ASIC
Australian Securities & Investments Commission

CONSULTATION PAPER 158

Redrafting the Electronic Funds Transfer Code of Conduct

May 2011

About this paper

As part of ASIC's review of the Electronic Funds Transfer Code of Conduct, we have redrafted the Code. The redrafted Code (to be renamed the EPayments Code) incorporates changes made as a result of the recent review of the Code, and uses plain English.

This consultation process is confined to drafting issues. ASIC is not consulting on policy issues relating to the Code.

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 20 May 2011 and is based on the Corporations Act as at 20 May 2011.

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 drafting of the new EPayments Code. The purpose of this consultation process is not to consult on policy issues relating to the Code.

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 17 June 2011 to:

Ailsa Goodwin
Senior Manager, Strategic Policy
Australian Securities and Investments Commission
GPO Box 9827
Melbourne Victoria 3001
email: eftreview@asic.gov.au

What will happen next?

Stage 1	20 May 2011	ASIC consultation paper released with draft EPayments Code
Stage 2	17 June 2011	Comments due on the consultation paper and draft EPayments Code
Stage 3	July 2011	EPayments Code released

A Redrafting the Code

Key points

This consultation process is confined to drafting issues. ASIC is not consulting on policy issues relating to the Code.

We have:

- adopted a new structure and new defined terms for the Code;
- redrafted the Code in plain English;
- tailored the Code for low value facilities; and
- included a mistaken internet payments regime.

We propose to allow a 12-month transition period to the commencement of the revised Code.

We are seeking feedback on the drafting of the revised Code generally, and on some of the specific issues set out below.

Background

1 ASIC is responsible for the Electronic Funds Transfer Code of Conduct and is required to review the Code periodically. We completed the most recent review of the Code in late 2010. The results of the review were published in our report *Electronic Funds Transfer Code of Conduct review: Feedback on CP 90 and final positions* (REP 218). The review recommended a number of improvements to the Code. It also recommended that the Code be redrafted in plain English.

2 We have redrafted the Code to reflect these recommendations. A draft of the revised Code is attached to this consultation paper and we are seeking feedback on this attached draft.

3 A reference group—the Plain English Reference Group—was formed to assist ASIC in redrafting the Code. The members of this group include:

- ASIC (Chair)
- Abacus Australian Mutuals
- Australian Bankers' Association
- Australian Payments Clearing Association
- Financial Ombudsman Service
- Chris Connolly, independent researcher (on behalf of CHOICE and Consumers' Federation of Australia)

4 We have decided to rename the Code the 'EPayments Code' to better reflect the products and services covered by the Code.

5 This consultation process is confined to drafting issues. We are not consulting on policy issues relating to the Code. We are seeking feedback on how the drafting implements the changes to the Code set out in REP 218.

Defined terms

Issue

A1 We have adopted new defined terms in the revised Code: see Appendix C of the revised Code.

Your feedback

A1Q1 Do you have any feedback about these defined terms?

6 The current Code includes numerous definitions. The definitions in Part A are specific to banks, credit unions and building societies. The definitions in Part B relate to prepaid stored value products.

7 We have decided to replace many of these definitions with terms that are easier to understand and are product neutral.

Low value facilities

Issue

A2 We have tailored the Code for low value facilities.

Your feedback

A2Q1 Do you have any feedback about the drafting of the Code clauses that are tailored for low value facilities?

8 Part B of the current Code provides a light-touch regime for stored value products. In practice, Part B has been underused.

9 Although we have replaced the two-part structure of the Code with a one-part structure, we recognise that it is appropriate to tailor the way the Code applies to products that are simple and low risk.

10 In the Code we call these 'low value facilities'. This is defined as a facility that is capable of having a balance of no more than $500 at one time: see Appendix C of the revised Code.

11 The tailored requirements for low value facilities are set out in Table 1.

Table 1: Tailored requirements for low value facilities

Clause	Tailored requirement
4.4	Subscribers do not have to give terms and conditions unless it is practical to do so. Otherwise, subscribers must give consumers a notice that highlights key terms.
4.9	Subscribers do not have to give consumers information about how to report the loss, theft or misuse of a device or breach of pass code security. Instead, subscribers must tell consumers whether they provide a process for doing this.
4.15	Subscribers do not have to give consumers advance notice of changes to terms and conditions unless they know the identity and contact details of the consumer. Otherwise, subscribers must simply publicise this information.
5.11	Subscribers do not have to give consumers receipts. Instead, subscribers must give consumers a process to check their balance and a simplified receipt or a mechanism for the consumer to check their transaction history.
7.7	Subscribers do not have to give consumers statements.
Chapter C	The rules for allocating liability for unauthorised transactions do not apply to low value facilities.

Mistaken internet payments

Issue

A3 We have included a mistaken internet payments regime in the revised Code.

Your feedback

A3Q1 Do you have any feedback about the drafting of the Code clauses dealing with mistaken internet payments?

12 Internet banking services allow consumers to use online banking to transfer funds to others ('Pay Anyone' transactions). Sometimes, consumers transfer funds to the wrong person because they enter the wrong payment details or because they have been given the wrong information.

13 In REP 218, we committed to including a regime for mistaken payments in the Code.

Transition period and implementation

Proposal

A4 We propose to allow a 12-month transition period to the commencement of the EPayments Code.

Your feedback

A4Q1 Is a 12-month transition period adequate?

14 The EPayments Code imposes some new obligations on subscribers. We accept the need for a transition period to the EPayments Code.

15 We expect existing subscribers to resubscribe to the revised Code during the transition period and to comply with the revised Code from the end of the transition period (if not before).

16 We anticipate that the transition period will begin when the final version of the revised Code is published.

Structure and drafting

Issue

A5 We have replaced the current two-part structure of the Code with a one-part structure. The new chapter structure is based on the main topics in the Code.

Your feedback

A5Q1 Do you have any feedback about the revised structure of the Code?

A5Q2 Do you have any feedback about the language and style (i.e. plain English) of the revised Code?

A5Q3 Do you have any other comments or feedback on the drafting of the revised Code? (We welcome comments on the drafting, generally—particularly, suggestions for clarification and improvement.)

17 The current Code has a two-part structure. Part A governs the relationship between account institutions and their clients. Part B applies to stored value products. REP 218 concluded that the two-part structure should be replaced by a one-part structure.

18 As part of the recently completed review of the Code, we committed to redrafting the Code in plain English. Other than to incorporate the changes agreed by the Plain English Reference Group and those set out in REP 218, we have not sought to change the current meaning of the Code. Redrafting

the Code in plain English is not intended to diminish the consumer protections afforded by the Code in any way.

19 As this is a complete redraft of the Code, stakeholders will be interested in the precise drafting. When redrafting the Code in plain English, we have sought to keep the meaning the same as the current Code (except for areas where we have made policy changes as set out in REP 218). We have consulted with a small stakeholder reference group during this drafting stage as issues arose in the drafting.

B Regulatory and financial impact

20 In developing the proposals in this paper, we have carefully considered their regulatory and financial impact.

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

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

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

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

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

Attachment: Draft EPayments Code

The following attachment is the draft revised Electronic Funds Transfer Code of Conduct, renamed the 'EPayments Code'. We are seeking feedback on this draft of the EPayments Code.

DRAFT

ASIC

Australian Securities & Investments Commission

EPayments Code

May 2011

Introduction

What is the EPayments Code?

The EPayments Code (**this Code**) regulates electronic payments, including **ATM**, **EFTPOS** and credit card **transactions**, online payments, internet banking and BPay.

This Code (formerly known as the Electronic Funds Transfer Code of Conduct) has existed since 1986. **ASIC** is responsible for the administration of **this Code**, including reviewing it regularly. The most recent review was completed in 2010.

Who is bound by the EPayments Code?

This Code is a voluntary code of practice.

Banks, credit unions, building societies and other providers of electronic payment facilities to consumers subscribe to **this Code**. A list of **subscribers** is available at: www.asic.gov.au/asic/asic.nsf/byheadline/List-of-EFT-Code-members-A-H?openDocument.

What does this Code do?

This Code plays an important role in the regulation of electronic payment **facilities** in Australia.

It complements other regulatory requirements, including financial services and consumer credit licensing, advice, training and disclosure obligations under the *Corporations Act 2001* and the *National Consumer Credit Protection Act 2009*.

This Code:

- requires **subscribers** to **give** consumers terms and conditions, information about changes to terms and conditions (such as fee increases), receipts and statements,
- sets out the rules for determining who pays for **unauthorised transactions**, and
- establishes a regime for recovering mistaken internet payments.

There are more limited requirements for **low value facilities** that can hold a balance of no more than $500 at any one time.

Subscribers must warrant that they will comply with **this Code** in the terms and conditions they **give** consumers. This means that compliance with **this Code** must be a term of the contract between the **subscriber** and each of its account or **facility holders**.

Consumers can complain about a breach of **this Code** to the **subscriber**. If a consumer is not happy with the outcome, they can complain to an external dispute resolution scheme, such as the Financial Ombudsman Service or the Credit Ombudsman Service Limited, if the **subscriber** belongs to a scheme.

ASIC also monitors compliance with **this Code**.

This Code commences on 1 July 2012.

For more information about **this Code**, see www.asic.gov.au/asic/asic.nsf/byheadline/Electronic+Funds+Transfer:+Code+of+Conduct?opendocument.

Note: 'Defined terms' (see Appendix C) are highlighted in **bold** throughout **this Code**. Both singular and plural defined terms appear in bold.

Contents

Page no.

Chapter A: Objectives, scope and definitions

Key points

This Chapter sets out:

- the objectives of **this Code**,
- what **transactions this Code** covers, and
- how **this Code** relates to other laws.

1 Objectives

Objectives

1.1 The objectives of **this Code** are to provide:

a) a quality consumer protection regime for payment **facilities**,

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

c) effective disclosure of information, to enable consumers to make informed decisions about **facilities**,

d) clear and fair rules for allocating liability for **unauthorised transactions**,

e) effective procedures for resolving **complaints**, and

f) a regime that is flexible and accommodates providers of new payment **facilities**.

2 Scope

Scope

2.1 **This Code** applies to **transactions**, other than **transactions** performed using:

a) a **facility** that is designed primarily for use by a business, and established primarily for business purposes,

b) a **facility** where the **holder** and the **subscriber** do not have a contractual relationship, or

c) **biller accounts**.

2.2 Subject to clause 43, a **subscriber** must comply with **this Code** for all **transactions** that are covered by **this Code**.

2.3 A **subscriber** can choose to adopt **this Code** for **transactions** that are not covered by **this Code**.

Definition – transaction

2.4 **This Code** applies to payment, funds transfer and cash withdrawal **transactions** that are:

a) initiated using electronic equipment, and

b) not intended to be authenticated by comparing a **manual signature** with a specimen signature.

2.5 **This Code** applies to the following **transactions** provided by a **subscriber**:

a) electronic card **transactions**, including **ATM, EFTPOS**, credit card and debit card **transactions** that are not intended to be authenticated by comparing a **manual signature** with a specimen signature,

b) telephone banking and bill payment transactions,

c) internet banking **transactions**, including 'Pay Anyone',

d) online **transactions** performed using a card number and **expiry date**,

e) online bill payments (including BPay),

f) **transactions** using **facilities** with contactless features and prepaid cards,

g) direct debits,

h) **transactions** using electronic toll devices,

i) **transactions** using mobile phone payment facilities,

j) **transactions** using electronic public transport ticketing facilities, and

k) mail order **transactions** not intended to be authenticated by comparing a manual signature with a specimen signature.

2.6 The list in clause 2.5 is not exhaustive.

Note: **ASIC** has the power to declare that **this Code** applies or does not apply to a type of **transaction**: see clause 43.

Other definitions

2.7 For a list of other defined terms used in **this Code**, please refer to Appendix C of **this Code**.

3 Relationship to laws

3.1 Where legislation and **this Code** both impose an obligation on **subscribers** to **give users** information at different times, **subscribers** must **give** the notice at the earliest time it is required under the legislation or **this Code**.

Chapter B: Disclosure

Key points

This Chapter requires **subscribers** to **give**:

- terms and conditions,
- information about changes to terms and conditions such as fee increases,
- receipts/statements, and
- information about **ATM** fees.

4 Terms and conditions

Terms and conditions requirements

4.1 A **subscriber** must prepare clear and unambiguous terms and conditions for **facilities**.

4.2 The terms and conditions must:

a) reflect the requirements of **this Code**,

b) not impose liability or responsibilities on **users** that exceed their liability and responsibilities under **this Code**, and

c) warrant that the **subscriber** will comply with **this Code**.

4.3 A **subscriber** must **give holders** a copy of the terms and conditions:

a) before, or at the time, a **user** first uses a **facility** to perform a **transaction**, and

b) at any other time, on request.

Tailored requirement for low value facilities

4.4 Clause 4.3 does not apply to a **low value facility**. Instead, a **subscriber** must **give holders** the following information before, or at the time, a **user** first uses a **low value facility** to perform a **transaction**:

a) if practical, a copy of the terms and conditions, or

b) a notice that highlights any key terms (for example, any **expiry date**) and explains how to obtain the full terms and conditions (for example, by referring the **holder** to a website).

Disclosure requirements

4.5 A **subscriber** must publicise the availability of the terms and conditions.

4.6 A **subscriber** must **give holders** all of the following information, before a **user** first performs a **transaction**:

a) fees or charges for issuing or replacing a **device** or **pass code**,

b) fees or charges for performing **transactions**,

c) fees or charges for adding funds into a **facility** (for example fees or charges for loading value onto a prepaid card),

d) any restrictions over which the **subscriber** has control, including any daily or other periodic **transaction** limit, on:

i. the number or value of **transactions**,

ii. the use of a **facility**, or

iii. the use of any electronic equipment, such as withdrawals at an **ATM** or purchase at an **EFTPOS** terminal,

and an explanation that merchants or other providers of facilities may impose additional limits,

e) a description of:

i. the types of **transactions** that **users** can perform, and

ii. the **facility** and any other facilities **user**s can access using it, including, if relevant, any credit **facility**,

f) a description of how to report the loss, theft or misuse of a **device**, or breach of security of a **pass code**, and

Note: **Subscribers** must have a process for **user**s to report the loss, theft or misuse of a **device** or **pass code**: see clause 17.

g) a description of how to make a **complaint** and, if the **subscriber** is required to **give** statements, how to query entries on a statement.

4.7 The information in clause 4.6(a)–4.6(c) must be disclosed separately from other charges.

Note: **Subscribers** must **give holders** statements unless an exception applies: see clause 7.

Expiry dates

4.8 If:

a) a **facility** has an **expiry date**, a **subscriber** must disclose that date to the **user** before a **user** first uses the **facility** to perform a **transaction**, or

b) a **subscriber** cannot ascertain the **expiry date**, because it depends on the date a **user** activates or reloads a **facility**, the **subscriber** must disclose the period during which the **facility** will be able to be used to make **transactions**, before a **user** first uses the **facility** to perform a **transaction**.

Note: For example, if a **facility** expires 12 months from the date it is activated or last reloaded, the **subscriber** can comply with this clause by disclosing this.

Tailored requirements for low value facilities

4.9 Clause 4.6(f) does not apply to a **low value facility**. Instead, a **subscriber** must tell **holders** whether or not the **subscriber** provides a process for reporting the loss, theft or misuse of a **device** or breach of security of a **pass code**.

4.10 A **subscriber** must **give** the information required under clause 4.9:

a) at point of sale, or

b) before **users** first use the **facility** to perform a **transaction**.

Notice of certain changes to terms and conditions

4.11 A **subscriber** must **give holders** at least 20 **days** advance written notice of the following changes to terms and conditions:

a) imposing or increasing fees or charges for issuing or replacing a **device** or **pass code**,

b) imposing or increasing fees or charges for performing **transactions**,

c) increasing a **holder's** liability for losses relating to **transactions**, or

Note: Any increases to a **holder's** liability for losses must also be consistent with the limits on a **holder's** liability for losses under Chapter C of **this Code**.

d) imposing, removing or changing a daily or other periodic limit on:

i. **transactions**,

ii. a **facility**, or

iii. electronic equipment (for example, limits on the number or value of **ATM** withdrawals).

4.12 If a **subscriber** removes or increases a **transaction** limit, the **subscriber** must **give** the **holder** a clear and prominent notice that this may increase the **holder's** liability in the case of **unauthorised transactions**. The **subscriber** must **give** this notice when the **subscriber** notifies the **holder** of the change to the **holder's transaction** limit under clause 4.11(d).

4.13 A **subscriber** must **give holders** notice of other changes to terms and conditions:

a) before the change takes effect, and

b) in the manner required by applicable legislation, or if there are no such requirements, in a way that is likely to come to the attention of as many **holders** as practicable.

4.14 If changes to terms and conditions are sufficiently important or numerous, a **subscriber** must **give holders** a single document, which may be consolidated terms and conditions, explaining all the changes.

Tailored requirements for low value facilities

4.15 Clauses 4.11–4.14 do not apply to changes to terms and conditions for **low value facilities**. Instead, a **subscriber** must **give holders** advance notice of changes to terms and conditions for **low value facilities**:

a) directly, if the **subscriber** knows the identity and contact details of the **holder**, or

b) by publicising the changes at places where the **facility** can be used, or

c) by publicising the changes using the process for **holders** to check the balance on the **facility**.

Note: **Subscribers** must provide a process (such as a website) for **users** to check the balance on **low value facilities**: see clause 5.11.

Exception

4.16 A **subscriber** is not required to **give** advance notice of changes to terms and conditions required to immediately restore or maintain the security of a system or an individual **facility**, including the prevention of systemic or individual criminal activity, including fraud.

Tailored requirements for anonymous facilities

4.17 If a **subscriber** does not know the identity or contact details of a **holder**, it must instead make information it is required to **give** a **holder** under clause 4 available in a way that is likely to come to the attention of the **holder**.

5 Receipts

Receipt requirements

5.1 A **subscriber** must take reasonable steps to offer **users** a receipt for all **transactions**, at the time of the **transaction**.

Note: This clause does not apply to **transactions** performed using telephone banking or **low value facilities**: see clauses 5.8 and 5.11.

5.2 A receipt must include the following information about the **transaction**:

a) amount,

b) date,

c) **transaction** type,

d) an indication of the **facility** or **facilities** being debited or credited, and

e) information to enable the **subscriber** to identify the **user** and the **transaction**.

5.3 A receipt for a payment to a merchant for goods or services must also include the name of the merchant.

5.4 Paper receipts must not include information which would increase the risk of **unauthorised transactions**, such as:

a) a complete **identifier**, or

b) an **expiry date** for a **device**.

5.5 A receipt must also include the following information about the **transaction**, if practicable:

a) time,

b) type, and general location, of equipment used to perform the **transaction**, or a number or symbol enabling the equipment to be identified, and

c) if it is not likely to compromise the **user's** privacy or security, the balance remaining on the **facility**.

5.6 A **subscriber** must not charge **users** for giving:

a) a receipt under clause 5.1, or

b) information about **transactions** performed using telephone banking under clause 5.8, or

c) information about **transactions** performed using a **low value facility** under clause 5.11.

5.7 Where a **user** does not use a **subscriber's** equipment or systems, and does not communicate with the **subscriber** or anyone acting on its behalf, the **subscriber** must use its best endeavours to comply with clauses 5.1–5.11.

Telephone banking

5.8 Clauses 5.1–5.6 do not apply to **transactions** performed using telephone banking. Instead, a **subscriber** must take reasonable steps to offer **users** the following information, at the time of a telephone banking **transaction**:

a) receipt number,

b) **transaction** amount,

c) **transaction** type, and

d) an indication of the **facility** or **facilities** being debited or credited.

5.9 Information on a receipt for a payment to a merchant for goods and services must also include either:

a) the name of the merchant, or

b) a reference number, where the merchant also **gives** the **user** an invoice that includes the merchant's name and the reference number.

Note: Giving the name of the merchant is best practice.

5.10 If practicable, and not likely to compromise the **user's** privacy or security, a **subscriber** should also include the balance remaining on the **facility**.

Tailored requirements for low value facilities

5.11 The requirements for receipts under clauses 5.1–5.7 and the requirements for **transaction** information for telephone banking under clauses 5.8–5.10 do not apply to **transactions** performed using a **low value facility**. Instead, the **subscriber** must **give users**:

a) a process for **user**s to check the balance on the **facility**, and

b) either:

i. a receipt or reference for each **transaction** that enables **users** to identify the **transaction**, the amount, and any fees or charges relating to the **transaction**, or

ii. a mechanism for **users** to check their **transaction** history. This must be available for a reasonable period.

6 Fees charged by ATM provider

ATM fees

6.1 A **subscriber** that is an **ATM** provider must disclose the amount of any fee or charge imposed on a **user** for a **transaction** using an **ATM** it provides, including any fee or charge imposed on:

a) an individual who is a customer of the **subscriber**, and

b) an individual who is not a customer of the **subscriber**.

6.2 This information must be disclosed before the **user** completes the **transaction**.

6.3 After receiving the information the **user** must be able to cancel the **transaction** at no cost.

6.4 When a **subscriber** has an agreement with an **ATM** provider about providing **ATMs**, the agreement must provide that:

a) the **ATM** provider must disclose the amount of any fee or charge the **ATM** provider imposes on a **user** who is not otherwise a customer of the **ATM** provider, before the **user** completes the **transaction**, and

b) after receiving the information in clause 6.4(a), the **user** must be able to cancel the **transaction** at no cost.

7 Statements

Subscribers must give statements

7.1 A **subscriber** must **give holders** a statement for facilities at least every 6 months, unless the **facility**:

a) is a passbook account, where there is no charge for either manually updating the passbook, or checking the account balances and activity electronically, or

b) has a zero balance and there were no **transactions** during the statement period.

7.2 A **subscriber** must also **give holders** the option of receiving more frequent statements and bring this option to the **holder's** attention when the **holder** first uses the **facility**.

7.3 A **subscriber** must also **give holders** statements on request.

Statement requirements

7.4 A statement under a usual statement cycle must include the following information about each **transaction** since the last statement:

a) amount,

b) date each **transaction** was debited or credited to the **facility**,

c) **transaction** type,

d) receipt number, or other information that will enable the **user** to reconcile the statement entry with a receipt or **transaction** information,

e) any charges imposed by the **subscriber** for performing **transactions**, listed separately from other charges,

f) contact details for making inquiries about the **facility** or reporting errors in the statement, and

g) a suggestion that the **holder** check each entry on the statement and promptly report any possible error or **unauthorised transaction** to the **subscriber**.

7.5 Where practicable, a **subscriber** should include in statements the amount of each fee or charge imposed for a **transaction** using an **ATM** provided by a different **ATM** provider.

7.6 A statement issued on request must include as much of the information in clause 7.4 as possible.

Tailored requirements for low value facilities

7.7 Clause 7.1 does not apply to a **low value facility**.

Note: When providing a **low value facility**, **subscribers** must **give users** a process to check the balance of the **facility** and either a receipt or a mechanism for **users** to check their **transaction** history: see clause 5.11.

Tailored requirements for anonymous facilities

7.8 If a **subscriber** does not know the identity or contact details of a **holder**, it must instead provide the holder with a means to access the information it is required to **give** a **holder** under clauses 7.1–7.6.

8 Mandatory consumer warning

8.1 If:

a) a **pass code** is required to perform **transactions**, and

b) a **subscriber** is required to **give holders** a statement under clause 7.1,

the **subscriber** must include on or with statements, at least annually, a clear, prominent and self-contained notice summarising **pass code** security guidelines, which are consistent with clause 13 of **this Code**.

Chapter C: Liability

Key points

This Chapter explains the rules for allocating liability for losses arising from:

- **unauthorised transactions**, and
- system or equipment malfunction.

9 Scope

Transactions not authorised by a user

9.1 This Chapter applies to **unauthorised transactions**. It does not apply to any **transaction** that is performed by a **user** or by anyone who performs a **transaction** with the knowledge and consent of a **user**.

10 When holder is not liable for loss

10.1 A **holder** is not liable for loss arising from an **unauthorised transaction** if the cause of the loss is any of the following:

a) fraud or negligence by a **subscriber's** employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent,

b) a **device**, **identifier** or **pass code** which is forged, faulty, expired or cancelled,

c) a **transaction** requiring the use of a **device** and/or **pass code** that occurred before the **user** received the **device** and/or **pass code** (including a reissued **device** and/or **pass code**),

d) a **transaction** being incorrectly debited more than once to the same **facility**, and

e) an **unauthorised transaction** performed after the **subscriber** has been informed that a **device** has been misused, lost or stolen, or the security of a **pass code** has been breached.

10.2 A **holder** is not liable for loss arising from an **unauthorised transaction** that can be made using an **identifier** without a **pass code** or **device**. Where a **transaction** can be made using a **device**, or a **device** and an **identifier**, but does not require a **pass code**, the **holder** is liable only if the **user** unreasonably delays reporting the loss or theft of the **device**.

10.3 A **holder** is not liable for loss arising from an **unauthorised transaction** where it is clear that a **user** has not contributed to the loss.

10.4 In a dispute about whether a **user** received a **device** or **pass code**:

a) there is a presumption that the **user** did not receive it, unless the **subscriber** can prove that the **user** did receive it,

b) a **subscriber** can prove that a **user** received a **device** or **pass code** by obtaining an acknowledgement of receipt from the **user**, and

c) a **subscriber** may not rely on proof of delivery to a **user**'s correct mailing or electronic address as proof that the **user** received the **device** or **pass code**.

10.5 A **subscriber** must not have any term in its terms and conditions that deems a **device** or **pass code** sent to a **user** by mail or electronic communication at the **user's** correct mailing or electronic address to be received by the **user**.

11 When holder is liable for loss

11.1 When clause 10 does not apply, a **holder** may only be made liable for losses arising from an **unauthorised transaction** regulated by **this Code** in the circumstances specified in this clause.

11.2 Where a **subscriber** can prove on the balance of probability that a **user** contributed to a loss through fraud, or breaching the **pass code** security requirements in clause 12,

a) the **holder** is liable in full for the actual losses that occur before the loss, theft or misuse of a **device** or breach of **pass code** security is reported to the **subscriber**, but

b) the **holder** is not liable for losses:

i. incurred on any one day that exceed any applicable daily **transaction** limit,

ii. incurred in any period that exceed any applicable periodic **transaction** limit,

iii. that exceed the balance on the **facility**, including any pre-arranged credit, or

iv. incurred on any **facility** that the **subscriber** and the **holder** had not agreed could be accessed using the **device** or **identifier** and/or **pass code** used to perform the **transaction**.

Note: Where the **holder** is the **user** who contributed to a loss, the **holder** is liable under this clause.

11.3 Where:

a) more than one **pass code** is required to perform a **transaction**, and

b) a **subscriber** proves that a **user** breached the **pass code** security requirements in clause 12 for one or more of the required **pass codes**, but not all of the required **pass codes**,

the **holder** is liable under clause 11.2 only if the **subscriber** also proves on the balance of probability that the breach(es) of the **pass code** security requirements under clause 12 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

11.4 The **holder** is liable for losses arising from **unauthorised transactions** that occur because a **user** contributed to losses by leaving a card in an **ATM**, as long as the **ATM** incorporates reasonable safety standards that mitigate the risk of a card being left in the **ATM**.

Note: Reasonable safety standards that mitigate the risk of a card being left in an **ATM** include **ATMs** that capture cards that are not removed after a reasonable time and **ATMs** that require a **user** to swipe then remove a card in order to commence a **transaction**.

11.5 Where a **subscriber** can prove, on the balance of probability, that a **user** contributed to losses resulting from an **unauthorised transaction** by unreasonably delaying reporting a security compromise (namely, the misuse, loss or theft of a **device** or that the security of all **pass codes** has been breached), the **holder**:

a) is liable for the actual losses that occur between:

i. when the **user** became aware of the security compromise, or, should reasonably have become aware in the case of a lost or stolen **device**, and

ii. when the security compromise was reported to the **subscriber**,

b) but is not liable for any losses:

i. incurred on any one day that exceed any applicable daily **transaction** limit,

ii. incurred in any period that exceed any applicable periodic **transaction** limit,

iii. that exceed the balance on the **facility**, including any pre-arranged credit, or

iv. incurred on any **facility** that the **subscriber** and the **holder** had not agreed could be accessed using the **device** and/or **pass code** used to perform the **transaction**.

Note: Where the **holder** is the **user** who contributed to a loss, the **holder** is liable under this clause.

Effect of charges

11.6 In deciding whether a **user** has unreasonably delayed reporting the misuse, loss or theft of a **device**, or a breach of **pass code** security, the effect of any charges imposed by the **subscriber** for making the report or replacing a **device** or **pass code** must be taken into account.

Note: For example, the reasonableness of a fee a **subscriber** charges for replacing a **device** must be taken into account.

Other situations – limited liability

11.7 Where a **pass code** was required to perform an **unauthorised transaction**, and clauses 11.2–11.6 do not apply, the **holder** is liable for the least of:

a) $150, or a lower figure determined by the **subscriber**,

b) the balance of the **facility** or **facilities** which the **subscriber** and the **holder** have agreed can be accessed using the **device** and/or **pass code**, including any prearranged credit, or

c) the actual loss at the time that the misuse, loss or theft of a **device** or breach of **pass code** security is reported to the **subscriber**, excluding that portion of the losses incurred on any one day which exceed any relevant daily **transaction** or other periodic **transaction** limit.

Proof that a user contributed to losses

11.8 In deciding whether a **subscriber** has proved on the balance of probability that a **user** has contributed to losses under clauses 11.2 and 11.5:

a) all reasonable evidence must be considered, including all reasonable explanations for the **transaction** occurring,

b) the fact that a **facility** has been accessed with the correct **device** and/or **pass code**, while significant, does not, of itself, constitute proof on the balance of probability that a **user** contributed to losses through fraud or a breach of the **pass code** security requirements in clause 12, and

c) the use or security of any information required to perform a **transaction** that is not required to be kept secret by **users** (for example, the number and expiry date of a **device**) is not relevant to a **user's** liability.

Discretion to reduce liability

11.9 Where a **subscriber** has not applied a reasonable daily or other periodic **transaction** limit, the **subscriber**, or an external dispute resolution body, may reduce the liability of the **holder** for an **unauthorised transaction** under clauses 11.2–11.7 by such amount as it considers fair and reasonable, having regard to:

a) prevailing industry practice regarding reasonable **transaction** limits,

b) whether the security and reliability of the means used by the **subscriber** to verify that the **transaction** was authorised adequately protected the **holder** from losses, in the absence of the protection that would have been provided by reasonable daily or other periodic **transaction** limits, and

c) if the **unauthorised transaction** involved a credit **facility,** including drawing on loan repayments made to a loan **facility,** accessible using a **device** and/or **pass code**, whether, at the time of making the credit **facility** available using the **device** and/or **pass code**, the **subscriber** had taken reasonable steps to warn the **holder** of the risk of the **device** and/or **pass code** being used to make **unauthorised transactions** on the credit **facility**.

Relationship to credit card, debit card and charge card schemes

11.10 When a **user** reports an **unauthorised transaction** on a credit card account, debit card account or charge card account:

a) the **subscriber** must not hold the **holder** liable for losses under clause 11 for an amount greater than the liability the **holder** would have if the **subscriber** exercised any rights it had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, charge-back rights), and

b) this clause does not require **subscribers** to exercise any rights they may have under the rules of the card scheme. However, a **subscriber** cannot hold a **holder** liable under this clause for a greater amount than would apply if the **subscriber** had exercised those rights.

12 Pass code security

Pass code security

12.1 This clause applies where one or more **pass codes** are needed to perform a **transaction**.

12.2 A **user** must not:

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

b) where a **device** is also needed to perform a **transaction**, write or record **pass code(s)** on a **device**, or keep a record of the **pass code(s)** on anything

i. carried with a **device**, or

ii. liable to loss or theft simultaneously with a **device**,

unless the **user** makes a reasonable attempt to protect the security of the **pass code**, or

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

12.3 For the purpose of clause 12.2(b) and (c), a reasonable attempt to protect the security of a **pass code** record includes making any reasonable attempt to disguise the **pass code** within the record, or prevent unauthorised access to the **pass code** record, including by:

a) hiding or disguising the **pass code** record among other records,

b) hiding or disguising the **pass code** record in a place where a **pass code** record would not be expected to be found,

c) keeping a record of the **pass code** record in a securely locked container, or

d) preventing unauthorised access to an electronically stored record of the **pass code** record.

This list is not exhaustive.

12.4 A **user** must not act with extreme carelessness in failing to protect the security of all **pass codes** where:

a) extreme carelessness means a degree of carelessness with the security of **pass codes** that greatly exceeds what would normally be considered careless behaviour, and

b) this clause does not apply to the selection of a **pass code** by a **user**. Clause 12.5 covers this.

Note: An example of extreme carelessness is storing a **user** name and **pass code** for internet banking in a diary, blackberry or computer that is not password protected under the heading 'Internet banking codes'.

12.5 On or after 1 April 2002 a **user** must not select a numeric **pass code** that represents their birth date, or an alphabetical **pass code** that is a recognisable part of their name, if a **subscriber** has:

a) specifically instructed the **user** not to do so, and

b) warned the **user** of the consequences of doing so.

12.6 A **subscriber** must **give** the specific instruction and warning in clause 12.5:

a) at the time of selecting a **pass code**,

b) in a way that is designed to focus the actual **user's** attention specifically on the instruction and the consequences of breaching it, and

c) taking account of the actual **user's** capacity to understand the instruction and warning.

12.7 The onus is on the **subscriber** to prove, on the balance of probability, that it has complied with clause 12.5.

12.8 Where a **subscriber** expressly authorises particular conduct by a **user**, either generally or subject to conditions, a **user** who engages in the conduct, complying with any conditions, does not breach the **pass code** security requirements in this clause.

12.9 Where a **subscriber** expressly or implicitly promotes, endorses or authorises the use of a service for accessing a **facility** (for example, by hosting an access service on the **subscriber's** electronic address) a **user** who discloses, records or stores a **pass code** that is required or recommended for the purpose of using the service does not breach the **pass code** security requirements in this clause.

Note 1: For example, a **subscriber** may permit **user**s to **give** their **pass code(s)** to an account aggregator service offered by the **subscriber** or an associated company. If the **subscriber**:

a) promotes or endorses the service, or authorises the use of the service, a user who discloses their pass code(s) to the service does not breach the pass code security requirements in clause 12, and

b) does not promote, endorse or authorise the use of the service, a user who discloses their pass code(s) to the service may breach the pass code security requirements in clause 12.

Note 2: For example, a **subscriber** may permit **user**s to store their **pass code(s)** in an electronic folder in the **user's** own computer. If the **subscriber**:

a) promotes, endorses or authorises the storage of **pass codes** in this way, a **user** who stores their **pass code(s)** in this way does not breach the **pass code** security requirements in clause 12, and

b) does not promote, endorse or authorise the storage of **pass code(s)** in this way, a **user** who stores their **pass code(s)** in this way may breach the **pass code** security requirements in clause 12.

13 Pass code security guidelines

13.1 A **subscriber** may **give users** guidelines on ensuring the security of **devices** and **pass codes** in their terms and conditions or other communications.

13.2 Guidelines under this clause must:

a) be consistent with clause 12,

b) clearly distinguish the circumstances when **holders** are liable for **unauthorised transactions** under **this Code**, and

c) include a statement that liability for losses resulting from **unauthorised transactions** will be determined by **this Code**, rather than the guidelines.

Note: **Subscribers** must provide a process for **users** to report the loss, theft or misuse of a **device** or **pass code**: see clause 17. **Subscribers** must include on or with statements, at least annually, a summary of the **pass code** security guidelines under this clause: see clause 8.

14 Liability for loss caused by system or equipment malfunction

14.1 A **holder** is not liable for loss caused by the failure of a system or equipment provided by any party to a shared electronic network to complete a **transaction** accepted by the system or equipment in accordance with a **user's** instructions.

14.2 Subject to clause 14.3, a **subscriber** must not deny, explicitly or implicitly, a **user's** right to claim consequential damages resulting from a malfunction of a system or equipment provided by any party to a shared electronic network, however caused.

14.3 Despite clause 14.2, where a **user** should reasonably have been aware that a system or equipment provided by any party to a shared electronic network was unavailable or malfunctioning, the **subscriber's** liability may be limited to:

a) correcting any errors, and

b) refunding any fees or charges imposed on the **user**.

15 Network arrangements

15.1 In this clause:

merchant acquirer means a **subscriber** that provides a service to merchants that enables them to accept/receive electronic payments

party to a shared electronic network includes retailers, merchants, communications services providers and other organisations offering facilities, merchant acquirers and **subscribers**

15.2 A **subscriber** must not avoid any obligation owed to **users** under **this Code** on the basis that:

a) it is a party to a shared electronic payments network, and

b) another party to the network caused the failure to meet the obligation.

15.3 A **subscriber** must not require a **user** who is their customer to:

a) raise a **complaint** or dispute about the processing of a **transaction** with any other party to a shared electronic payments network, or

b) have a **complaint** or dispute investigated by any other party to a shared electronic payments network.

15.4 Where a merchant acquirer:

a) is advised by another party to a shared electronic payments network, or

b) forms the view

that a **transaction** has been debited or credited incorrectly to a **facility**, the **merchant acquirer** must report this to the **subscriber** that provides the **facility** to the **holder**.

15.5 A **subscriber** that is informed of an incorrect **transaction** under clause 15.4 must investigate the report and make any correction to a **facility** it considers appropriate.

15.6 A **subscriber** that makes a correction under clause 15.5 must:

a) notify the **holder** as soon as practicable, if the **subscriber** knows their identity and contact details,

b) include any correction in the next statement the **subscriber gives** the **holder** under a normal statement cycle, if the **subscriber** is required to **give** statements (see clause 7), and

c) on request, **give** the **holder** any further information the **holder** requests about the correction.

16 Audit trails

Subscribers must be capable of producing audit trails

16.1 A **subscriber** must ensure that it can generate sufficient records to enable **transaction**s to be traced and checked and to identify and correct errors.

17 Process for reporting

Process for reporting unauthorised transactions, loss, theft etc

17.1 A **subscriber** must have an effective and convenient process for **users** to report:

a) **unauthorised transactions**,

b) loss, theft or misuse of a **device**, or

c) breach of security of a **pass code**.

17.2 The process must be free, or for the cost of a local call only.

Note: For example, a telephone hotline that is available 24 hours a day, 7 days a week or includes a **facility** for leaving messages after hours satisfies this requirement.

17.3 If a **user** reports the loss, theft or misuse of a **device** or breach of security of a **pass code**, the liability of the **user** for **unauthorised transactions** is limited by Chapter C of **this Code**.

17.4 A **subscriber** is liable for any loss that occurs while its process is unavailable, provided that a report is made within a reasonable time of the process again becoming generally available.

17.5 A **subscriber** must acknowledge the receipt of every report of an **unauthorised transaction**, the loss, theft or misuse of a **device**, or breach of security of a **pass code**, including telephone reports. An acknowledgment:

a) does not have to be in writing, but

b) must enable **users** to verify that they have made a report and when it was made.

Note: For example, **subscribers** may **give** the **user** a reference number to verify that a report has been made by telephone.

18 Low value facilities

Tailored requirements for low value facilities

18.1 Chapter C does not apply to a **low value facility**.

Note: A **subscriber** that provides a **low value facility** must tell **users** whether the **subscriber** provides a process to report the loss, theft or misuse of a **device** or breach of **pass code**: see clause 4.9.

Chapter D: Conduct

Key points

This Chapter requires **subscribers** to:

- comply with minimum **expiry date** requirements for products that have **expiry date**s,
- ensure the security of deposits, and
- not allow merchants to engage in **book-up** practices.

This chapter also:

- sets out requirements for electronic communication, and
- provides guidelines to help **subscribers** comply with privacy laws.

19 Minimum expiry dates

Minimum expiry dates

19.1 If a **facility**:

a) is not reloadable, and

b) the **facility** and/or a **device** used to perform **transactions** on the **facility** cannot be used after a certain date,

the **expiry date** must be at least 12 months from the date the **user** activates the **facility**.

19.2 If a **facility**:

a) is reloadable, and

b) the **facility** and/or a **device** used to perform **transactions** on the **facility** cannot be used after a certain date,

the **expiry date** must be at least 12 months from the date the **user** last reloads the **facility**.

Conditions

19.3 A **subscriber** that offers a **facility** that has an **expiry date** must:

a) not unilaterally bring forward the **expiry date**, and

b) **give user**s a way to check the **expiry date** (for example, using the mechanism provided for **users** to check their balance).

19.4 If a **device** is needed to perform **transactions**:

a) a **subscriber** must disclose the **expiry date** on the **device**, or

b) if a **subscriber** cannot ascertain the **expiry date**, because it depends on the date a **user** activates or reloads a **facility**, the **subscriber** must disclose on the **device** the period during which the **facility** will be able to be used to make **transactions**,

in a way that is clear and prominent before the **user** first uses the **facility** to perform a **transaction**.

Note: For example, if a **facility** expires 12 months from the date it is activated or last reloaded, the **subscriber** can comply with this clause by disclosing this on the **device**.

20 Deposits using electronic equipment

20.1 A **subscriber** is responsible for a deposit or payment into a **facility** received at a **subscriber's** equipment, from the time the **user** completes the deposit, subject to verification of the amount or amounts deposited.

20.2 If a **user** deposits or loads funds onto a **facility**, and there is a discrepancy between the amount recorded by electronic equipment or a **device** as being deposited, and the amount recorded by the **subscriber** as being received, the **subscriber** must contact the **user** as soon as practicable, and notify the **user** of the difference, and the amount that will be adjusted to the **facility**.

21 Book up

21.1 When a **subscriber** and a merchant have a merchant agreement, the agreement must prohibit the merchant from holding a **user's pass code** as part of a **book up arrangement**.

22 Electronic communication

22.1 A **subscriber** can meet its obligations under **this Code** by either sending information by electronic communication, or using electronic communication to notify **users** that information is available from an electronic address, if the following conditions are met:

a) **users** must positively agree to electronic communication,

b) it must be easy for **users** to retrieve, read, save electronically and print the information,

c) the information must be available at an electronic address provided by the **subscriber** for a reasonable period,

d) the **user** must be able to request a paper copy of the information, for up to seven years, and

e) the **subscriber** must provide a **user**-friendly process for **users** to update their electronic contact details.

22.2 When a **subscriber** provides a **facility** designed exclusively for electronic use,

a) the **subscriber** can meet its obligations under **this Code** by either:

i. sending information using electronic communication, or

ii. using electronic communication to notify **user**s that information is available from an electronic address,

if the **subscriber** clearly discloses that it will use this method of communication before the **user** first performs a **transaction** using the **facility**, and

b) clause 22.1(d) does not apply.

Note: While the use of hyperlinks to **give** disclosures or information under **this Code** is not prohibited, it is discouraged as a matter of best practice.

23 Privacy

23.1 The following guidelines are provided to help a **subscriber** interpret the National Privacy Principles, or any statutory Privacy Principles that replace the National Privacy Principles in the future, and apply them to **transactions**:

a) Where a **subscriber** may use surveillances **devices** (for example, visual, sound or data recording) to monitor **transactions**:

i. the **subscriber** must notify **users** before the commencement of each **transaction** or session of **transactions** that the **transaction(s)** may be recorded by a surveillance **mechanism**, and explain the nature of the surveillance, but

ii. this does not apply to general surveillance **mechanisms** that are not specifically designed to monitor **transactions**.

Note: For example, this does not apply to cameras that are designed to record the entrance to a building.

b) A **subscriber** must take reasonable steps to ensure that no equipment or system the **subscriber** operates can **give** information about a **facility** to a person who is not authorised to access the information.

c) **Transaction** receipts must not disclose information that would reveal a:

i. full **identifier**, or

ii. a **user's** name or address.

d) If **users** can obtain information about, or perform, **transactions** through a **subscriber's** electronic address, the **subscriber** must:

i. make a clear privacy policy available through that address, and

ii. **give** the privacy policy to **users** on request.

Note: For example, a **subscriber** can comply with clause 23.1(d) by putting its privacy policy on its website.

Chapter E: Additional conduct requirements for ADIs

Key points

This Chapter explains the procedures for:

- dealing with mistaken internet payments, and
- providing listing and switching services.

24 Scope and definitions

Scope

24.1 This Chapter applies to **subscribers** that are **ADIs** except **ADIs** that are solely providers of purchased payment facilities.

Definitions

24.2 In this Chapter:

account means an account maintained by a **subscriber** that belongs to an identifiable **holder** who is a customer of the **subscriber**

BECS Procedures means the Bulk Electronic Clearing Systems Procedures as existing from time to time

BECS return request procedures means the Bulk Electronic Clearing Systems Return Request Procedures

Note: A summary of the BECS Return Request Procedures is available at the Australian Payments Clearing Association website at: www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/RP_BECS.

direct entry means a direct debit or direct credit as defined in the Bulk Electronic Clearing System Procedures

direct entry user means a person who issues credit or debit payment instructions using the Bulk Electronic Clearing System Procedures

mistaken internet payment means a payment by a user through a 'Pay anyone' internet banking **facility** and processed by an **ADI** through direct entry where funds are paid into the account of an unintended recipient because the user enters or selects a BSB number and/or **identifier** that does not belong to the named and/or intended recipient as a result of:

a) the **user's** error, or

b) the **user** being advised of the wrong BSB number and/or **identifier**.

This does not include payments made using BPay.

purchased payment facility means a facility that satisfies all of the following conditions:

a) the **facility** is purchased by a person from another person,

b) the **facility** can be used to make payments up to the amount that from time to time is available for use under the conditions that apply to the **facility**,

c) those payments are to be made by the provider of the **facility** or by a person acting under an arrangement with the provider (rather than by the **user** of the **facility**), and

d) is not covered by a declaration under section 9(3) of the *Payments Systems (Regulation) Act 1998*.

Note: See section 9 of the *Payment Systems (Regulation) Act 1998*.

sending ADI means an **ADI** whose customer has made an internet payment

receiving ADI means an **ADI** whose customer has received an internet payment

unintended recipient means the recipient of funds as a result of a mistaken internet payment.

Mistaken internet payments

25 Preventing mistaken internet payments

25.1 A **subscriber** must clearly warn **user**s about the importance of entering the correct **identifier** and the risks of mistaken internet payments, including that:

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

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

25.2 The warning required under clause 25.1 must be delivered:

a) on-screen, and

b) when a **user** is performing a **transaction** using a pay anyone internet banking **facility**, and

c) before the **transaction** is finally confirmed, at a time when the **user** can cancel the **transaction**.

26 Disclosure

26.1 The terms and conditions for accounts that enable **users** to make a payment through a 'Pay anyone' internet banking **facility** must set out the processes prescribed in this clause including:

a) the circumstances in which a **subscriber** will recover funds from an unintended recipient without their consent, and

b) the circumstances in which a **holder** will be liable for losses arising from mistaken internet payment.

27 Reporting

27.1 A **subscriber** must have a clear and accessible way for **users** to report mistaken internet payments.

27.2 The mechanism must be free, or for the cost of a local call only.

Note: For example, a telephone hotline that is available 24 hours a day, 7 days a week or includes a **facility** for leaving messages after hours satisfies this requirement.

27.3 A **subscriber** must acknowledge the receipt of every report of a mistaken internet payment, including telephone reports. An acknowledgement does not have to be in writing, but must enable **users** to verify that they have made a report and when it was made.

28 ADIs must investigate

28.1 Where a **user** reports a mistaken internet payment, the sending **ADI** must investigate whether a mistaken internet payment has occurred.

28.2 If the sending **ADI** is satisfied that a mistaken internet payment has occurred:

a) the sending **ADI** must send the receiving **ADI** a request for the return of the funds, and

b) the receiving **ADI** must acknowledge a request by a sending **ADI** for the return of funds within 5 **business days**.

28.3 If not satisfied that a mistaken internet payment has occurred, the sending **ADI** is not required to take any further action.

29 Process where funds are available and report is made within 10 business days

29.1 The following process applies where a **user** reports a mistaken internet payment within 10 **business days** of making the payment, and the sending **ADI** is satisfied that:

a) a mistaken internet payment has occurred, and

b) there is sufficient credit funds available in the account of the unintended recipient to the value of the mistaken internet payment.

29.2 If satisfied that a mistaken internet payment has occurred, the receiving **ADI** must return the funds to the sending **ADI**, within 5 **business day**s of receiving the request from the sending **ADI** if practicable or such longer period as is reasonably necessary, up to a maximum of 10 **business days**.

29.3 If not satisfied that a mistaken internet payment has occurred, the receiving **ADI** may seek the consent of the unintended recipient to return the funds to the holder.

29.4 The sending **ADI** must return the funds to the holder as soon as practicable.

30 Process where funds are available and report is made within 7 months

30.1 The following process applies where a **user** reports a mistaken internet payment between 10 **business days** and seven months of making the payment, and the sending **ADI** is satisfied that:

a) a mistaken internet payment has occurred, and

b) there is sufficient credit funds available in the account of the unintended recipient to the value of the mistaken internet payment.

30.2 The receiving **ADI** must complete its investigation into the reported mistaken payment within 10 **business days** of receiving the request.

30.3 If satisfied that a mistaken internet payment has occurred, the receiving **ADI** must:

a) prevent the unintended recipient from withdrawing the funds for 10 further **business days**, and

b) notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish that they are entitled to the funds within 10 **business days** commencing on the day the unintended recipient was prevented from withdrawing the funds.

30.4 If the unintended recipient does not, within 10 **business days**, establish that they are entitled to the funds, the receiving **ADI** must return the funds to the sending **ADI** within 2 **business days** after the expiry of the 10 **business day** period during which the unintended recipient is prevented from withdrawing the funds from their account.

30.5 If the receiving **ADI** is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to the holder.

30.6 The sending **ADI** must return the funds to the **holder** as soon as practicable.

31 Process where funds are available and report is made after 7 months

31.1 The following process applies where a **user** reports a mistaken internet payment more than seven months after making the payment, and the sending **ADI** is satisfied that:

a) a mistaken internet payment has occurred, and

b) there is sufficient credit funds available in the account of the unintended recipient to the value of the mistaken internet payment.

31.2 If the receiving **ADI** is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds to the **user**.

31.3 If not satisfied that a mistaken internet payment has occurred, the receiving **ADI** may seek the consent of the unintended recipient to return the funds to the holder.

31.4 If the unintended recipient consents to the return of the funds:

a) the receiving **ADI** must return the funds to the sending **ADI**, and

b) the sending **ADI** must return the funds to the **holder** as soon as practicable.

32 Relationship with Code of Operation for Centrelink Direct Credit Payment

32.1 Where the unintended recipient of a mistaken internet payment is receiving income support payments from Centrelink, the receiving **ADI** must recover the funds from the unintended recipient in accordance with the Code of Operation for Centrelink Direct Credit Payment.

33 Process where funds are not available

33.1 Where the sending **ADI** and the receiving **ADI** are satisfied that a mistaken internet payment has occurred, but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving **ADI** must use reasonable endeavours to retrieve the funds from the unintended recipient for return to the **holder** (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

34 Sending ADI must inform user of outcome

34.1 The sending **ADI** must inform the **user** of the outcome of the reported mistaken internet payment:

a) in writing, and

b) within 30 **business days** of the day on which the report is made.

35 Complaints about mistaken payments

35.1 A **user** who reports a mistaken payment can complain to the sending **ADI** about how the report is dealt with, including that the sending **ADI** and/or the receiving **ADI**:

a) is not satisfied that a mistaken internet payment has occurred, or

b) has not complied the processes and timeframes set out in clauses 25–34.

35.2 A sending **ADI** that receives a **complaint** under clause 35.1:

a) must deal with the **complaint** under its internal dispute resolution procedures, and

b) must not require the **user** to complain to the receiving **ADI**.

Note: **Subscribers** cannot require a **user** who is their customer to raise a **complaint** with another party to a shared electronic payments network: see clause 17.1.

35.3 If the **user** is not satisfied with the outcome of a **complaint** under clause 35.1, the **user** must be able to complain to the external dispute resolution scheme the sending **ADI** belongs to.

35.4 Both the sending **ADI** and the receiving **ADI** must cooperate with the sending **ADI**'s external dispute resolution scheme, including complying with any decision of that scheme (for example, about whether a mistaken payment did in fact occur).

Note: The procedures for dealing with mistaken internet payments under this clause are different to the procedures for dealing with complaints under Chapter F of this Code and do not diminish the obligations of subscribers to comply with Chapter F of this Code.

36 Listing and switching

Listing service

36.1 A **user** seeking to switch to a different can ask their current **ADI** to provide a listing service.

36.2 If a **holder** requests a listing service under clause 36.1, their current **ADI** must **give** the **holder** lists of their:

a) direct debit arrangements,

b) direct credit arrangements, and

c) periodical payments

for the previous 13 months.

36.3 The lists of direct debit arrangements and direct credit arrangements under clause 36.2(a) and (b) must include all of the following information:

a) the direct entry **user** identity,

b) the name of the direct entry **user**,

c) the name of the remitter,

d) the unique lodgement reference,

e) the last payment date,

f) the type of arrangement (whether debit or credit), and

g) the amount of the **transaction**.

36.4 The list of periodical payments under clause 36.2(c) must include all of the following information:

a) BSB and **identifier** of the payee,

b) name of the payee,

c) narrative,

d) payment date, and

e) amount of **transaction**.

36.5 Where, for a periodical payment, a duplicate lodgement reference is used for the same direct entry **user** identity, the list of periodical payments under clause 36.2(c) must include the most recent payment date for the arrangement.

36.6 If a **holder** requests a listing service under clause 36.2 their current **ADI** must **give** the **holder** instructions to help the **holder** identify their own internet 'Pay Anyone' payments.

36.7 **Subscribers** must **give** the lists and information under clauses 36.2–36.6 as soon as practicable, and no later than 5 **days** after the request.

36.8 An **ADI** that provides a listing service must, if relevant, advise the **holder** that:

a) the lists may not include one-off payments, and

b) some cancelled arrangements may appear on the lists.

Switching service

36.9 When opening a personal **transaction** account for a **holder** who is switching from another **ADI**, an **ADI** must **give** the **holder** relevant information to help them make the switch.

36.10 This must include a customised switching service, which must incorporate an industry standardised 'change of account' letter template for the **holder** to **give** organisations with which they have arrangements for direct debits, direct credits or periodical payments.

36.11 A **holder** who is switching from one **ADI** to another can request the new **ADI** to provide a switching service to help the **holder** notify organisations with which the **holder** has arrangements for direct debits, direct credits or periodical payments that the **holder** has switched to a new **ADI**.

36.12 If a **holder** requests a switching service under clause 36.11, their **ADI** must:

a) ask the **holder** to provide a list of their direct debit and direct credit arrangements,

b) on receiving the **holder's** consent, notify the direct entry **user's ADIs** of the changed account details within 2 **business days** of the **holder's** request, and

c) advise the **holder** of the **holder's** responsibilities for direct debit and credit arrangements.

36.13 When a direct entry **user's ADI** receives information about a **holder's** changed account details, the **ADI** must forward the relevant information to the direct entry **user** within 3 **business days**.

36.14 A direct entry **user** that is an **ADI** making direct debits or direct credits on behalf of its customers, is responsible for notifying the originator of the debit or credit of the changed account details.

Chapter F: Complaints

Key points

This Chapter:

- requires **subscribers** to maintain internal dispute resolution procedures that comply with AS ISO 10002-2006 consistent with Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165),
- imposes a limitations period for **complaints** and time frames for resolving **complaints**,
- sets out procedures for dealing with **complaints**, and
- includes tailored requirements for **complaints** about credit cards, debit cards and charge cards and **complaints** about a **subscriber** that is not required to comply with RG 165.

37 AS ISO 10002-2006

Compliance with AS ISO 10002-2006

37.1 A **subscriber** that is an Australian financial services licensee, unlicensed product issuer, unlicensed secondary seller, Australian credit licensee or credit representative must have internal dispute resolution procedures that comply with:

a) **ASIC** Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165); and

b) AS ISO 10002-2006 *Customer satisfaction – Guidelines for complaints handling in organizations* to the extent required by RG 165.

38 Complaints procedures

Limitations period

38.1 A **subscriber** must accept a **complaint** if it receives the **complaint** within 6 years from the day that the **user** first became aware, or should reasonably have become aware, of the circumstances giving rise to the **complaint**.

Complaints procedures

38.2 When a **user** complains about an **unauthorised transaction**, the **subscriber** must make reasonable efforts to obtain from the **user** at least the information set out in Appendix A, where it is relevant and available.

38.3 A **subscriber** must resolve **complaints** in accordance with **this Code**.

Timeframes

38.4 Within 21 **days** of receiving a **complaint**, a **subscriber** must:

a) complete the investigation and advise the **user**, in writing, of the outcome, or

b) advise the **user** in writing of the need for more time to complete its investigation.

38.5 Unless there are exceptional circumstances, a **subscriber** must complete its investigation within 45 **days** of receipt of the **complaint**.

Note: For example, exceptional circumstances may include delays caused by other subscribers or foreign merchants involved in resolving the complaint.

Cooperation between subscribers

38.6 A **subscriber** must respond to requests for information from other **subscriber**s within 15 **days**, unless there are exceptional circumstances.

Explain outcome of complaint

38.7 A **subscriber** must tell a **user** who makes a **complaint**:

a) the outcome of the **complaint**, and

b) the reasons for the outcome, including references to the relevant clauses of **this Code**.

38.8 When a **complaint** is settled to the complete satisfaction of a **user** and a **subscriber** within 5 **business day**s, the **subscriber** is not required to advise the **user** in writing of the outcome of the **complaint**, unless the **user** requests a written response.

38.9 When a **complaint** is not settled to the complete satisfaction of a **user** and a **subscriber** within 5 **business day**s, the information in clause 38.7 must be given in writing.

Compensation for non-compliance with this Code

38.10 Where a **subscriber**, its employees or agents do not comply with **this Code**, and this contributes to:

a) a decision about a **complaint** that is against the **user** (including an initial decision), or

b) delaying the resolution of a **complaint** (including by contributing to the **user** referring the **complaint** to external dispute resolution),

the **subscriber**, or an external dispute resolution scheme, may decide the **subscriber** is liable for part or all of the amount of a disputed **transaction**, as compensation for the effect of the decision about the **complaint** or delay in resolving it, even if the **subscriber** or external dispute resolution scheme decide the **subscriber** is not liable under Chapter C.

38.11 The amount of any award in favour of a **user** under clause 38.10 is matter for the senior management of the **subscriber** or the external dispute resolution body, having regard to all the circumstances.

Note: For example, where a **subscriber** does not obtain the information required under Appendix A or analyse it in accordance with Chapter C, an award of part or all of the disputed amount to the **holder** may be justified, to compensate the **holder** for the inconvenience and expense caused to them.

Providing information to EDR schemes

38.12 Where an external dispute resolution scheme asks a **subscriber** for information to help it resolve a **complaint** and the **subscriber** does not provide the information:

a) the scheme must **give** the **subscriber** an opportunity to explain why it 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 information available to it.

Tailored requirements for certain subscribers

38.13 A **subscriber** that is not an Australian financial services licensee, unlicensed product issuer, unlicensed secondary seller, Australian credit licensee or credit representative:

a) does not have to comply with this Chapter, and

b) instead, must comply with Appendix B.

39 Tailored requirements for complaints covered by card scheme rules

Tailored requirements for complaints covered by card scheme rules

39.1 When a **subscriber** decides to resolve a **complaint** about a credit card, debit card or charge card by exercising its rights under the rules of the card scheme:

a) the time limits under the rules of scheme apply instead of the time limits in clauses 38.4–38.5,

b) clause 38.6 does not apply. Instead, if the **subscriber** is not able to resolve the **complaint** within 60 **days**, it must **give** the **user**:

i. the reason for the delay,

ii. updates on progress with the **complaint** once every two months, and

iii. a date when the **user** can reasonably expect a decision, unless the **subscriber** is waiting for a response from the **user**, and has advised the **user** that it requires their response,

c) the **subscriber** must inform the **user** in writing of:

i. the time limits under this clause, and

ii. when the **user** can reasonably expect a decision, and

d) the **subscriber** must:

i. suspend the **user's o**bligation to pay any amount which is the subject of the **complaint**, and any credit and other charges related to that amount, until the **complaint** is resolved, and

ii. inform the **user** of this.

Chapter G: Administration

Key points

This Chapter:

- sets out when **this Code** commences,
- **gives ASIC** a general power to modify the application of **this Code**,
- requires **subscriber**s to report information about **unauthorised transactions**, and
- requires **ASIC** to monitor compliance with **this Code** and review **this Code** every five years.

40 Commencement

Commencement date

40.1 **This Code** commences on 1 July 2012.

40.2 A **subscriber** can choose to be bound by **this Code** at an earlier date than 1 July 2012.

41 Subscription

Subscription

41.1 An entity may **subscribe** to **this Code** by:

a) completing the EPayments Code subscription form available at www.asic.gov.au, and

b) returning the completed form electronically or by mail to:

ASIC
Consumers, Advisers and Retail Investors
GPO Box 9827
Melbourne VIC 3001

c) A **subscriber** to the previous version of this Code will need to re-subscribe to this version of **this Code** by 1 July 2012 to remain a **subscriber**.

42 Interpretation

42.1 **ASIC** may issue guidelines interpreting **this Code**.

42.2 The Headings and Notes to clauses in **this Code** do not form part of the Code but may be used to interpret the Code.

43 Modification

Exemptions and declarations by ASIC

43.1 **ASIC** may, by written instrument:

a) exempt a **subscriber** or a class of **subscriber**s from specified clauses of **this Code**, or

b) declare that **this Code** applies in relation to:

i. a particular facility or class of facility, or

ii. a subscriber or class of subscribers,

as if the specified clauses were modified as specified in the declaration.

43.2 An exemption may be unconditional, or may be subject to specified conditions. A **subscriber** to whom a condition specified in an exemption applies must comply with the condition.

43.3 Before making an exemption or declaration, **ASIC** must be satisfied that any consultation that is considered by **ASIC** to be appropriate and that is reasonably practicable to undertake, has been undertaken.

43.4 Before making an exemption or declaration, **ASIC** must have regard to the following:

a) whether the exemption or declaration would be consistent with the objectives of **this Code**,

b) whether the application of **this Code** would be inappropriate in the circumstances, and

c) whether the application of **this Code** would impose unreasonable burdens.

43.5 **ASIC** must publish notice of the written instrument on its website as soon as reasonably practicable after making the instrument.

44 Monitoring and periodic review

Compliance monitoring

44.1 A **subscriber** must report to **ASIC** or its agent annually the following information about **unauthorised transactions**:

a) number,

b) value,

c) channels, and

d) how **complaint**s about **unauthorised transaction**s were resolved, outcomes and average timeframes for these resolutions.

44.2 **ASIC** or its agent may undertake targeted compliance monitoring of specific obligations under **this Code**. The focus of this may change from time to time. A **subscriber** may be required to report information about compliance with specific clauses of **this Code** as part of targeted compliance monitoring activities.

Review

44.3 **ASIC** or its agent must review **this Code** five years following the conclusion of each preceding review.

44.4 As part of each review, **ASIC** or its agent must consult with stakeholders, including:

a) **subscribers** and their respective industry associations,

b) federal, state and territory government agencies,

c) consumer representatives, and

d) external dispute resolution schemes.

Appendix A: Unauthorised transactions

A1.1 When a **user** complains about an **unauthorised transaction**, the **subscriber** must make reasonable efforts to obtain from the **user** the following information:

1. type of **facility**,
2. where relevant, **identifier**,
3. type of **device** and/or **pass code** used to perform the **transaction**,
4. name and address of **holder**,
5. name of other **user/s**,
6. whether a **device** used to perform the **transaction** was signed by the **user**,
7. whether a **device** was lost, stolen or misused or the security of a **pass code** was breached and if so:
   a) the date and time of the loss, theft, or misuse of the **device** or breach of **pass code** security,
   b) the time the loss, theft, or misuse of the **device** or breach of **pass code** security was reported to the **subscriber**, and
   c) the date, time and method of reporting the loss, theft, or misuse of the **device** or breach of **pass code** security to the police,
8. where one or more **pass codes** were required to perform **transactions**, whether the **user** recorded the **pass code(s)**, and if so:
   a) how the **user** recorded the **pass code(s)**,
   b) where the **user** kept the record, and
   c) whether the record was lost or stolen, and if so, the date and time of the loss or theft,
9. where one or more **pass codes** were required to perform **transactions**, whether the **user** had disclosed the **pass code(s)** to anyone,
10. details of where and how the loss, theft or misuse of a **device** or breach of **pass code** security occurred (for example, housebreaking, stolen wallet),
11. details of the **transaction** to be investigated including:
    a) description,
    b) date and time,
    c) amount, and
    d) type and location of electronic equipment used,
12. details of any surrounding circumstances,
13. any steps taken by the **user** to ensure the security of any **device** or **pass code(s)** needed to perform **transactions** that the **user** considers relevant to the liability of the **holder**, and
14. details of the last authorised **transaction** performed using the **facility**.

Appendix B: Complaints procedures

Scope

B1.1 A **subscriber** that is an Australian financial services licensee, unlicensed product issuer, unlicensed secondary seller, Australian credit licensee or credit representative must comply with RG 165 and Chapter F of **this Code**.

B1.2 Other **subscriber**s must instead comply with this Appendix.

Limitations period

B2.1 A **subscriber** must accept a **complaint** if it receives the **complaint** within 6 years from the day that the **user** first became aware, or should reasonably have become aware, of the circumstances giving rise to the **complaint**.

Timeframes

B3.1 Within 21 **days** of receiving a **complaint**, a **subscriber** must:

a) complete the investigation and advise the **user**, in writing, of the outcome, or

b) advise the **user** in writing of the need for more time to complete its investigation.

B3.2 Unless there are exceptional circumstances, a **subscriber** must complete its investigation within 45 **days** of receipt of the **complaint**.

Note: For example, exceptional circumstances may include delays caused by other **subscribers** or foreign merchants involved in resolving the **complaint**.

B3.3 If a **subscriber** cannot resolve a **complaint** within 45 **days**, it must:

a) explain the reason for the delay to the **user**,

b) **give** the **user** monthly updates on progress with the **complaint**, and

c) **give** the **user** a date when they can reasonably expect a decision,

unless the **subscriber** is waiting for a response from the **user**, and has advised the **user** that it requires this response.

B3.4 Where a **subscriber** is a member of an external dispute resolution scheme, and the rules of the scheme provide that it can accept a **complaint** if a **subscriber** has not made a decision within a specified time period, the **subscriber** must inform the **user** that they can complain to the scheme on this basis. The **subscriber** must provide this information no more than 5 **business day**s after the **user** can complain to the scheme on this basis.

Australian standard on complaints handling

B4.1 Definition of **complaint**: A **subscriber** must adopt the following definition of **complaint** under AS ISO 10002-2006 *Customer satisfaction – Guidelines for complaints handling in organizations*, which is:

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

B4.2 A **subscriber** must have internal dispute resolution procedures that comply with AS ISO 10002-2006 *Customer satisfaction – Guidelines for complaints handling in organizations,* or its successor, to the extent required by RG 165.

Disclosure

B5.1 A **subscriber** must explain the procedure for making **complaints**:

a) in the terms and conditions for facilities,

b) in its general documentation, and

c) on request.

B5.2 When a **complaint** is not settled to the complete satisfaction of a **user** and a **subscriber** within 5 **business days**, a **subscriber** must advise the **user** in writing of its **complaint**s handling procedures.

Complaints procedures

B6.1 When a **user** complains about an **unauthorised transaction**, the **subscriber** must make reasonable efforts to obtain from the **user** at least the information set out in Appendix A, where it is relevant and available.

B6.2 A decision about a **complaint** must be made on the basis of all relevant established facts and not on the basis of inferences unsupported by evidence.

Cooperation between subscribers

B7.1 A **subscriber** must respond to requests for information from other **subscriber**s within 15 **days**, unless there are exceptional circumstances.

Explain outcome of complaint

B8.1 A **subscriber** must tell a **user** who makes a **complaint**:

a) the outcome of the **complaint**, and

b) the reasons for the outcome, including references to the relevant clauses of **this Code**.

B8.2 When a **complaint** is settled to the complete satisfaction of a **user** and a **subscriber** within 5 **business** days, the **subscriber** does not have to advise the **user** in writing of the outcome of the **complaint**, unless the **user** requests a written response.

B8.3 When a **complaint** is not settled to the complete satisfaction of a **user** and a **subscriber** within 5 **business days**, the information in clause B8.1 of this Appendix must be given in writing.

B8.4 If a **complaint** is not resolved completely in favour of a **user**, the **subscriber** must also:

a) **give** the **user** contact details for any external dispute resolution scheme the **subscriber** belongs to, or

b) if the **subscriber** does not belong to any external dispute resolution scheme, give the **user** the contact details for the consumer affairs agency small claims tribunal or court in the **user's** jurisdiction.

This information must be in writing.

B8.5 If a **subscriber** decides that a **facility** has been incorrectly debited or credited, it must:

a) adjust the balance of the **facility**, including appropriate adjustments for interest and fees or charges, where relevant,

b) notify the **holder** in writing as soon as practicable of the amount with which the **facility** has been debited or credited, if the **subscriber** knows their identity and contact details,

c) include the correction in the next statement the **subscriber gives** the **holder** under a normal statement cycle, if the **subscriber** is required to **give** statements under clause 7 of **this Code**, and

d) **give** the **holder** any further information the **holder** requests about the correction.

B8.6 Where a **subscriber** decides that a **holder** is partly or wholly liable for a **transaction** under Chapter C of **this Code**, the **subscriber** must:

a) **give** the **user** copies of any documents or other evidence, including information about the **transaction** from any logs or audit trails, and

b) advise the **holder**, in writing, whether there was any system or equipment malfunction at the time of the **transaction**.

Compensation for non-compliance with this Code

B9.1 Where a **subscriber**, its employees or agents do not comply with **this Code**, and this contributes to:

a) a decision about a **complaint** that is against the **user** (including an initial decision), or

b) delaying the resolution of a **complaint** (including by contributing to the **user** referring the **complaint** to external dispute resolution),

the **subscriber**, or an external dispute resolution scheme, may decide the **subscriber** is liable for part or all of the amount of a disputed **transaction**, as compensation for the effect of the decision about the **complaint** or delay in resolving it, even if the **subscriber** or external dispute resolution scheme decide the **subscriber** is not liable under Chapter C.

B9.2 The amount of any award in favour of a **user** under this clause is a matter for the senior management of the **subscriber** or the external dispute resolution body, having regard to all the circumstances.

Note: For example, where a **subscriber** does not obtain the information required under Appendix A, or analyse it in accordance with Chapter C, an award of part or all of the disputed amount to the **holder** may be justified to compensate the **holder** for the inconvenience and expense caused to them.

Providing information to EDR schemes

B10.1 Where an external dispute resolution scheme asks a **subscriber** for information to help it resolve a **complaint** and the **subscriber** does not provide the information:

a) the scheme must **give** the **subscriber** an opportunity to explain why it 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 information available to it.

Tailored requirements for complaints covered by card scheme rules

B11.1 When a **subscriber** decides to resolve a **complaint** about a credit card, debit card or charge card by exercising its rights under the rules of the card scheme:

a) the time limits under the rules of the scheme apply instead of the time limits in clause B3.1 and B3.2 of this Appendix,

b) clause B3.3 of this Appendix does not apply. Instead, if the **subscriber** is not able to resolve the **complaint** within 60 **days**, it must **give** the **user**:

   i. the reason for the delay,

   ii. updates on progress with the **complaint** once every two months, and

   iii. a date when the **user** can reasonably expect a decision, unless the **subscriber** is waiting for a response from the **user**, and has advised the **user** that it requires their response,

c) the **subscriber** must inform the **user** in writing of:

   i. the time limits under this clause, and

   ii. when the user can reasonably expect a decision, and

d) the **subscriber** must:

   i. suspend the **user**'s obligation to pay any amount which is the subject of the **complaint**, and any credit and other charges related to that amount, until the **complaint** is resolved, and

   ii. inform the **user** of this.

Appendix C: Defined terms

Term	Meaning
ADI	Has the same meaning as Authorised Deposit-Taking Institution in the *Banking Act 1959* (Cth) or any successor term adopted by the Australian Prudential Regulation Authority
ASIC	The Australian Securities and Investments Commission
ATM	Means automatic teller machine
biller account	An internal account maintained by a business for the purpose of recording amounts owing and paid for goods or services provided by the business
book up arrangement	Credit offered by merchants for the purchase of goods or services commonly used by Aboriginal people in remote and regional areas of Australia. It is common for merchants to hold a consumer's debit card and/or pass code as part of a book up arrangement.
business day	A day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned
complaint	An expression of dissatisfaction made to an organisation, related to its products or services, or the handling process itself, where a response or resolution is explicitly or implicitly expected. This is the definition in AS ISO 10002-2006 *Customer satisfaction – Guidelines for complaints handling in organizations*.
days	Calendar days, unless otherwise specified
device	A device given by a subscriber to a user that is used to perform a transaction. Examples include: • ATM card, • debit card or credit card, • prepaid card (including gift card), • electronic toll device, • token issued by a subscriber that generates a pass code, and • contactless device.
EFTPOS	A network for facilitating transactions at point of sale
expiry date	A restriction on a facility that means the facility cannot be used after a certain date
facility	An arrangement through which a person can perform transactions
give	Includes giving electronically, where the subscriber complies with clause 22
holder	An individual in whose name a facility has been established, or to whom a facility has been issued
identifier	Information that a user: • knows but is not required to keep secret, and • must provide to perform a transaction. Examples include: account number, serial number.
low value facility	A facility that is capable of having a balance of no more than $500 at any one time
manual signature	A handwritten signature including a signature written on paper and a signature written on an electronic tablet
merchant acquirer	This term is defined in clause 15.1
modification	Includes added, amended, omitted and substituted
pass code	A password or code, that the user must keep secret, that may be required to authenticate a transaction user. A pass code may consist of numbers, letters, a combination of both, or a phrase. Examples include: • Personal Identification Number (PIN), • internet banking password, • telephone banking password, and • code generated by a security token. A pass code does not include a number printed on a device (e.g. a security number printed on a credit or debit card).
subscriber	An entity that has subscribed to this Code
this Code	This Code: • as existing from time to time, • as it applies to a subscriber, and • to the extent it requires or enables the subscriber to do or not do something. Note: Under clause 34, ASIC may make a written instrument that affects how this Code applies in relation to a subscriber.
transaction	A transaction as defined in clause 2.4–2.6
unauthorised transaction	A transaction that is not authorised by a user
user	A holder or an individual who is authorised by a subscriber and a holder to perform transactions using a facility held by the holder