees

C3 We are interested in your feedback on different approaches to notifying consumers of changes to fees and charges.

Questions

C3Q1 Should the current EFT Code requirements for notifying changes to existing fees and charges be retained?

[43] Suncorp, *Submission* (1 May 2007) at 3; ANZ, *Submission* (2 May 2007) at 2; Abacus, *Submission* (25 June 2007) at 12; Australian Bankers Association, *Submission* (6 June 2007) at 16.
[44] Code of Banking Practice, clause 18.
[45] Law Council of Australia, *Submission* (27 April 2007) at 4; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 22; P Hobson, *Submission* (1 May 2007) at 10.

C3Q2 Alternatively, should subscribers be allowed to use media advertisements to disclose changes to existing fees and charges, and either give consumers written notice in their next statement, without giving personal notification to consumers before the change, or notify consumers by email where these email details are available, and giving consumers written notice in their next statement?

C3Q3 What are the compliance costs of the current requirement? How would changing this requirement affect these compliance costs?

Consistency between the EFT Code, the Corporations Act and the Code of Banking Practice

(January Consultation Paper, Q17)

125 The January Consultation Paper asked whether there is any duplication or inconsistency between the EFT Code and the Corporations Act that needs reviewing.

126 A number of submissions argued that the obligations in the EFT Code on disclosure as discussed in proposals C1 and C2 are inconsistent with the Corporations Act and should be removed.[46]

127 Our view is that the role of industry codes is to do more than restate the law by offering consumer protection benefits that go beyond the protections afforded by law and providing for a higher standard of conduct than required by law. We do not consider that there is any inconsistency between a law and an industry code where the industry code affords additional consumer protections and does not make it impossible to comply with the law.

128 This view is set out in ASIC Regulatory Guide 183 *Approval of financial services codes of conduct* at RG 183.28–RG 183.29. We consider that this is generally applicable to all industry codes, including those that have not been approved under RG 183 such as the EFT Code of Conduct.

129 The requirements under the Corporations Act for basic deposit products and related non-cash payment facilities are less onerous than the requirements for other deposit products. This is a result of amendments to the Corporations Act in 2005.[47] When introducing these changes, the Government noted that issuers

[46] Law Council, *Submission* (27 April 2007) at 5; Australian Bankers Association, *Submission* (6 June 2007) at 18; P Hobson, *Submission* (1 May 2007) at 11.
[47] Corporations Regulation reg 7.9.07FA, inserted by the *Corporations Amendment Regulations 2005 (No 5)*.

of basic deposit products are subject to industry codes that contain requirements and standard practice for disclosure in the banking industry.[48]

130 Appendix 3 of this consultation paper compares the regulatory obligations relating to disclosure, receipts and statements under the EFT Code, the Banking Code of Practice and the Corporations Act.

131 The EFT Code imposes more onerous requirements in several respects:

- It imposes more onerous initial disclosure requirements than the Corporations Act or ASIC relief for low value non-cash payments.
- It imposes more onerous requirements for disclosure on request than the Corporations Act.
-
- It imposes receipt requirements that are not required under the Corporations Act, ASIC's relief or the Code of Banking Practice.
- It imposes a requirement to provide statements that is more onerous than the Corporations Act requirements and ASIC's relief.

132 The initial disclosure requirements and the requirement to provide copies of terms and conditions on request under the EFT Code are consistent with the Code of Banking Practice. We think that upfront disclosure of terms and conditions and the ability to get a copy of terms and conditions on request is important to enable consumers to decide whether to buy or keep a product and compare different products. We do not propose to modify these requirements.

133 Receipts are important for electronic banking because they help consumers to reconcile their statements and identify unauthorised transactions. We think consumers should have the opportunity to request a receipt: see Proposal C 1.

134 Statements are important for electronic banking because they enable consumers to identify unauthorised transactions. We think subscribers should generally be required to provide statements. .We accept that consumers should be able to agree to receive statements electronically. Our proposal dealing with electronic communication permits this (see Proposal F 1). We recognise the costs of complying with the obligation to give statements. We are interested in feedback on whether to modify the EFT Code so that subscribers need not give statements where an account has a zero balance and there has been no activity on it during the statement period (see Proposal C4).

[48] Explanatory Statement, Select Legislative Instrument 2005 No 324, *Corporations Amendment Regulations 2005 (No 5), Item 8.*

Disclosing online fraud risks

(January Consultation Paper, Q18)

135 The January Consultation Paper asked whether the EFT Code should be amended to require subscribers to give consumers pre-contractual information about the risks of online fraud.

136 Two submissions supported pre-contractual disclosure about online fraud risks.[49] Most submissions on this issue did not support this.[50] The joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre argued that pre-contractual disclosure is not a suitable vehicle for communicating information about online security risks and argued that a more appropriate vehicle should be established. ASIC accepts this argument. The Australian Bankers Association supported amending the EFT Code to recognise the extent to which banks already give new customers information about online fraud risks, but not to introduce any new obligation.

137 We accept that one-off disclosure before a consumer enters a contract with a subscriber is unlikely to be an effective tool for educating consumers about how to guard against the risks of online fraud. Subscribers must give consumers a notice summarising their security guidelines annually, on or with a periodic statement: see clause 4.5. Many subscribers also do much more than this. Therefore, at this time we don't propose to add to the mandatory requirements for educating consumers about online fraud.

138 We acknowledge the existing work already undertaken by subscribers in disclosing the risk of online fraud. We encourage subscribers to continue their work in this area and develop innovative approaches to improving consumer awareness of online fraud risks. We do not propose to make this a mandatory requirement.

Discrepancies in deposits and third party transfers

(January Consultation Paper, Q19)

139 Clause 7.1 of the EFT Code requires subscribers to inform consumers of a discrepancy between an amount recorded as having been deposited to an account and the amount recorded as received.

---

[49] Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 18; Abacus, *Submission* (1 May 2007) at 13.
[50] Suncorp, *Submission* (1 May 2007) at 4; Law Council, *Submission* (27 April 2007) at 5; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 23; BPay, *Submission* (4 May 2007) at 8; P Hobson, *Submission* (1 May 2007) at 11; Australian Bankers Association, *Submission* (6 June 2007) at 19.

140 The January Consultation Paper asked whether this clause should be strengthened and expanded. Few submissions addressed this issue. We are not aware of any problems with the practical operation of this requirement. Therefore, we do not propose to pursue this proposal.

Statements

141 Clause 4 of the EFT Code requires subscribers to give statements every six months and prescribes the content of statements. While the Code of Banking Practice also imposes statement requirements, it does not require statements for accounts where there have been no transactions during the statement period.[51]

Statements

C4 We recognise the costs of complying with the obligation to give statements. We are interested in your feedback on whether to modify the EFT Code so that subscribers need not give statements in certain circumstances.

Your feedback

C4Q1 Should the EFT Code be modified to so that subscribers need not give statements for accounts with a zero balance where there are no transactions during the statement period?

[51] Code of Banking Practice clause 24.1(c).

D Complaints handling

Key points

ASIC proposes to modify the EFT Code to:

- reflect the introduction of a new Australian Standard on complaints handling (see proposal D1);
- clarify the obligation for subscribers to give consumers written information about how they investigate complaints unless the complaint is immediately settled (see proposal D2);
- introduce a requirement for subscribers to respond to requests for information from another subscriber within 30 days (see proposal D3)
- deal with the situation where a subscriber does not respond to a request by an external dispute resolution scheme for information (see proposal D4); and
- introduce a limitations period for making complaints (see proposal D5).

PROPOSALS

New Australian Standard on complaints handling (proposal D1)

(January Consultation Paper, Q20–Q21)

Proposal

D1 We propose to amend the EFT Code to:

(a) include a definition of 'complaint' using the definition in Australian Standard ISO 10 002 2006 *Complaints Satisfaction—Guidelines for complaints handling in organisations*; and

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

Your feedback

D1Q1 Do you agree with this proposal? Please give reasons.

Rationale

142 On 5 April 2006, a new Australian Standard on complaints handling was introduced: Australian Standard ISO 10 002 2006 *Complaints Satisfaction—Guidelines for complaints handling in organisations*. Clause 10.1 of the EFT Code currently requires subscribers to establish internal dispute resolution procedures that comply with the previous Australian Standard, Australian

Standard 4269–1995 *Complaints Handling*. We propose to update the EFT Code to reflect the introduction of the new Standard.

143 In ASIC Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165), Australian financial services licensees are also required to satisfy the Essential Elements of Complaints Handling under the previous Standard. We will update RG 165 to reflect the introduction of the new Standard in coming months.

144 The new Standard introduces a definition of 'complaint'. The definition is:

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

145 We propose to include this definition in the EFT Code. In our view, including this definition in the EFT Code would help clarify the scope of subscribers' obligations to investigate and resolve complaints. In particular, this definition clarifies that there is an onus on subscribers to identify complaints, rather than requiring investors and consumers to explicitly state that something is a complaint. There is no definition of complaint in the current EFT Code.

146 Most submissions to the January Consultation Paper supported this proposal.[52]

147 However, the Australian Bankers Association did not support this approach. The Australian Bankers Association argued that the EFT Code should be aligned with the Code of Banking Practice in this area.[53] The Code of Banking Practice uses the expression 'dispute' instead of 'complaint'. It defines a 'dispute' as a complaint about a banking service that is not immediately resolved: clause 40.

148 The definition of 'dispute' under the Code of Banking Practice is narrower than the definition of 'complaint' under the new Standard. Our view is that the broader definition is preferable. Consumer protection is better served by a wider definition that captures expressions of dissatisfaction where a consumer expects a response. We propose to update the EFT Code to reflect the definition in the new Standard.

---

[52] Bendigo Bank, *Submission* (27 April 2007) at 1; Suncorp, *Submission* (1 May 2007) at 4; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 19; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 24; Care Financial Counselling Service, *Submission* (31 May 2007) at 16; Abacus, *Submission* (25 June 2007) at 13; P Hobson, *Submission* (1 May 2007) at 12.
[53] Australian Bankers Association, *Submission* (6 June 2007) at 20.

Complaints that are not immediately settled (proposal D2)

(January Consultation Paper, Q22)

Proposal

D2 We propose to amend clause 10.3 to provide that a subscriber can investigate a complaint for one business day before giving consumers written information about how it resolves complaints.

Your feedback

D2Q1 Do you agree with this proposal? Please give reasons.

Rationale

149 Subscribers have argued that the requirement to give consumers whose complaint is not immediately settled written notice about how complaints are handled should be modified to give subscribers a brief period to investigate the complaint first. If the complaint is resolved in this time, the subscriber would not need to give the consumer the information. ASIC accepts this.

150 Most submissions supported giving subscribers one or two business days to resolve the complaint before the requirement for written notice applied.[54] The joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre and the submission by Care Financial Counselling Service opposed this proposal but argued that if it is adopted subscribers should be given only one day to resolve complaints before the requirement for written notice applied.[55] Abacus argued that specifying a number of days would be too prescriptive.[56]

151 On balance, we accept that it is reasonable that given the broad definition of complaint we are proposing under proposal D1, subscribers should have a brief period to investigate complaints before giving consumers written notice about their complaint handling processes. This will mean that where a complaint is resolved within this time, consumers will not be inundated with unnecessary information. It will also save paper, where this information is provided in hard copy.

[54] Law Council, *Submission* (27 April 2007) at 6; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 20; P Hobson, *Submission* (1 May 2007) at 12.
[55] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 24; Care Financial Counselling Service, *Submission* (31 May 2007) at 16.
[56] Abacus, *Submission* (25 June 2007) at 13.

Complaints involving two or more subscribers (proposal D3)

Proposal

D3 We propose to introduce a requirement for subscribers to respond to requests for information from another subscriber within 30 days, unless there are exceptional circumstances.

Your feedback

D3Q1 Do you agree with this proposal? Please give reasons.

Rationale

152 Section C of this consultation paper outlines industry-based reforms designed to remove barriers to participation in the ATM system. As noted above, the Australian Bankers Association argued that these reforms will require changes to the time frame for resolving complaints because where a consumer complains to a subscriber about an EFT transaction performed using an independent ATM, the subscriber will need to deal with the independent ATM owner to resolve the complaint.[57]

153 We propose to address this, at least in part, by introducing a requirement for subscribers to respond to requests for information from other subscribers about EFT code related issues within 30 days, unless there are exceptional circumstances.

154 This will of course only bind ATM owners that subscribe to the EFT Code. Section B of this consultation paper discusses possible ways to expand membership of the EFT Code, including making the Code mandatory.

Providing information to external dispute resolution schemes (proposal D4)

(January Consultation Paper, Q26)

Proposal

D4 We propose to amend the EFT Code so that where an external dispute resolution 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.

[57] Australian Bankers Association, *Submission* (6 June 2007) at 21.

Your feedback

D4Q1 Do you agree with this proposal? Please give reasons.

Rationale

155 The January Consultation Paper noted that external dispute resolution bodies sometimes have difficulty obtaining information from subscribers. It asked whether the EFT Code should be amended so that in this situation, external dispute resolution schemes are entitled to resolve factual issues on the basis of the information available.

156 A number of submissions supported this proposal.[58] The Banking and Financial Services Ombudsman argued that this amendment is unnecessary for it because its procedures already reflect this approach.[59] Abacus argued that this should be addressed in the rules of the external dispute resolution schemes rather than in the EFT Code.[60]

157 Our view is that there is merit in amending the EFT Code to expressly reflect this approach, to promote subscriber awareness of it.

Limitations period for complaints (proposal D5)

(January Consultation Paper, Q27)

Proposal

D5 We propose to amend the EFT Code to introduce a six-year time limit for complaints. 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.

Your feedback

D5Q1 Do you agree with this proposal? Please give reasons.

Rationale

158 Clause 4.4 of the EFT Code currently prohibits subscribers from imposing a time limit on complaints about mistaken or unauthorised transactions.

159 We accept that it may be difficult for subscribers to properly investigate very old complaints due to difficulty in obtaining information. Most external

[58] Bendigo Bank, *Submission* (date) at 2; Law Council, *Submission* (date) at 6; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 25; Care Financial Counselling Service, *Submission* (31 May 2007) at 18; Australian Bankers Association, *Submission* (date) at 22; P Hobson, *Submission* (1 May 2007) at 13.
[59] Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 22–23.
[60] Abacus, *Submission* (25 June 2007) at 13.

dispute resolution schemes impose a time limit. For example, the Financial Ombudsman Service applies a time limit from the time when the event to which the dispute relates occurred.

160 All submissions that addressed this issue supported introducing a time limit.[61] Suggestions for an appropriate time frame ranged from two months to six years.

161 While it is desirable for consumers to promptly review statements, consumers do not necessarily always do so within two months and sometimes it is not possible to do so (e.g. if the consumer is away on holiday). We believe that a six-year time frame is appropriate. This is also consistent with statutory limitations periods.

OTHER ISSUES

Time frame for resolving complaints

(January Consultation Paper, Q23)

162 Under clause 10 of the EFT Code, the time frame for resolving complaints is 45 days unless there are exceptional circumstances. If a subscriber cannot resolve a complaint within 45 days, it must inform the consumer, provide monthly progress reports and tell the consumer when a decision can reasonably be expected.

163 The January Consultation Paper asked whether any changes should be made to the 45-day time frame.

164 Two industry submissions argued that the time frame should be 45 business days.[62] This would effectively extend the time frame to nine weeks or 63 days. Given that there is scope under the current EFT Code to extend the time frame in exceptional circumstances, ASIC does not accept this argument.

165 The Australian Bankers Association argued that the industry-led ATM reforms discussed in Section C will require changes to the time frame for resolving complaints. Their argument is that a 45-day time frame may not be sufficient where a subscriber needs to deal with a third party ATM provider to resolve a complaint.[63] Proposal D 3 requires subscribers to respond to

[61] Bendigo Bank, *Submission* (27 April 2007) at 2; Suncorp, *Submission* (1 May 2007) at 5; ANZ, *Submission* (2 May 2007) at 5; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 25; Care Financial Counselling Service, *Submission* (31 May 2007) at 19; Abacus, *Submission* (25 June 2007) at 13; Australian Bankers Association, *Submission* (6 June 2007) at 22; P Hobson, *Submission* (1 May 2007) at 13. The Banking and Financial Services Ombudsman acknowledged that it may be reasonable to introduce a time limit: see Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 23.
[62] Suncorp, *Submission* (1 May 2007) at 4; ANZ, *Submission* (2 May 2007) at 5.
[63] Australian Bankers Association, *Submission* (6 June 2007) at 21.

requests from information from other subscribers within 30 days. We think that this proposal, combined with the ability to extend the timeframe in exceptional circumstances, addresses this issue.

166 Submissions by consumer groups argued that the time frame for resolving complaints should include a requirement to take account of situations where a consumer will suffer financial hardship as a result of the time taken to resolve a complaint.[64]

167 While ASIC supports subscribers taking account of financial hardship issues as part of dispute resolution processes, we do not consider that the EFT Code is an appropriate vehicle for this.

Internal dispute resolution

(January Consultation Paper, Q24–Q26)

168 The January Consultation Paper asked for information about the level of compliance with clause 10, which imposes a range of obligations relating to internal dispute resolution. Subscribers and the Banking and Financial Services Ombudsman reported reasonable compliance,[65] while submissions by consumer groups argued that there are compliance problems.[66]

169 Clause 10.12 provides that where a subscriber does not comply with the requirements under clause 10, or the liability allocation rules in clauses 5 and 6, an external dispute resolution body can determine that they are liable for the disputed transaction. The purpose of this clause is to provide an incentive for subscribers to implement sound internal dispute resolution procedures and compensate consumers for delays in resolving complaints.

170 The January Consultation Paper asked whether this incentive is effective. Most industry submissions argued that it is.[67] Two submissions argued that requiring subscribers to establish internal audit committees to investigate and report on non-compliance would also improve compliance with the internal dispute resolution requirements.[68] Our view is that in the absence of firm evidence of compliance problems, the introduction of additional compliance requirements is not justified.

---

[64] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 24; Care Financial Counselling Service, *Submission* (31 May 2007) at 17.
[65] Suncorp, *Submission* (1 May 2007) at 4; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 21.
[66] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 24; Care Financial Counselling Service, *Submission* (31 May 2007) at 17–18.
[67] Suncorp, *Submission* (1 May 2007) at 4; Abacus, *Submission* (25 June 2007) at 13.
[68] Australian Bankers Association, *Submission* (date) at 21; P Hobson, *Submission* (1 May 2007) at 13.

E Liability for unauthorised transactions and mistaken payments

Key points

ASIC proposes to retain the current approach to allocating liability for unauthorised transactions in clause 5 with proposed amendments to:

- provide that a consumer would liable for unauthorised transactions that occur because they leave a card in an active ATM which has automatically shut down within 40 seconds(see proposal E1);
- require subscribers to prohibit merchants from taking consumers' PINs as part of 'book up' practices in merchant agreements (see proposal E2); and
- deal with mistaken payments in the EFT Code (see proposal E3).

PROPOSALS

Liability for losses caused by a person leaving their card in a ATM (proposal E1)

(January Consultation Paper, Q33)

Proposal

E1 We propose to amend 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.

Your feedback

E1Q1 Do you agree with this proposal? Please give reasons.

Rationale

171 The EFT Code does not specifically allocate liability for unauthorised transactions that occur because a person leaves a card in an ATM. However, we understand that in practice, internal and external dispute resolution processes allocate liability to the consumer in this situation.

172 ASIC accepts that a person who uses an ATM is best placed to avoid the risk of loss in this situation by being careful to retrieve their card. We propose to

amend the EFT Code to reflect this. All the submissions that addressed this issue supported this proposal.[69]

173 We understand that ATMs owned by some subscribers currently shut down within 40 seconds after a consumer is prompted to withdraw their card and does not do so. ATMs owned by other subscribers require consumers to 'swipe' their card rather than enter it into a slot. We understand that these ATMs also close and revert to the welcome screen if a consumer does not enter an instruction within 15 seconds. Consumers must re-swipe their card to reactivate the ATM.

Book up (proposal E2)

(January Consultation Paper, Q39)

Proposal

E2 We propose to require subscribers to prohibit merchants from taking consumers' PINs as part of book up practices in merchant agreements.

Your feedback

E2Q1 Do you agree with this proposal? Please give reasons.

Rationale

174 The January Consultation Paper noted that the practice of book up is widespread in remote Aboriginal communities and that merchants can abuse the practice.

175 We propose to require subscribers to prohibit merchants from taking consumers' PINs as part of book up practices in merchant agreements. Our proposal does not seek to prohibit merchants holding consumers' cards as part of book up arrangements. Most submissions on this issue supported measures to restrict book up practices.[70] The Australian Competition and Consumer Commission argued that the EFT Code should require subscribers to specifically notify merchants that if they seek consumers' PINs, they are encouraging consumers to breach their contract with the subscriber.[71]

[69] Bendigo Bank, *Submission* (27 April 2007) at 2; Suncorp, S*ubmission* (1 May 2007) at 6; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 28; Abacus, *Submission* (25 June 2007) at 14; Australian Bankers Association, *Submission* (6 June 2007) at 24; Australian Payments Clearing Association, *Submission* (9 May 2007) at 7–8.
[70] Suncorp, S*ubmission* (1 May 2007) at 6; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 32; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 36; Abacus, *Submission* (25 June 2007) at 15; Australian Bankers Association, *Submission* (6 June 2007) at 25.
[71] Australian Competition and Consumer Commission, *Submission* (24 April 2007) at 3–4.

176 Our view is that a consumer will not be liable for unauthorised transactions performed by merchants under book up arrangements: see clause 5.2(a) of the EFT Code. While this protection is available under the EFT Code, requiring subscribers to prohibit merchants from taking consumers' PINS will clarify and strengthen this position. Our aim is to lessen the risk of abuse by some merchants from materialising in the first place. We consider this to be a preferable position to the alternative of subscribers having to resolve more claims of unauthorised transactions.

177 The Government of Western Australia has recently released a discussion paper about book up.[72] ASIC supports this work.

178 There may be situations where exemptions to this general prohibition may be appropriate. This consultation paper proposes that ASIC should be able to modify the EFT Code if necessary: see proposal G1. This power could be used to deal with such situations should the need arise.

Mistaken payments (proposal E3)

(January Consultation Paper, Q41)

179 Internet banking facilities allow consumers to use online banking to pay third parties. From time to time, people accidentally pay the wrong person (e.g. because they key in the wrong account number or because they have been given the wrong account number).

Proposal

E3 We propose to deal with the issue of mistaken payments in the EFT Code. We propose to convene a stakeholder roundtable to advance this issue in coming weeks. Your feedback

- E3Q1 Do you agree with this proposal? Why?
- E3Q2 What approach would provide the most effective consumer protection and best address the practical limitations consumers currently face when trying to exercise their legal right to recover mistaken payments?
- E3Q3 What would be the costs to subscribers and consumers?

[72] Department of Consumer and Employment Protection, *Book up: Running a tab, buying on tick or using other forms of informal credit*, Discussion Paper (February 2008).

Rationale

180 In ASIC's view, it is appropriate to deal with the issue of mistaken payments in the EFT Code as this Code is the single source, accessible body of rules for consumers around electronic banking.

181 While we do not have comprehensive data on the extent of mistaken payments using internet banking 'pay anyone' facilities, anecdotal evidence provided by the industry representative bodies suggests there are only a small number of mistaken payment complaints in practice.

182 The information provided by industry bodies also suggests that there are two causes of mistaken payments in these situations. First, some mistakes occur because a consumer makes an error in keying in the BSB or account number.

183 Mistakes also arise because the consumer is provided with an incorrect BSB or account number. However, we do not know what proportion of mistakes is attributable to each of these causes.

184 In designing a policy response to the problem of mistaken payments, our primary concern is to provide an effective mechanism for consumers to recover mistaken payments. Our objectives are to:

(a) implement systems changes that minimise the possibility of consumers making a mistake when they key in an account number; and

(b) establish a system that ensures that consumers who make a mistaken payment can recover their money; without

(c) requiring consumers to initiate legal proceedings against the unintended recipient of the mistaken payment.

185 We are also mindful of the fact that financial institutions have encouraged consumers away from using cheques, the most expensive payments instrument, towards online forms of payment. This has created considerable savings for institutions, removed existing protections for consumers and created new risks for them.

186 It is also worth noting that there is a cause of action that allows people to recover payments made under a mistake of fact.[73] Arguably, this would apply at least where a consumer makes a mistaken payment because of a keying error. It is not clear whether it would apply where they are given the wrong information by a third party.

[73] Alan Tyree, 'Mistaken internet banking', March 2003, <http://austlii.edu.au/~alan/mistaken-epayments.html>.

187 In practice, however, it is extremely difficult for consumers to recover mistaken payments. A consumer who pays the wrong person by mistake will not generally know the identity of the person they have paid by mistake. Further, in the vast majority of cases the cost of legal proceedings outweighs the amount of money involved.

188 We propose to convene a roundtable to advance this issue in coming weeks. We will invite industry and consumer representatives as well as the Financial Ombudsman Service to participate in this process.

189 Stakeholders have raised several concerns about amending the EFT Code to deal with mistaken payments. The following paragraphs summarise these concern.

Ambiguity in the law of mistaken internet payment

190 One of the concerns raised by stakeholders is that amending the EFT Code to deal with mistaken payments may (depending on the approach taken) create new legal rights that do not currently exist.

191 While the law in this area is not settled, our view, as noted at paragraph127, is that the role of the EFT Code is to do more than restate the law by offering consumer protection benefits that go beyond the protections afforded by law and providing for a higher standard of conduct than required by law.

Risk of abuse and fraud

192 There is also a concern that depending on the approach taken, dealing with mistaken payments in the EFT Code could make the system more open to abuse and fraud by account holders who collude with each other, or where a single person opens two accounts using false identities.

193 While we acknowledge this concern, we believe that this risk is and will always be present in any electronic payment system. The risk can be managed by building a process into the system allowing subscribers to investigate a claim by a consumer that they have made a mistaken payment and to reject it if the subscriber reasonably believes that the payment was not a mistake. A consumer that did not accept this decision could complain to an EDR scheme. This is comparable to the approach taken to disputes about unauthorised transaction claims.

194 Subscribers also have the option of switching off a customer's access to internet banking or ending their relationship with the customer entirely.

195 We anticipate that if the EFT Code is amended to deal with mistaken payments, industry would actively monitor the incidence of abuse and fraud involving the mistaken payments regime. If the data showed a significant increase of fraud and abuse, theapproach to dealing with mistaken payments under the EFT Code would need to be reconsidered.

Increased carelessness

196 It is also argued that, if the EFT Code is amended to deal with mistaken payments, depending on the approach taken, consumers may have less incentive to ensure that they enter the intended recipient's account details correctly. ASIC does not accept this. The inconvenience and time that will still be involved in fixing a mistaken payment will ensure that getting the numbers right remains a priority for consumers.

Increased costs

197 Another concern is that amending the EFT Code to deal with mistaken payments could lead to increased costs for ADI subscribers.

198 The migration from the cheque payment system to online banking has been driven by the ADIs using pricing mechanisms. It has meant moving from an expensive payment mechanism for ADI's to administer to one that is considerably cheaper. Consumers were well protected by the law when using cheques. They should be no less protected when using the pay anyone facilities which systems are driving consumers to use more and more.

199 Any increase of costs now may be justified for a better operation of the system in the long run.

OTHER ISSUES

Liability for unauthorised transactions

(January Consultation Paper, Q28–30, 32)

200 Clause 5 sets out how liability is allocated for unauthorised transactions. We propose to retain the current approach.

201 The January Consultation Paper asked whether consumers should be exposed to additional liability for unauthorised transactions arising from malicious software attacks or 'phishing' attacks.

202 All submissions opposed modifying the current rules for allocating liability for unauthorised transactions.[74] Reasons included:

[74] Suncorp, *Submission* (1 May 2007) at 5; ANZ, *Submission* (2 May 2007) at 3; Victoria Police, *Submission* (12 April 2007) at 1–3; Consumer Telecommunications Network, *Submission* (13 April 2007) at 4; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 8 and 26–33; Care Financial Counselling Service, *Submission* (31 May 2007) at 3; AUSCert, *Submission* (30 April 2007) at 2–4 and 7; Law Council, *Submission* (27 April 2007) at 7; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 9-10 and 25; Abacus, *Submission* (25 June 2007) at 14; Australian Bankers Association, *Submission* (6 June 2007) at 23; BPay, *Submission* (8 May 2007) at 4 and 9–11; P Hobson, *Submission* (1 May 2007) at 14–15; N Murdoch, *Submission* (27 April

- technical limitations mean it is not possible to prevent online fraud (home computers were not designed as secure platforms);
- compared with subscribers, consumers do not have the skills or resources to implement adequate online security;
- determining liability would involve extensive forensic analysis that would outweigh any benefit; and
- imposing additional liability on consumers would undermine community trust in online banking.

203 As one submission noted, if a consumer experiences multiple loses from online fraud, subscribers can withdraw the consumer's access to online banking.[75]

204 The January Consultation Paper also asked whether the imposition of liability on consumers who act with extreme carelessness should be extended.

205 No submissions supported this, although a small number of submissions argued that further examples dealing with extreme carelessness in implementing online security measures should be included.[76]

206 We do not propose to extend the circumstances in which consumers are liable for unauthorised transactions as a result of extreme carelessness. In light of the feedback in submissions that the EFT Code should be reformulated as a set of less prescriptive, more flexible high level principles (see paragraphs 80 and 112 of this paper), we also do not propose to include additional specific examples of extreme carelessness.

Restriction on PINs based on birth date or name

(January Consultation Paper, Q31)

207 Clause 5.6(d) provides that a subscriber is not liable for losses resulting from unauthorised transactions where the consumer has chosen a PIN based on their birth date or name after the subscriber has instructed them not to do so.

208 Most submissions reported that subscribers rarely relied on this provision but supported retaining this restriction in its current form because it serves as a

---

2007); Xamax Consultancy, *Submission* (12 April 2007) ; A Tyree, *Submission* (15 February 2007) at 1–3.Contrast Australian Settlements Ltd, *Submission* (24 April 2007) at 2.

[75] BPay, *Submission* (8 May 2007) at 4 and 9–11.

[76] Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 27; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 34; Australian Bankers Association, *Submission* (6 June 2007) at 24; P Hobson, *Submission* (1 May 2007) at 16. Suncorp, *Submission* (1 May 2007) at 5 argued that that clause 5 should include additional examples dealing with extreme carelessness in failure to implement adequate online security. See also Australian Payments Clearing Association, *Submission* (9 May 2007) at 7 and Abacus, *Submission* (25 June 2007) at 14.

basis for subscribers to remind consumers not to choose a PIN based on their birth date or name.[77]

209 One submission argued that in reality, consumers often share PINs.[78] Examples include elderly people, people with disabilities and married couples. This submission argued that it may be appropriate to modify the EFT Code to reflect this.

210 While we recognise the importance of this issue, our view is that it would be more appropriate to address it through traditional tools such as powers of attorney and guardianship arrangements.

Unreasonable delay in notifying security breaches

(January Consultation Paper, Q34–Q36)

211 Clause 5.5(b) allocates liability for losses arising from unauthorised transactions if a consumer unreasonably delays telling a subscriber after becoming aware of the misuse, loss or theft of a 'device forming part of the access method' or that the security 'of all the codes forming part of the access method' has been breached.

212 The January Consultation Paper asks whether this clause should be expanded to cover unreasonable delay in reporting online security breaches. Submissions were divided on this issue.[79] This consultation paper proposes redrafting the EFT Code in plain English: see proposal B6. As part of this process, we will redraft this clause to make it technology neutral.

213 The joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre argued that unreasonable delay is an important test of liability that should apply in all relevant circumstances, but emphasised that it should only apply where the consumer becomes aware of a security breach.[80] This is currently a requirement and we propose to retain it.

214 In practice, many consumers do not have adequate skills to identify online security breaches. Further, it is not possible for consumers to identify some online security breaches due to the sophisticated nature of some forms of online fraud such as malicious software. We recognise that it is important to

[77] Suncorp, *Submission* (1 May 2007) at 5; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 26; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 33; Abacus, *Submission* (25 June 2007) at 14; Australian Bankers Association, *Submission* (6 June 2007) at 23.
[78] Bendigo Bank, *Submission* (27 April 2007) at 2.
[79] Suncorp, *Submission* (1 May 2007); Abacus, *Submission* (26 June 2007) at 15 and Australian Payments Clearing Association, *Submission* (9 May 2007) at 8 supported this. The Banking and Financial Services Ombudsman, *Submission* (3 May 2007) opposed this.
[80] The joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 35.

consider this when assessing whether a consumer has unreasonably delayed reporting a breach of online security.

215 The January Consultation Paper also asked whether the standard of unreasonable delay should be replaced by a specific time frame. Submissions did not support this.[81] We do not propose to replace the current standard with a specific time frame.

Is there a case for increasing the current 'no fault' amount of $150?

(January Consultation Paper, Q37–Q38)

216 The January Consultation Paper asked whether the current 'no fault' amount of $150 should be increased. Some submissions supported increasing this amount in certain circumstances.[82] Bendigo Bank argued that the amount should be a percentage of the amount disputed. The Banking and Financial Services Ombudsman suggested increasing the amount to a percentage for higher value transactions. Abacus also suggested increasing the amount for higher value transactions. Suncorp simply argued that consideration should be given to increasing the limit.

217 On the other hand, the Australian Bankers Association, the joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre and a legal practitioner supported the current no-fault amount.[83] In particular, consumer groups argued that $150 is a significant amount for low income and disadvantaged consumers.

218 This consultation paper raises for further consideration the possibility of extending the consumer protections afforded by the EFT Code to protect small business consumers: see proposal B7. As noted there, ASIC accepts that some aspects of the EFT Code may not be appropriate in the small business context. For example, if the EFT Code is extended to cover small business consumers, the liability allocation rules may need to be adjusted to reflect the higher value of small business transactions. It may be appropriate that a no fault liability amount is set at 5% of the amount in dispute for disputes between subscribers and small business consumers.

---

[81] Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 30; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 35; Abacus, *Submission* (25 June 2007) at 15; Australian Bankers Association, *Submission* (6 June 2007) at 25.
[82] Bendigo Bank, *Submission* (27 April 2007) at 2; Suncorp, *Submission* (1 May 2007) at 6; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 31; Abacus, *Submission* (25 June 2007) at 15.
[83] *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre (30 May 2007) at 35–36; Australian Bankers Association, *Submission* (6 June 2007) at 25; P Hobson, *Submission* (1 May 2007) at 16.

219 Apart from this, ASIC agrees that $150 is a significant amount for low income and disadvantaged consumers. We do not propose to make any other changes to the current 'no fault' amount.

Liability in cases of system or equipment malfunction

(January Consultation Paper, Q40)

220 Clause 6.1 makes subscribers liable for losses arising from system or equipment malfunction when this causes the failure of a transaction that has been accepted into the system according to a consumer's instructions.

221 This was intended to cover systems and equipment owned by third parties (e.g. independent ATMs) although it has been suggested that the drafting of clause 6.1 does not achieve this.

222 The January Consultation Paper proposed amending clause 6.1 to make it clear that subscribers are liable for losses arising from third party system or equipment malfunction.

223 The Australian Bankers Association, Abacus and APCA opposed this approach in that after the proposed ATM reforms, consumers will be using independent ATMs. In this situation, subscribers will have no commercial relationship with the independent ATM owner and the consumer will have a direct commercial relationship with the independent ATM owner. These submissions argued that where a consumer complained to a subscriber about losses arising from a failed transaction caused by system or equipment malfunction and the system or equipment was owned by a third party, the subscriber should not be liable and the third party ATM owner should be liable.[84]

224 Our guiding philosophy has always been that the person who is best placed to investigate and resolve a complaint should have the onus of doing so. We believe that subscribers, rather than consumers, are better placed to investigate and resolve complaints in this situation. While it is open for consumers to complain directly to the independent ATM provider, they can choose to complain to their provider. Our view is that this requirement should continue to apply as their provider will be better placed than the consumer to resolve the complaint.

225 This consultation paper discusses possible ways to expand membership of the EFT Code, including making the Code mandatory for all businesses that offer electronic payments, including independent ATM owners: see proposal B5.

[84] Australian Bankers Association, *Submission* (6 June 2007 at 25; Abacus, *Submission* (25 June 2007) at 15; Australian Payments Clearing Association, *Submission* (9 May 2007) at 8.

F Electronic communications and privacy

Key points

ASIC proposes to:

- amend the requirements for delivering information electronically (see proposal F1); and
- introduce new requirements for what is printed on receipts to protect consumers' privacy (see proposal F2).

PROPOSALS

Clarifying the requirements for electronic communication (proposal F1)

(January Consultation Paper, Q60–Q63)

235 We propose to modify the requirements so that subscribers can deliver information that must be disclosed under the EFT Code electronically.

Proposal

F1 We propose to:

(a) 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; and

(b) impose the following conditions:

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

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

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

(iv) 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;

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

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

Your feedback

F1Q1 Do you agree with this proposal? Please give reasons.

F1Q2 Is 18 months/two years a reasonable period for requiring information to be available on a website? If not, what would be an alternative?

F1Q3 What are the likely cost implications to subscribers of changing systems to meet the proposed conditions?

Rationale

226 Several submissions to the January Consultation Paper supported amending the EFT Code to simplify the conditions for delivering disclosure obligations under the EFT Code electronically.[85] ASIC considers that electronic communication can be an effective way to disclose information to consumers, provided that certain conditions are met. We also acknowledge the costs savings to subscribers, and environmental benefits, of being able to provide information electronically.

227 Our proposal is broadly consistent with ASIC Consultation Paper 93 *Facilitating online financial services disclosures* (CP 93).

228 Many submissions supported using the Code of Banking Practice as a model. Under the Code of Banking Practice, a subscriber and a consumer can agree that all information that must be given under that Code can be given electronically, subject to certain conditions.[86]

229 Our proposal is consistent with clause 33 of the Code of Banking Practice with one exception. Under our proposal, consumers are entitled to request hard copy of statements for up to six years if they are not still available electronically to download and print. Under the Code of Banking Practice, consumers are entitled to request hard copy statements for up to six months.

230 In September 2007, the Government amended the Corporations Act to permit a range of notices relating to annual financial reports to be delivered electronically.[87]

231 Submissions to the January Consultation Paper were divided on this issue. One submission supported consumers being able to obtain hard copy statements for up to six months, in line with the Code of Banking Practice.[88] The Australian Bankers Association argued that providing hard copy

[85] Law Council of Australia, *Submission* (27 April 2007) at 4; Abacus, *Submission* (25 June 2007) at 12; P Hobson, *Submission* (1 May 2007) at 10.
[86] Code of Banking Practice clause 33.
[87] *Corporations Amendment Regulations 2007 (No 13)*, reg 5.6.11A.
[88] Suncorp, *Submission* (1 May 2007) at 9.

information on request is ordinary business practice. Therefore, it is unnecessary and overly prescriptive for the EFT Code to address this.[89]

232 The Banking and Financial Services Ombudsman argued that generally subscribers should be required to provide hard copy statements, because hard copy statements are crucial to the investigation of disputes and for consumers to manage their financial affairs (e.g. to comply with taxation requirements).[90] ASIC accepts this argument.

233 Our proposal also requires subscribers to make information available on a website for a reasonable period. We are interested in feedback about what constitutes a reasonable period and whether this differs for terms and conditions, changes to terms and conditions, receipts and statements.

234 The January Consultation Paper noted at paragraph 10.16 that clause 22.2(b)(ii) of the EFT Code implies that a consumer that agrees to receive information electronically must confirm receipt of each communication. ASIC's understanding is that the drafter of the EFT Code did not intend this. We accept that it would be an onerous and unworkable requirement. We propose to delete this clause. All submissions on this issue agreed with this proposal.[91]

235 The January Consultation Paper also asked whether the EFT Code should address the situation where a subscriber sends an email to a consumer containing information mandated under the EFT Code and receives a mail delivery failure or 'bounce back' notice.

236 Submissions opposed any changes to the EFT Code to address this.[92] We will require subscribers to have a user-friendly process for consumers to update their email address. We consider that this requirement adequately addresses this issue.

Privacy issues for receipts (proposal F2)

(January Consultation Paper, Q57–Q59)

Proposal

F2 We propose to require that receipts:

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

[89] Australian Bankers Association, *Submission* (6 June 2007) at 32.
[90] Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 34.
[91] Suncorp, *Submission* (1 May 2007) at 9; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 42; Abacus, *Submission* (25 June 2007) at 18; Australian Bankers Association, *Submission* (6 June 2007) at 32.
[92] Suncorp, *Submission* (1 May 2007) at 9; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 35; Abacus, *Submission* (25 June 2007) at 18; Australian Bankers Association, *Submission* (6 June 2007) at 33; BPay, *Submission* (8 May 2007) at 16.

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

Your feedback

F2Q1 Do you agree with this proposal? Please give reasons.

F2Q2 What are the likely cost implications to subscribers of changing systems to meet this requirement?

Rationale

237 The January Consultation Paper asked whether the EFT Code should require that receipts:

- include a truncated version of account number; and
- do not include the expiry date or any other extraneous information.

238 Most submissions supported this.[93] Including a full account number or expiry date raises privacy concerns. Our proposal addresses these concerns.

OTHER ISSUES

Hyperlinks

(January Consultation Paper, Q60)

239 The EFT Code imposes a range of disclosure obligations on subscribers, including obligations to give consumers terms and conditions, notice of changes to terms and conditions, receipts and statements. Clause 22 of the EFT Code allows information to be provided electronically, subject to certain conditions.

240 One condition is that the consumer must be able to readily retrieve the information by electronic communication. The examples given include sending the consumer an email containing an electronic link to the information at the subscriber's website.

241 There is a risk that using hyperlinks might facilitate 'phishing' and other internet scams. To reduce this risk, ASIC, the Australasian Consumer Fraud Taskforce and the banking industry have for some time encouraged consumers not to follow hyperlinks in emails purporting to be from their financial services provider.

[93] Bendigo Bank, *Submission* (27 April 2007) at 2; Suncorp, *Submission* (1 May 2007) at 8; Law Council of Australia, *Submission* (27 April 2007) at 13; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 15; Victoria Police, *Submission* (12 April 2007) at 4; P Hobson, *Submission* (1 May 2007) at 20. See also Abacus, *Submission* (25 June 2007) at 18; Australian Bankers Association, *Submission* (6 June 2007) at 30; Australian Payments Clearing Association, *Submission* (9 May 2007) at 10.

242 The January Consultation Paper proposed prohibiting the use of hyperlinks. All submissions on this issue supported this proposal.[94]

243 On the other hand, hyperlinks are increasingly prevalent and are a quick and simple way to deliver information to consumers. ASIC has recently released a consultation paper that proposes granting relief to enable financial services provider to use hyperlinks to deliver disclosure required under Chapter 7 of the Corporations Act using hyperlinks.[95]

Hyperlinks

F3 We are interested in your views on using hyperlinks to deliver disclosures.

Your feedback

F3Q1 Should the EFT Code prohibit the use of hyperlinks to deliver disclosure required under the EFT Code?

F3Q2 What would be the costs savings if subscribers were permitted to use hyperlinks?

F3Q3 If hyperlinks are permitted, should this be limited in any way? For example, should hyperlinks be prohibited where they are used to enable a consumer to retrieve personal information which would then require them to enter a password to access the information?

Privacy guidelines

(January Consultation Paper, Q55–Q56)

244 The January Consultation Paper sought feedback on whether to modify or extend the privacy guidelines in clause 21.2 of the EFT Code. Most submissions did not support this.[96] We do not propose to modify or extend clause 21.2 as part of this review.

245 The privacy guidelines under clause 21.2 are not binding. The January Consultation Paper asked whether the guidelines should be made contractually binding between subscriber and consumer.

---

[94] Suncorp, *Submission* (1 May 2007) at 9; Abacus, *(Submission)* at 18*;* Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 34; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 42; Australian Bankers Association, *submission* (6 June 2007) at 31; BPay, *Submission* (8 May 2007) at 16; P Hobson, *Submission* (1 May 2007) at 20; A Tyree, *Submission* (15 February 2007) at 7.

[95] See ASIC Consultation Paper 93 *Facilitating online financial services disclosures* (CP 93), issued April 2008, at www.asic.gov.au/CP.

[96] Suncorp, *Submission* (1 May 2007) at 8; Law Council, *Submission* (27 April 2007) at 13; Abacus, *Submission* (25 June 2007) at 17; BPay, *Submission* (8 May 2007) at 5 and 16. Contrast P Hobson, *Submission* (1 May 2007) at 20 who argued that subscribers should be required to notify consumers of a security breach on their account. *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 41 argued that the existing requirements should be retained. The Australian Privacy Foundation supported this submission: Australian Privacy Foundation, *Submission* at 1.

246 Most submissions did not support this.[97] The Law Council, the joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre, the Australian Privacy Foundation and a submission by an individual practitioner supported this. We accept that if the EFT Code is to focus on high level principles, it would be overly prescriptive for it to make the privacy guidelines binding. We do not propose to make the privacy guidelines contractually binding as part of this review.

[97] Law Council of Australia, *Submission* (27 April 2007) at 13 and P Hobson, *Submission* at 20 supported making the privacy guidelines contractually binding. *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 41 argued that certain elements should be contractually binding, but that some elements of the privacy guidelines should be removed. Abacus, *Submission* (25 June 2007) at 17; Australian Bankers Association, *Submission* (6 June 2007) at 30 and Suncorp, Submission (1 May 2007) opposed this.

G Administration and review

Key points

ASIC proposes that:

- we should have a general power to modify the application of the EFT Code as it applies to particular products or classes of products (see proposal G1);
- the EFT Code should be reviewed every five years (see proposal G2); and
- we would monitor compliance with specific requirements of the EFT Code, including a requirement for subscribers to provide certain information on unauthorised transactions (see proposals G3 and G4).

PROPOSALS

Modifying the EFT Code (proposal G1)

(January Consultation Paper, Q65)

Proposal

G1 We propose that ASIC should have a general power to modify the EFT Code as it applies to a product or class of products, subject to principles of procedural fairness.

Your feedback

G1Q1 Do you agree with this proposal? Please give reasons.

Rationale

247 ASIC has limited powers to modify the application of specific aspects of the EFT Code.[98] To date we have not used these powers.

248 We propose to introduce a general power to modify the EFT Code. We think this is potentially a beneficial mechanism for dealing with new circumstances and enhancing the flexibility and responsiveness of the EFT

[98] See EFT Code clause 23.3 (power to modify the application of Part B); clause 23.4(a) (limited power to modify disclosure obligations); clause 23.4(b) (limited power to modify requirement to notify consumers of surcharges for using foreign electronic equipment); clause 23.4(c) (power to modify internal dispute resolution requirements).

Code to marketplace developments. A number of submissions supported this proposal,[99] although others opposed it.[100]

249 A number of submissions that supported introducing a general power to modify the EFT Code emphasised the importance of comprehensive stakeholder consultation before any modifications. We recognise the importance of consulting with EFT Code subscribers and other stakeholders before exercising this power and we will build this requirement into the revised EFT Code.

Reviews (proposal G2)

(January Consultation Paper, Q67)

Proposal

G2 We propose to require that the EFT Code must be reviewed every five years.

Your feedback

G2Q1 Do you agree with this proposal? Please give reasons.

Rationale

250 ASIC is currently required to undertake periodic reviews of the EFT Code: clause 24.1.

251 Regular reviews are an accepted feature of administering codes of conduct. All submissions on this issue supported regular reviews of the EFT Code with time frames of three or five years.[101]

252 We consider that it is appropriate that the EFT Code specify the frequency of reviews. Given the relative maturity of the EFT Code and our proposal to amend the EFT Code to give ASIC a power to modify the application of the code (see proposal G1), we consider that going forward, five-yearly reviews of the EFT Code are appropriate. If the need arises for reviews on specific issues between the five-yearly reviews, additional reviews could be conducted.

---

[99] Suncorp, *Submission* (1 May 2007) at 9–10; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 35; Joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 44; Abacus, *Submission* (25 June 2007) at 18; Australian Payments Clearing Association, *Submission* (9 May 2007) at 12.
[100] Law Council of Australia, *Submission* (27 April 2007) at 14; Australian Bankers Association, *Submission* (6 June 2007) at 33.
[101] Suncorp, *Submission* (1 May 2007); Law Council of Australia, *Submission* (27 April 2007); Joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 45; Abacus, *Submission* (25 June 2007) at 19; Australian Bankers Association, *Submission* (6 June 2007) at 34; Australian Payments Clearing Association, *Submission* (9 May 2007) at 12; BPay, *Submission* (8 May 2007) at 5; P Hobson, *Submission* (1 May 2007) at 21.

253 ASIC Regulatory Guide 183 *Approval of financial services codes of conduct* (RG 183) requires that codes must provide for reviews at least every three years.[102] We will update this requirement to provide for five-yearly reviews.

Monitoring compliance (proposal G3 and G4)

(January Consultation Paper, Q64 and Q66)

Proposal

G3 We propose that going forward, subscribers should be required to give ASIC 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.

Subscribers should be required to provide this data annually.

G4 We also propose that ASIC will also 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. ASIC may also use other monitoring mechanisms such as shadow shopping exercises.

Your feedback

G4Q1 Do you agree with the proposal for subscribers to provide information about the number, nature and resolution of unauthorised transactions? Please give reasons.

G4Q2 If you are a subscriber or potential subscriber, would you be able to provide this data annually?

G4Q3 Do you agree with the proposal for ASIC to monitor compliance? Please give reasons.

Rationale

254 The January Consultation Paper asked how compliance with the EFT Code should be monitored.

255 Until recently, ASIC has monitored compliance through an annual self-assessment survey which subscribers must complete. We examine the survey

[102] See ASIC Regulatory Guide 183 *Approval of financial services sector codes of conduct* at RG 183.79–RG 183.81.

results and report on non-compliance and aggregated transaction and complaints data.

256 There have been significant difficulties with this process because subscribers cannot consistently extract and report data about transactions and complaints.

257 ASIC's view is that effective compliance monitoring is an essential feature of an effective code of conduct.

258 Submissions were divided on the most appropriate approach to compliance monitoring:[103]

- Bendigo Bank favoured requiring subscribers to submit a simplified quarterly report.
- Suncorp argued that subscribers should be required to self-report breaches.
- The joint submission by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre supported one-off evaluations such as shadow shopping exercises.
- Abacus argued that subscribers should be required to complete an issues-based survey and certify compliance and ASIC should collect data about complaints from EDR schemes.
- The Australian Bankers Association argued a Working Group should be establish to improve the current requirements.

259 We accept that requiring subscribers to provide compliance reports covering every clause of the EFT Code imposes an unreasonable compliance burden. For this reason, we do not propose to continue the current approach.

260 ASIC's view is that the most productive use of everyone's resources is for compliance monitoring to focus on specific areas each time, either because problems are suspected or because they are particularly important and that this is done well, rather than attempting a comprehensive, but probably more superficial, regular review of everything.

261 Our view is that the most important information we can obtain about EFT Code compliance is regular statistical information about the number and type of unauthorised transactions and how subscribers resolve disputes about unauthorised transactions.

262 From time to time, it may also be appropriate to focus on other specific consumer protection issues. This may be relevant to further reviews of the

[103] Bendigo Bank, *Submission* (27 April 2007) at 2; Suncorp, *Submission* (1 May 2007) at 10; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 44; CARE Financial Counselling Service, *Submission* (31 May 2007) at 18; Abacus, *Submission* (25 June 2007) at 19; Australian Bankers Association, *Submission* (6 June 2007) at 33; Australian Payments Clearing Association, *Submission* (9 May 2007) at 12; P Hobson, *Submission* (1 May 2007) at 21; Australian Settlements Limited, *Submission* (24 April 2007) at 4.

EFT Code to inform our consumer protection activities generally. For example, in future it may be appropriate to consider the extent and nature of mistaken internet payments.

263 We will determine the focus of any additional specific compliance monitoring activities in consultation with subscribers and other stakeholders, including consumer representatives.

264 Subscribers may be required to report information about particular EFT Code requirements as part of this targeted compliance monitoring. ASIC may also use other monitoring mechanisms such as shadow shopping exercises to conduct targeted compliance monitoring of the EFT Code.

OTHER ISSUES

Who should be responsible for administering the EFT Code?

265 The January Consultation Paper asked whether ASIC should continue to be primarily responsible for administering the EFT Code. Although one submission argued that it is not appropriate for ASIC to administer an industry code,[104] all other submissions that addressed this issue supported ASIC continuing to administer the EFT Code.[105] Given the number of different industry sectors covered by the code, our view is that ASIC remains the most suitable body to be primarily responsible for administering the EFT Code.

[104] Suncorp, *Submission* (1 May 2007) at 9.
[105] Law Council of Australia, *Submission* (27 April 2007) at 14; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 14; Banking and Financial Services Ombudsman, *Submission* (3 May 2007) at 35; *Joint submission* by Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law, Griffith Law Centre at 44; Abacus, *Submission* (25 June 2007) at 18; Australian Bankers Association, *Submission* (6 June 2007) at 33; Australian Payments Clearing Association, *Submission* (9 May 2007) at 12.

H Regulatory and financial impact

266 In developing the proposals in this paper, we have carefully considered their regulatory and financial impact. On the information currently available to us we think they will strike an appropriate balance between:

(a) consumer protection; and

(b) regulatory impact.

267 Before settling on a final policy, we will comply with the requirements of the Office of Best Practice Regulation (OBPR) by:

(a) considering all feasible options;

(b) if regulatory options are under consideration, undertaking a preliminary assessment of the impacts of the options on business and individuals or the economy;

(c) if our proposed option has more than low impact on business and individuals or the economy, consulting with OBPR to determine the appropriate level of regulatory analysis; and

(d) conducting the appropriate level of regulatory analysis, that is, complete a Business Cost Calculator report (BCC report) and/or a Regulation Impact Statement (RIS).

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

269 To ensure that we are in a position to properly complete any required BCC report or RIS, we ask you to provide us with as much information as you can about our proposals or any alternative approaches including:

(a) the likely compliance costs;

(b) the likely effect on competition; and

(c) other impacts, costs and benefits,

See ‘The consultation process’ p. 5.

Appendix 1: Submissions to the January Consultation Paper

In January 2007, ASIC released a consultation paper as part of our review of the EFT Code, *Reviewing the EFT Code* (January Consultation Paper).

We received over 40 public submissions from consumers and consumer bodies, financial services providers, industry bodies, businesses, lawyers, academics, law enforcement bodies, government agencies and experts in online fraud. We also received a number of confidential submissions.

Table 5: List of non-confidential submissions

- Abacus Australian Mutuals
- ACCC
- ANZ
- A Tyree
- AusCERT
- Australian Bankers Association
- Australian Merchant Payments Forum
- Australian Payments Clearing Association
- Australian Privacy Foundation
- Australian Settlements
- Banking and Financial Services Ombudsman
- Bendigo Bank
- BPAY
- B Caelli
- Care Financial Counselling Service
- Choice, Consumer Action Law Centre and Centre for Credit and Consumer Law
- Consumers' Telecommunications Network
- Family Business Australia
- Hobson Legal
- J S Roth
- Law Council of Australia
- M Murphy
- N Murdoch
- Queensland Retail Traders and Shopkeepers Association
- Reserve Bank of Australia
- Small Business Development Corporation, Western Australia
- S Saunders
- S Singh
- Suncorp
- Suncorp letter to Australian Financial Review
- Trust Defender
- Victoria Police
- Xamax Consultancy

Appendix 2: International developments

Canada

In 2006, the Canadian Government conducted a review of the federal financial services regulatory framework. The resulting recommendations were released in a report '2006 Financial Institutions Legislation Review: Proposals for an Effective and Efficient Financial Services Framework' (the White Paper). The White Paper noted general support for the enhancement of consumer protection for all forms of electronic transactions,[106] and recommended adopting a voluntary consumer protection regime to cover electronic transactions, building on the Canadian Code of Practice for Consumer Debit Card Services.[107]

A discussion paper 'Developing a Code of Conduct for Electronic Funds Transfer' (the Discussion Paper) was released in September 2007. It proposed introducing a new EFT Code covering face-to-face, online debit transactions and electronic banking, including debit cards, stored value cards, on-line and telephone banking. The new code would not cover credit card transactions, but stored value products offered by credit card issuers would be included.[108]

Work on the Canadian EFT Code will focus on developing general principles including a commitment to clear and concise language in communicating with consumers, the provision of safe and secure payment services, and a timely response to consumer concerns and complaints.[109]

A working group consisting of industry representatives, consumer groups, provincial governments and other interested parties has been formed to discuss the development of the Canadian EFT Code. It is anticipated that it will be ready for industry adoption in 2008. The Financial Consumer Agency of Canada will monitor the adherence to the code by federally-regulated financial institutions.[110]

European Union

In October 2007, the Council of the European Union (EU) adopted a directive establishing a legal framework for payment services in the EU (the EU Directive).[111] The EU Directive harmonises the rules that apply to payment services in the EU.[112]

---

[106] White Paper, p 5.
[107] White Paper, p 10.
[108] Discussion Paper, p 3.
[109] Discussion Paper, p 2.
[110] White Paper, p 10.
[111] Available at http://register.consilium.europa.eu/pdf/en/07/st03/st03613.en07.pdf. See also: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:HTML
[112] Press Release, Council of the European Union, available at http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/misc/96508.pdf

The EU Directive applies to six categories of 'payment services providers': credit institutions, electronic money institutions, post office giro institutions, payment institutions, the European Central Bank and national central banks, and member states or their regional or local authorities.[113]

The EU Directive includes provisions on liability for unauthorised transactions. A user may be reimbursed for an unauthorised transaction if they notify the provider without undue delay on becoming aware of any unauthorised or incorrectly executed transaction. The notification must be made no later than 13 months after the debit date, unless the provider has failed to provide information on that payment transaction in accordance with the EU Directive.[114] Where a user denies having authorised an executed payment transaction, the onus is on the provider to prove that the transaction was properly executed and not affected by a technical breakdown or other deficiency.[115]

A user will be liable for all unauthorised transaction losses incurred by them acting fraudulently or with gross negligence in failing to:

- use the payment instrument in accordance with the governing terms and conditions;
- take all reasonable steps to keep its personalised security features safe; or
- notify the provider of the loss, theft, misappropriation or an unauthorised use of a payment instrument.[116]

Otherwise, the user's liability is limited to a maximum of EUR 150 before notification to the provider. If, however, the provider does not provide means for notification, the user will not be held liable unless the user had acted fraudulently. Following notification, the user is not liable for any financial consequences of the unauthorised transaction, except where the user has acted fraudulently.[117]

EU members are also required to ensure that adequate and effective out-of-court complaint and dispute resolution procedures are available for disputes arising under the EU Directive.[118]

The EU Directive will be reviewed for its implementation and effectiveness by 1 November 2012.[119]

[113] Art 1(1), EU Directive.
[114] Art 58, EU Directive.
[115] Art 59(1), EU Directive.
[116] Art 61(2) and art 56, EU Directive.
[117] Art 61, EU Directive.
[118] Art 83(1), EU Directive.
[119] Art 87, EU Directive.

Hong Kong

The Hong Kong Code of Banking Practice (HK Code) is a voluntary code issued for institutions dealing with consumers.[120] It covers current accounts, savings, other deposit accounts, loans and overdrafts, card services, electronic banking services and stored value card services.[121] The current revised HK Code is effective from 1 December 2001.

Under the HK Code, subscribers must give consumers 30 days' notice before introducing any changes in fees, charges, liabilities or obligations of consumers.[122] A shorter notice period of 14 days applies to dormant accounts.[123] Where the changes are substantial or complicated, a written summary of the key features of the changes must be provided to consumers.[124] While the HK Code recommends individual notification as an effective means of notifying changes to consumers, it recognises that such method may not be appropriate due to disproportionate costs. In such cases, the institutions may adopt other means of notification (e.g. media advertisements, prominent display of notice in banking halls and ATM sites/screens, phone banking messages and notices on the institution's website).[125]

Consumers must be allowed at least 90 days to report any unauthorised transactions.[126] The notification period for credit card transactions is 60 days from the statement date.[127] Subscribers should warn consumers that they reserve the right to treat the statement as conclusive if no report of unauthorised transaction was received within the specified period. However, this right is not available in certain circumstances, including where a forgery or fraud by any third party arises due to the institution's failure to exercise reasonable care and skill.[128]

Subscribers bear the full loss incurred when the card has not been received by the cardholder, or when the transaction occurs after the card issuer has been given adequate notification that the card/PIN has been lost or when someone else knows the PIN. Subscribers also bear the loss if it was caused directly by faults in their terminals or other systems, unless the fault was obvious or advised by a message or notice on display. Subscribers are also liable for transactions made using counterfeit cards.[129] A subscriber that is a party to a shared electronic system cannot avoid liability because the other

[120] Available at http://www.hkab.org.hk/PDF/rules_guidelines/code_e_09_2005.doc
[121] Section 1.2, HK Code.
[122] Section 5.8, HK Code.
[123] Section 6.7, HK Code.
[124] Section 5.9, HK Code.
[125] Section 6.4, HK Code.
[126] Section 16.4, HK Code.
[127] Section 28.1, HK Code.
[128] Section 16.4, HK Code.
[129] Section 30.1, HK Code.

party to the system has either caused or contributed to the loss arising from the use of the card.[130]

Consumers may be held liable for losses if they act fraudulently, with gross negligence, or fail to inform the subscriber as soon as practicable.[131] Examples of gross negligence include failure to properly safeguard a device or secret code, or knowingly allowing others to use their device or code.[132]

Subscribers must provide an effective and convenient means for consumers to notify the institution of their lost or stolen cards, or unauthorised use of their cards[133] or electronic banking accounts.[134] When such facilities are not available, subscribers are liable for any losses due to non-notification, provided the consumer notifies the subscriber within a reasonable time after the facility is made available.[135]

New Zealand

On 1 July 2007, the New Zealand Banking Association introduced the fourth edition of its Code of Banking Practice (NZ Banking Code).[136] The NZ Banking Code sets a minimum standard of good banking practices applicable to all members of the New Zealand Bankers' Association, replacing the previous Code of Banking Practice which had been in effect from 2 December 2002.[137]

The new NZ Banking Code stipulates that a consumer will not be liable for unauthorised transactions which occur before the consumer receives the card, PIN or password, or where it is clear that the consumer could not have contributed to the loss.[138]

Consumer liability for unauthorised transactions before notification to the bank is generally limited to NZ$50. However, the $50 limit is subject to a non-exhaustive list of exceptions. Generally a consumer will not be protected where the consumer is deemed to have acted fraudulently or negligently, or contributed to the unauthorised use of the card (e.g. by selecting unsuitable PINs or passwords). The limit is also not available where the consumer fails to take all reasonable steps to prevent disclosure to

[130] Section 30.5, HK Code.
[131] Section 30.3, 30.4, HK Code.
[132] Section 40.1, 40.2, HK Code.
[133] Section 29.2, HK Code.
[134] Section 41.3 HK Code.
[135] [135] Section 29.3, 41.4, HK Code.
[136] Available at http://www.nzba.org.nz/public.asp
[137] Paragraph 1.1, NZ Banking Code.
[138] Paragraph 7.2, NZ Banking Code.

any person when entering PINs or passwords.[139] The terms 'fraud', 'negligence' or 'reasonableness' are not defined in the NZ Banking Code.

Consumers are not liable for unauthorised transactions that occur after notification. Again, this protection will not apply if the consumer is deemed to have acted fraudulently or negligently.[140]

The NZ Banking Code requires banks to ensure that their internet banking systems are secure and updated.[141] Users of internet banking may be liable for unauthorised transactions if they did not take all reasonable steps in maintaining their own computers, or other devices used to access internet banking service, with the latest protective systems.[142] The NZ Banking Code also allows banks to request access to the consumer's computer or device in determining whether or not the consumer has met the required standard of safety, and refuse the consumer's claim if the consumer refuses the bank's request for access.[143] Further, if the consumer had allowed another person to use their account to process unauthorised transactions, the consumer may be liable for some or all of the loss suffered by the other party, regardless of the balance available in the consumer's account.[144]

United Kingdom

The UK Banking Code is a voluntary code which, since 1992, has set the standard for banks and building societies when dealing with consumers in the United Kingdom. A third independent review of the UK Banking Code was concluded in May 2007.[145] The new UK Banking Code came into operation on 31 March 2008.

The UK Banking Code covers personal current accounts, savings and deposit accounts, cards and PINs, loans and overdrafts, and payment services.[146] It introduces an overarching principle of fairness to be applied by subscribers when providing consumers with products and services covered in the Code.[147]

Under the UK Banking Code, subscribers must provide information to potential customers about the features of their services and products, and the suitability of those products to the needs of the consumer. Important

[139] Paragraph 7.2(d), NZ Banking Code.
[140] Paragraph 7.2(c), NZ Banking Code.
[141] Paragraph 8(a)(i), NZ Banking Code.
[142] Paragraph 8(c)(iii), NZ Banking Code.
[143] Paragraph 8(c)(v), NZ Banking Code.
[144] Paragraph 8(c)(iv), NZ Banking Code.
[145] Report of the Independent Reviewer to the Sponsors of the Banking Codes' Review 2007, available at http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=140&a=11541.
[146] Art 1.1, UK Banking Code.
[147] Section 2, UK Banking Code.

information for savings accounts and unsecured loans will be made available in a summary box on pre-sale material from 1 October 2008.[148]

Subscribers must disclose fees and charges and must tell consumers personally of any new charges at least 30 days before the change comes into effect.[149]

Subscribers must help consumers who want to move their account to another financial institution by giving the latter information on the consumer's standing orders and direct debits within three working days of receiving the request to do so. The account must be closed or moved free of charge.[150] Any bank charges incurred by the consumer as a result of any mistake or unnecessary delay by subscribers when transferring their accounts must be cancelled.[151] Subscribers cannot close an account, or threaten to do so, when solely responding to a valid complaint made by a consumer.[152]

Consumers who act fraudulently will be responsible for all losses on their account. A consumer may also be liable if the loss was caused by failure to act with reasonable care.[153] Section 12.5 and 12.9 give examples of ways in which consumers can ensure their accounts and transactions are secure.

Unless a subscriber can show that the consumer has acted fraudulently or without reasonable care, the consumer's liability for misuse of their card is limited.[154] If someone else uses the consumer's card without the consumer telling the subscriber that it has been lost or stolen or that someone else knows the PIN, the maximum liability is capped at £50. If someone else uses the consumer's card without permission and the card has not been lost or stolen, the consumer will not pay anything. If the card is used before the consumer receives it, the consumer will not pay anything. A consumer will not be liable for losses caused by someone else through online banking unless the consumer has acted fraudulently or without reasonable care.[155]

[148] Section 3.1, UK Banking Code.
[149] Section 5.3, and section 5.4 UK Banking Code.
[150] Section 7.3, UK Banking Code.
[151] Section 7.5, UK Banking Code.
[152] Section 7.7, UK Banking Code.
[153] Section 12.11, UK Banking Code.
[154] Section 12.12, UK Banking Code.
[155] Section 12.13, UK Banking Code.

Appendix 3: Regulation of electronic transactions

Table 6: Comparison of regulatory obligations for disclosure, receipts and statements

Issue	EFT Code	Code of Banking Practice	Corporations Act requirements for basic deposit products and related non-cash payment facilities[156]	ASIC relief for low-value non-cash payments[157]
Coverage	Regulates 'electronic transactions'.	Regulates transactions relating to consumer accounts.	Regulates non-cash payment facilities related to basic deposit products.[158]	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; the total amount available under all facilities of the same class does not exceed $10 million at any time; and the facility is not part of another financial product.
Initial disclosure requirements	Subscribers must give consumers a copy of the terms and conditions before their first transaction.[159]	Banks must give consumers terms and conditions before or when entering into a contract, except where it is impracticable to do so.[160]	Product issuers must give retail consumers information about the cost of the product and ask whether the consumer wants further information.[161]	Issuers must give a written disclosure document that prominently discloses the terms and conditions and other prescribed information.[162]

[156] As a starting point, Corporations Act obligations apply in full to non-cash payment facilities. However, the Corporations Act makes special provision for non-cash payment facilities related to basic deposit products, requiring compliance with a scaled-back version of the Corporations Act disclosure obligations.
[157] ASIC has granted conditional relief to providers of low value non-cash payment facilities on the basis that they are generally simple, easy-to-use and well understood by retail consumers: see ASIC Class Order CO 05/736. Whether a non-cash payment facility is granted relief or declared not to be a financial product for the purposes of the Corporations Act, the consumer protection provisions in Div 2 of Part 2 of the ASIC Act continue to apply. The misconduct provisions in Part 7.10 of the Corporations Act will also continue to operate where ASIC has granted relief from financial services licensing, conduct and disclosure obligations. ASIC has also granted unconditional relief to persons providing financial services in relation to gift vouchers and cards and prepaid mobile phone facilities and declared loyalty schemes and electronic road toll devices not to be 'financial products' for the purpose of Chapter 7 of the Corporations Act: see ASIC Class Orders CO 05/737, CO 05/738, CO 05/739 and CO 05/740.
[158] The definition of financial product includes a facility through which, or through the acquisition of which, a person makes non-cash payments: s763A(1)(c). The definition of a non-cash payment facility is set out in s761A and 763D(1). The definition of a basic deposit product is set out in s 761A.
[159] Clause 2.2(a) and 2.3 and 12.2(a) and 12.3.

Issue	EFT Code	Code of Banking Practice	Corporations Act requirements for basic deposit products and related non-cash payment facilities[156]	ASIC relief for low-value non-cash payments[157]
Disclosure on request	Subscriber must give consumers a copy of the terms and conditions on request.[163]	Banks must also give information on request.[164]	Nil	Issuers must provide information on request.[165]
Ongoing disclosure	Subscribers must give written notice of certain changes (e.g. introducing new charges or increasing existing charges) 20 days in advance. Other changes must be disclosed in advance, but written notice is not required.[166]	Banks must give written notice of certain changes (e.g. the introduction of a new fee), 30 days in advance.[167] Banks must give notice of other changes by the day the change takes effect. This can be done by advertising in the media.[168] However, these requirements do not apply to non-cash payment facilities regulated under the Corporations Act.[169]	Nil	Issuers must disclose changes in the publicly accessible areas of their business and on their website.[170]

[160] Code of Banking Practice, clause 10.2(d).
[161] Corporations Act s1012D(7A), inserted by Corporations Regulations reg 7.9.07FA.
[162] See ASIC Class Order CO 05/736, subparagraph 5(a) and 6(a).
[163] Clauses 2.2(b) and 12.2(b).
[164] Code of Banking Practice, clause 10.1.
[165] See ASIC Class Order CO 05/736, subparagraph 5(e)(iii).
[166] Clauses 3 and 13.
[167] Code of Banking Practice, clause 18.1.
[168] Code of Banking Practice, clause 18.3.
[169] Code of Banking Practice, clause 18.4.
[170] See ASIC Class Order CO 05/736, subparagrahs 5(e)(i) and 5(e)(iv).

Issue	EFT Code	Code of Banking Practice	Corporations Act requirements for basic deposit products and related non-cash payment facilities[156]	ASIC relief for low-value non-cash payments[157]
Receipts	Subscribers must give receipts unless the consumer specifically elects otherwise and the content is heavily prescribed.[171] This consultation paper proposes permitting consumers to opt-in to receiving receipts (see proposal C1). Receipts are not required for products regulated under Part B.	Nil	If the issuer provides a statement within six months of the transaction, a receipt is not required.[172]	Nil
Statements	Subscribers must give a statement every six months and the content is prescribed.[173] This requirement does not apply to passbook accounts. Receipts are not required for products regulated under Part B.	Banks must give consumers a statement every six months, unless the consumer agrees that they do not want one.[174]	Consumers must receive a statement for the basic deposit product every 12 months and the content is prescribed. This requirement does not apply where the basic deposit product is a passbook.[175]	Issuers are not required to provide statements but must provide a free, convenient way for consumers to check their balance and a record of the last ten transactions.[176]

[171] Clause 4.1.
[172] Corporations Regulations, reg 7.9.62.
[173] Clause 4.2–4.4.
[174] Code of Banking Practice, clause 24.1.
[175] Corporations Act s1017D and Corporations Regulations reg 7.9.60B and reg 7.9.71–7.9.75D.
[176] See ASIC Class Order CO 05/736, subparagraph 5(d).