The ePayments Code Compliance Manual

August 2020

GRC solutions

IMPORTANT DISCLAIMER

All care was taken in the preparation of this Manual. However, this Manual is not to be used or relied upon as a substitute for professional legal advice on a particular matter.

Governance Risk & Compliance Solutions Pty Ltd (GRC Solutions), its directors and officers, and the authors, expressly disclaim all liability to any person in respect of this Manual and any consequence arising from its use by any person in reliance on the whole or any part of this Manual. This disclaimer does not exclude any warranties implied by law that may not be lawfully excluded.

RECORD OF UPDATES

Original Version – July 2012. Drawing on the previous EFT Manual, the new ePayments Manual was released to help organisations prepare for the commencement of the new ePayments Code on 20 March 2013.

First Update - March 2013. Provides more details about Mistaken Internet Payments and Account Switching.

Second Update - November 2014. Incorporating various updates and new case studies, together with information about reporting to ASIC.

Third Update - April 2016. Incorporating changes to the ePayments Code about electronic delivery of information that commenced on 29 March 2016, together with various other changes.

Fourth Update – August 2020

- Reflects the new AFCA external dispute resolution scheme, while noting previous FOS guidance remains a useful indicator of likely AFCA approaches.
- Clarifies coverage of the Code for business transactions.
- Notes that ASIC has commenced its review of the ePayments Code.
- Outlines how industry code of practice requirements for electronic disclosure about products and facilities relates to the ePayments Code.
- Explains the interaction of the new Open Banking regime and the ePayments Code.
- Includes new cases about an "unknown disclosure" and a disputed MOTO transaction.
- Details the ASIC review of expired travel money cards.
- Notes the change of name from Australian Payments Clearing Association (APCA) to Australian Payments Network (AusPayNet).
- Notes that ASIC RG 165 *Licensing: Internal and external dispute resolution* will be replaced by RG 271 *Internal dispute resolution* from 5 October 2021.
- Makes other changes to bring the Manual up to date.

Table of Contents

1. About this Manual

This Manual has been developed to assist subscribers to the ePayments Code [‘**the Code’**] to understand and comply with the requirements of the Code.

The Code, which replaced the Electronic Funds Transfer Code of Conduct from 20 March 2013, is the main consumer protection regulatory instrument covering electronic payments, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking and BPAY. The Code also covers transaction account switching between authorised deposit-taking institutions [**ADIs**] (Clause 35). The Australian Securities and Investments Commission [**ASIC**] is the Code administrator.

This Manual assumes your institution is a subscriber to the Code.

1.1. Structure of the Manual

This Manual has a roughly similar structure to that of the Code.

Part A: Provides a summary of the Code’s scope and key concepts.

Part B: Provides a summary of the various disclosure obligations applicable to electronic payment facilities regulated under the Code.

Part C: Sets out the general principles for determining and allocating liability for unauthorised transactions under the Code.

Part D: Outlines some of the circumstances in which an unauthorised transaction dispute may arise and gives guidance on the appropriate allocation of liability.

Part E: Outlines some additional conduct requirements related to expiry dates, deposits by electronic equipment and privacy.

Part F: Sets out additional obligations imposed on ADIs in relation to mistaken internet payments.

Part G: Sets out additional obligations imposed on ADIs in relation to the switching of transaction accounts between institutions.

Part H: Outlines the Code’s complaints handling regime and procedures to be applied when an EFT complaint is made.

Part I: Summarises Code administration arrangements, including subscribers’ obligations related to monitoring of the Code by ASIC.

1.2. Who the Manual is written for

This Manual has been written for retail banking institutions [ADIs], and focuses on the Code’s application to account-based products and facilities offered by such institutions as part of their generic banking activities.

1.3. *Low value facilities* not covered in Manual

As well as covering general account-based electronic payments, the Code includes a more limited set of requirements applicable to low value facilities (such as gift cards) where those facilities can hold a balance of no more than

$500 at any one time. Except in passing, the requirements for low value facilities under the Code are not covered in this Manual.

1.4. Use of illustrative examples

This Manual provides examples to help readers better understand the point in question. These examples indicate our opinion regarding how the Code is likely to be applied in a specific situation.

While the examples are intended to provide practical guidance on the point in question, readers should note that the actual outcome in any situation will always depend on the particular facts and circumstances involved.

1.5. References to the Code

Right-justified references in this Manual are references to the Code unless otherwise specified.

1.6. Currency of law

The regulatory requirements referred to in this Manual are current as at 31 August 2020.

1.7. Other resources

ASIC resources: Information about subscribers to the Code, reporting requirements and related matters is available on ASIC's ePayments Code homepage:

http://www.asic.gov.au/regulatory-resources/financial-services/epayments-code/

AFCA resources: see www.afca.org.au for information about AFCA approaches to dispute resolution and previous AFCA decisions. See ¶2.5 for the role of AFCA.

1.8. Important note on the Manual

All care was taken in the preparation of this Manual. However, this Manual is not to be used or relied upon as a substitute for professional legal advice on a particular matter. See the *Important Disclaimer* on the inside front page of this Manual.

You should seek advice from your legal advisers if you are uncertain about your institution's compliance with any aspect of the Code regime.

2. Introduction to the Code

The Code is an important consumer protection regulatory instrument dealing with electronic funds transfers and payments made electronically. It was released by ASIC on 20 September 2011[1]. It was updated to include additional requirements in relation to account switching on 1 July 2012[2]. A further update took effect from 29 March 2016 to facilitate easier electronic communication.[3]

2.1. Overview

The Code sets out rules and obligations that Code subscribers commit to in connection with ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking, BPAY and other consumer payment services.

It complements and extends regulatory requirements applicable to payment facilities and services under the *Corporations Act 2001* and the *National Consumer Credit Protection Act 2009*.

The Code includes:

- detailed disclosure obligations covering: the provision of terms and conditions; information about changes to terms and conditions (such as fee increases); and the provision of receipts and statements;
- a comprehensive set of rules for allocating liability for loss in cases of unauthorised transactions;
- a regime facilitating recovery of mistaken internet payments;
- rules relating to transaction account switching between institutions—these rules (which do not relate to electronic payments) have been included in the Code as a matter of administrative convenience;
- rules governing the handling of complaints about regulated transactions and facilities;
- a 'light touch' regulatory regime covering low value payment facilities (i.e. facilities capable of having a balance of no more than $500 at any one time). As retail banking institutions do not generally offer these facilities, the Code's requirements relating to low value facilities are not covered in this Manual.

[1] See ASIC Media release 11-205MR *ASIC releases new ePayments Code*
[2] See ASIC Media release 12-139MR *ASIC Implements new account switching rules*
[3] See https://asic.gov.au/regulatory-resources/financial-services/epayments-code/modifications-to-the-epayments-code/

2.2. Commencement

Since 20 March 2013 the Code has replaced the Electronic Funds Transfer (EFT) Code of Conduct [**EFT Code**], which had been in operation in various forms since 1986. While 20 March 2013 was the date on which the Code replaced the EFT Code, organisations were able to subscribe to the Code (in place of the EFT Code) from 20 September 2011. The process for subscribing to the Code is set out in *Part I – Code Administration* of this Manual.

See "About this Code" and clause 40

2.3. Voluntary Code to which entities subscribe

The Code is a voluntary industry code of conduct. As such, it is only binding on organisations that subscribe to it (called "**subscribers**").

See "About this Code"

Note, however, that:

- the great majority of Australian banks, credit unions and building societies subscribe to the Code, just as they previously subscribed to the EFT Code;
- subscribers to the Customer Owned Banking Code of Practice commit to also subscribing to the Code;
- the Code reflects good banking practice and, as such, will be regarded as setting conduct standards for retail banking institutions by regulators and AFCA , irrespective of whether a particular institution subscribes to it or not.

2.3.1 Process for subscribing to the Code

An entity may subscribe to the Code by completing the ePayments Code subscription form available at www.asic.gov.au/epaymentscode.

See clause 41.1

2.3.1. Updating subscriber details

Subscribers should periodically check that subscriber details remain up to date on the ASIC list of ePayments Code subscribers available at: http://www.asic.gov.au/for-consumers/banking /epayments-code/epayments-code-subscribers/

Some issues to check include:

- A change of subscriber's name or trading name; and
- A transfer of engagements means an organisation no longer exists.

Changes should be notified to ASIC.

2.4. Subscribers must warrant to comply with Code

By subscribing to the Code, an organisation agrees to be contractually bound by its requirements. The organisation must reflect this commitment by warranting in the terms and conditions for all its facilities that apply to consumer electronic transactions that it will comply with the Code.

See "About this Code" and clause 4.2

2.5. Role of AFCA scheme & ASIC

The Australian Financial Complaints Authority (AFCA) plays a key role in ensuring consumers receive the benefit of the protections afforded them under the Code. AFCA receives, and determines, disputes from consumer account holders seeking compensation for, in particular, alleged unauthorised transaction losses.

AFCA's predecessor, the Financial Ombudsman Service (FOS), developed detailed guidance on how it applies the Code in dealing with these disputes; and compliance staff of subscriber institutions should be aware of FOS's guidance. This Manual refers to FOS's guidance at a number of points, where there is no comparable AFCA's guidance. FOS's guidance may serve as the most current guidance about how AFCA is likely to approach individual matters.

Code compliance is also monitored by ASIC in its role as Code administrator: see *Part I – Code Administration* of this Manual for further details.

2.6. Code's relation to other legal obligations

The Code complements and extends the protections of the financial services laws, including the Corporations Act 2001 and the National Consumer Credit Protection Act 2009. As such, it imposes a range of additional obligations on subscribers to those imposed under the law.

As far as we are aware, however, the Code does not impose any obligations on subscribers which would require the subscriber to *breach* a legal obligation. Were such a situation to arise, the subscriber would be required to comply with the applicable law rather than the Code to the extent of any inconsistency. This reflects the fact that the status of the Code is subordinate to Commonwealth, State and Territory legislation.

2.7. ASIC review of ePayments Code

ASIC Consultation Paper CP 310 initiated a review of the ePayments Code. Further stages of the review process will result in a new version of the ePayments Code. It is unclear when the revised ePayments Code will commence.

See ASIC 19-049MR ASIC consultation on coverage of ePayments Code review (6 May 2019)

Part A – Scope and Key Concepts

3. Scope of the Code

As its name suggests, the Code applies to electronic payment transactions. Put simply, if a transfer is made to or from an individual account holder's account electronically, it will probably be covered by the Code.

3.1. Electronic transactions

The Code applies to electronic transactions rather than products per se. These are any payments, fund transfers or cash withdrawal transactions that are:

- initiated using electronic equipment, and
- not intended to be authenticated by comparing a manual signature with a specimen signature.

See clause 2.4

The Code is technology neutral. This allows it to apply to almost all forms of electronic transactions initiated by a consumer. Thus, the Code is specified to regulate:

- electronic card transactions, including ATM, EFTPOS, credit card and debit card transactions,
- telephone banking and bill payment transactions,
- internet banking transactions, including 'Pay Anyone',
- online transactions performed using a card number and expiry date,
- online bill payments (including BPAY),
- transactions using facilities with contactless features and prepaid cards,
- direct debits,
- transactions using mobile devices, and
- card-not-present transactions (for example, when goods and services are purchased by phone or over the telephone or Internet).

ASIC also has the power to declare that the Code applies or does not apply to a particular type of transaction.

See clause 2.5

The Code generally applies to funds transfers initiated using facilities such as Apply Pay, Android Pay, Samsung Pay, etc.

3.2. Exemption - business accounts

Transactions performed "using a facility that is designed primarily for use by a business and established primarily for business purposes" are outside the scope of the Code. This means:

- If funds are transferred from a business account to another business account or to a consumer account, the transaction will be out of scope

because it is performed using a facility designed primarily for use by a business.

- If funds are transferred from a consumer account to a business account (or another consumer account), the transfer will be covered by the Code because it is performed using a consumer facility and not a facility designed primarily for use by a business.

See clause 2.1(a)

In order to determine whether an account is a business account, it is easiest to use the "primarily for personal, domestic or household purposes" test set out in section 5(4), National Credit Code. Where the account is not for purposes that are primarily personal, domestic or household purposes, the account will usually be a business account.

3.3. Exemption – manual transactions

The Code does not apply to transactions that use a manual signature for authorisation purposes—i.e. where the transaction is "not intended to be authenticated by comparing a manual signature with a specimen signature".[4]

See clause 2.4

This means that, where a user signs a voucher to authorise a credit or debit card payment, the transaction will not be covered by the Code even though the transaction itself may be processed through electronic equipment.

Since 1 August 2014, however, PIN has become the generally mandated form of card payment authorisation for EFTPOS transactions using a credit or debit card. In consequence, the signature authorisation exemption is now of limited practical significance.

[4] This exemption can be explained historically. The predecessor EFT Code was developed primarily to address unauthorised transaction disputes involving a non-signature based means of authorisation (such as use of a PIN or password) where there was no settled common law doctrine that could be applied. By contrast, signature-authorised payment instruments have long been regulated under the common law doctrine of mandate. For this reason, the drafters of the EFT Code, and more recently the ePayments Code, did not think it necessary to extend the Code's scope to payment transactions requiring a physical signature.

4. Key concepts

The Code uses a number of defined terms. These are set out in Clause 2.6. This Chapter provides a summary of some key definitions used throughout the Code. Other terms are defined in the sections of this Manual dealing with the aspects of the Code to which those terms relate.

4.1. Device

A device is a physical item given by your institution to a user that is used to perform a transaction. Examples include:

- ATM card, debit card or credit card,
- prepaid card (including gift card),
- a token that generates a pass code, and
- a contactless device.

4.2. Facility

A facility refers to an arrangement through which a person can perform transactions. In the case of retail banking institutions, the facility will usually be the underlying account through which the electronic transactions are processed. In this Manual, we generally use the term "account" rather than "facility" as the former is the more familiar term in the banking context.

4.3. Holder

A holder means an individual in whose name a facility (such as an account) has been established, or to whom a facility has been issued. In this Manual, we generally use the term "account holder" rather than "holder" as the former is the more familiar term in the banking context.

4.4. Identifier

An identifier is information:

- known to a user (but not necessarily only to the user)
- which they must provide to or through a device or electronic equipment in order to perform a transaction, and
- which is not required to be kept secret.

Some examples include an account number or a card number.

The use of an identifier to effect a transaction will bring the transaction within the scope of the Code even if no secret pass code is involved (e.g. using a credit card number to make a purchase over the Internet).

4.5. Pass code

A pass code is a password or code that may be required to authenticate a transaction by a user. A key aspect of a pass code is that it must be kept secret. That is it must only be known to the user, or to the user and your institution.

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 number printed on a device (e.g. a security number printed on the reverse side of a credit or debit card) is not a pass code as it is not required to be kept secret.

4.6. User

A user is a person authorised by your institution and a holder to perform electronic transactions on the holder's facility. A user includes both:

- the named account holder, and
- any other person authorised by the account holder to give instructions and/or use an access method connected to their account.

The distinction between a 'user' and an 'account holder' is important because various requirements of the Code apply to one and not to the other.

FOR EXAMPLE	An account holder may have a debit card which allows them to access their savings account. The account holder may authorise another person to have access to their account via a subsidiary card. In this case, both the account holder and the subsidiary cardholder fall within the definition of 'user', even though only the first of them falls within the definition of 'account holder'.

Part B – Disclosure Obligations

5. Terms and conditions

Under the Code, your institution must provide customers with terms and conditions that apply to facilities (e.g. accounts) regulated by the ePayments Code. All individual customer accounts through which electronic transactions can be processed are subject to these requirements.

5.1. Clarity

The Code requires that your institution's terms and conditions be clear and unambiguous.

See clause 4.1

The Code does not provide specific guidance as to what this obligation of clarity means or requires. However, it can be assumed to require that:

- all information is provided in a concise and effective manner,
- plain language is used, and legal and technical jargon avoided, as far as possible
- the intended audience is able to readily understand all relevant terms and conditions.

5.2. Compliance with the Code

The Code requires your institution's terms and conditions to reflect the requirements of the Code.

It specifically prohibits subscribing institutions from attempting to create liabilities and impose responsibilities on users which exceed those set out in the Code.

The Code further requires that your institution's terms and conditions must include a warranty that the requirements of the Code will be complied with.

See clause 4.2

5.3. T&Cs for mistaken internet payments

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 the Code for dealing with mistaken payments.

In this respect the terms and conditions must include:

- the circumstances in which your institution will recover funds from an unintended recipient without their consent, and
- the circumstances in which a holder will be liable for losses arising from a mistaken internet payment.

See clause 24.1

See also: The Code's requirements covering mistaken internet payments are set out in detail in *Part F – Mistaken Internet Payments* of this Manual.

5.4. Other content of terms and conditions

Other than in relation to the matters referred to above, the Code does not prescribe the content of your institution's terms and conditions.

However, the Code does set out a list of information that must be provided to a person before they use an access method for the first time. Generally, this information will be contained in the terms and conditions document.

See also: For further details on the information that must be disclosed to a user before their first use of an access facility refer to Chapter 6.

5.5. Timeframe for provision of terms and conditions

The Code requires your institution to provide a copy of its terms and conditions to an account holder prior to or at the time a transaction is first performed using the facility.

See clause 4.3

FOR EXAMPLE	Before an account holder is able to use an ATM/EFTPOS card for the first time, you must ensure they have been provided with a copy of your institution's electronic transactions' terms and conditions.

Your institution is also required to provide account holders with a copy of the relevant terms and conditions at any other time on request.

See clause 4.3

5.5.1. Authorised users

Your institution is not required to provide a copy of its terms and conditions to an authorised user (other than the account holder) prior to their initial use of an access method.

However, while your institution is not obliged to do so, it is recommended that users such as secondary card holders be generally provided with a copy of your institution's terms and conditions at the time their authorisation is approved.

5.6. Publicise terms and conditions

The Code requires your institution to publicise the availability of its terms and conditions.

See clause 4.5

The Code does not provide any specific guidance regarding the extent to which your institution must actively promote the ability of an account holder to request a terms and conditions document.

It is likely that your institution will satisfy this obligation by including information about the availability of T&Cs: on your institution's website; in terms and conditions documents, and in promotional material for electronic transaction facilities

5.7. Changing terms and conditions

The Code requires your institution to provide account holders with notice when it changes the terms and conditions that apply to ePayment facilities.

The type of notice and nature of information which must be provided varies depending on the nature of the condition being changed.

Appendix 5.1 provides a summary of the various notification requirements.

5.7.1. Significant changes

Where the variations to the terms and conditions are important, or a significant number of changes have been made, account holders must be provided with a single document which provides a consolidated explanation of the variations made to your institution's terms and conditions.

See clause 4.14

5.7.2. Other laws

When your institution makes a change to its EFT terms and conditions, it must ensure that it also complies with any other relevant laws or Codes.

Where notification requirements are imposed under both legislation and the Code, notice must be provided in compliance with the longest notice period.

Appendix 5.1 – Summary of notification requirements

The following table summarises the various notification requirements that apply when your institution wishes to make to a change to an ePayments related term or condition. See clause 4.11 – 4.13.

Type of change	Is advance notice required?	When must notice by given	How notice must be given
Impose (i.e. for the first time) charges for issuing or replacing a device or pass code	Yes	20 days before the change takes effect	Either by: • individual notice, or • on or with account statement
An increase in a charge for issuing or replacing a device or pass code	Yes	20 days before the change takes effect	Either by: • individual notice, or • on or with account statement
Impose charges for performing electronic transactions	Yes	20 days before the change takes effect	Either by: • individual notice, or • on or with account statement
An increase in charges for performing electronic transactions	Yes	20 days before the change takes effect	Either by: • individual notice, or • on or with account statement
An increase in an account holder's liability for losses relating to transactions	Yes	20 days before the change takes effect	Either by: • individual notice, or • on or with account statement

Type of change	Is advance notice required?	When must notice by given	How notice must be given
Impose, remove or adjust a daily transaction limit or other periodic transaction limit applying to: • transactions • an account • electronic equipment **NOTE:** At the time notice is provided you must also provide the account holder with prominent advice that the removal of or an increase in that transaction limit may increase account holder liability in the case of unauthorised transactions.	Yes	20 days before the change takes effect	Either by: • individual notice, or • on or with account statement
A change required because of an immediate need to restore or maintain the security of a system or an individual account, including the prevention of criminal activity.	No	As soon as possible after the change is made	Either by: • individual notice, or • on or with account statement
All other changes	Yes	In advance of the date the change takes effect (i.e. at latest the day before the change occurs)	In a manner likely to come to the notice of as many account holders as possible.

6. Disclosure requirements prior to use

The Code requires your institution to provide *account holders*, and in some instances, *users* (i.e. both account holders and any other authorised persons), with certain information before a user performs a transaction on the account for the first time. These disclosure requirements are discussed below.

Note that this information must be provided prior to the first use of an access method.

6.1. Charges

Your institution must disclose to the *account holder* any fees or charges it imposes for the issue or replacement of a device or pass code.

Your institution must disclose to the *account holder* any fees or charges it imposes for performing a transaction. This would include any fees and charges imposed in relation to:

- withdrawals made by way of online banking or telephone banking,
- EFTPOS transactions,
- transactions at both branded and non-branded ATMs.

See clause 4.6(a) – (c)

This information must be disclosed separately from other charges that apply to the account holder's account more generally.

See clause 4.7

6.2. Restrictions

Your institution must disclose to the *account holder* details of any restrictions that it may impose on a facility. This includes the disclosure of any daily, or other periodic transaction limits which might apply to:

- the number or value of transactions a user can make,
- the use of a facility, or
- the use of any electronic equipment (such as withdrawals at an ATM).

This disclosure should also provide an indication that merchants or other institutions may impose additional restrictions.

See clause 4.6(d)

See also: For more information on determining appropriate daily or periodic transaction limits, refer to Chapter 16.

6.3. Access

Your institution must outline to the *account holder* the types of transactions that a user can perform. For example: withdrawals, deposits, transfers and bill payments.

Your institution must also disclose to the *account holder* all of the accounts that the user may access to make electronic payments. This includes a

description of any credit facility, which may be accessed through the access method.

See clause 4.6(e)

If a credit facility is accessible by an access method, your institution should take reasonable steps to warn the account holder of the risk of the access method being used to make an unauthorised transaction on that line of credit.

Failure to provide this warning may result in the account holder having their liability reduced by the AFCA scheme in the event of an unauthorised transaction drawing on an accessible line of credit.

See clause 11.9(c)

Some appropriate wording for this purpose may be as follows:

FOR EXAMPLE	"If a line of credit is made available through the access method, there is a risk that the access method may be used to make unauthorised transactions on that line of credit. Please ask a staff member if you are unsure about this risk."

6.4. Notification procedures

Your institution must disclose to the *account holder* the methods by which a user can, or is required to, provide notification of:

- the loss, theft or unauthorised use of a device, or
- the breach of security of a code.

See clause 4.6(f)

This disclosure should include the means by which a user is able to provide notification outside of normal business hours – such as a hotline telephone number.

See also: For further information on appropriate notification procedures see Chapter 12.5.

6.5. Complaint procedure

Your institution must outline to the *account holder* the means by which a user may make a complaint in relation to electronic payment facilities. This includes the procedure for querying entries listed on a periodic account statement.

See clause 4.6(g)

6.6. Expiry dates

If a facility has an expiry date[5], your institution must disclose that date to the *user* before the user first uses the facility to perform a transaction.

[5] This requirement will only be relevant to limited use, generally low value payment facilities (such as gift and other pre-paid cards). It is not applicable to account-based facilities issued by ADIs.

See clause 4.8

An expiry date is a restriction on a facility that means the facility cannot be used after a certain date.

See clause 2.6

FOR EXAMPLE	Prepaid travel cards will generally have an expiry date after which they can no longer be used for performing transactions. This date must be disclosed to the user prior to their use of the card.

If the expiry date cannot be ascertained because it depends on the date the user activates or reloads a facility, your institution must instead disclose to the *user* the period during which the facility will be able to be used to make transactions.

See clause 4.8

FOR EXAMPLE	If a facility expires 12 months from the date it is activated or last reloaded, this fact must be disclosed to the user.

6.7. Frequency of statements

Your institution should inform *account holders* of their right to receive a periodic account statement and the frequency with which such statements will be provided.

In addition, your institution must inform account holders of their right to receive account statements more frequently than the prescribed six-monthly basis.

See clause 7.2

See also: For further information on the requirement to provide account statements under the Code including the form and content of the account statements, refer to Chapter 9.

6.8. Security guidelines

Although not compulsory, it is generally recommended that your institution provide *users* with guidelines on ensuring the security of devices and pass codes.

However, where such guidelines are provided, the Code requires that your institution:

- ensure the guidelines are consistent with the pass code security requirements of the Code,
- clearly differentiate the guidelines from the circumstances in which an account holder is liable for losses resulting from unauthorised transactions under the Code, and

- include a statement that an account holder's liability for losses resulting from unauthorised transactions will be determined under the Code rather than the guidelines.

See clause 13

See also: For further information on the circumstances where an account holder is liable for losses under the Code, refer to Chapter 13.

6.9. Industry Code of Practice

If your institution subscribes to the Customer Owned Banking Code of Practice (COBCOP), certain additional information must be provided when your institution issues a subsidiary credit or debit card.

Under the COBCOP, your institution must provide the *account holder* with information on:

- the account holder's liability for any debts incurred by the subsidiary cardholder when using their card,
- how the account holder may cancel the subsidiary card, and
- that cancellation may not be effective until the subsidiary card is surrendered or unless the account holder has taken all reasonable steps to have the card destroyed or returned.

See COBCOP D.10

This information must be provided to the account holder before or at the same time as the account holder instructs your institution to issue a subsidiary card.

See also: For further information on the disclosure requirements for subsidiary cards refer to GRC Solutions' Customer Owned Banking Code of Practice Compliance Manual.

7. Transaction receipts

The ePayments Code requires that your institution take reasonable steps to offer users a receipt for all electronic transactions. Such receipts must be provided to users free of charge.

See clause 5.1 and 5.9

7.1. Required content of receipts

The Code contains rules about what information must be included in a receipt. The required content varies depending on the method by which the transaction is conducted.

7.1.1. General transactions

For transactions (e.g. ATM, EFTPOS, Internet Banking) that are conducted other than by way of voice communication, the receipt must include:

- the amount of the transaction,
- the date of the transaction (as well as the time if practicable),
- the type of transaction – for example "deposit", "withdrawal", "transfer, etc (symbols explained on the receipt and easily understood abbreviations may be used),
- an indication of the account(s) being debited or credited,
- sufficient data to identify the holder and the transaction (such as a reference code or number), and
- where practicable, the type and general location of any institutional equipment used to make the transaction (e.g. ATM – George Street).

See clause 5.2 and 5.4

In the case of a payment to a merchant for goods or services, *either*:

- the name of the merchant to whom payment was made, *or*
- a merchant reference number (where the merchant also gives the user an invoice that includes the merchant's name and reference number)

must also be recorded.

See clause 5.5

If practicable, a receipt should also indicate the remaining balance of the account which has been debited or credited. However, this information should only be provided if it is not likely to compromise the privacy or security of the user or the account holder.

See clause 5.6

FOR EXAMPLE	Privacy or security concerns would generally preclude providing balance information as part of an EFTPOS transaction. However, similar concerns would not generally arise for transactions conducted at an ATM.

7.1.2. Transactions conducted by telephone

Although it is not possible to issue a paper receipt at the time of a telephone banking transaction, the Code requires that certain information be provided orally to a user.

Where a transaction is conducted by telephone, your institution must take reasonable steps to offer users the following information:

- a receipt number,
- the amount of the transaction,
- the type of transaction – for example "deposit", "withdrawal", "transfer, and
- an indication of the account(s) being debited or credited

See clause 5.7

7.2. Prohibited content for receipts

Under the Code, a transaction receipt must not include information that would increase the risk of unauthorised transactions, such as:

- the holder's full account number,
- a full credit card number or card expiry date,
- name or address of the account holder.

See clause 5.3

7.3. When must the receipt be provided

Unless an exemption applies, a transaction receipt must be provided at the time of each individual transaction.

See clause 5.1

7.3.1. Exception – User declines receipt

Your institution is only required to offer users a receipt. As such, it is not required to provide a receipt when a user specifically elects not to receive one.

See clause 5.1

Institutions generally provide users with the option to specify, at the time of each transaction, whether or not a receipt is required (e.g. at an ATM).

7.3.2. Exception - Periodic payments

ASIC has advised that, while your institution must provide a receipt each time a customer uses electronic equipment to set up a new periodic payment, it is not necessary to provide a receipt for each automatic periodic payment itself.

7.3.3. Exception – No direct connection with transaction

Your institution is not obliged to provide a receipt for a transaction with which it does not have a direct connection. That is:

- the transaction is not conducted through systems or equipment belonging to your institution, or

- there is no direct communication between the user and your institution (or a person acting on its behalf).

However, the Code does require that your institution use its best efforts to ensure a receipt is provided.

See clause 5.10

FOR EXAMPLE	A user makes a credit card payment over the internet via a retailer's website. Your institution is not required to provide a receipt for this transaction, but must use its best endeavours (e.g. through the retailer's acquiring institution or the card association) to see that the retailer provides a receipt.

7.4. Electronic receipts

Your institution may provide a receipt by making it available to the user via an electronic communication channel.

FOR EXAMPLE	Where a user performs a transaction through your institution's internet banking website, your institution may provide a receipt to the user electronically immediately on completion of the transaction.

The receipt must be provided in a manner and format that meets the general requirements for electronic communications.

See also: For more information on the electronic communication requirements refer to Chapter 10.

8. Notice of ATM Fees

Under the Code a subscriber that is an ATM provider must disclose the amount of any fee or charge it imposes for using its ATM. This disclosure must be provided to a user, whether or not they are a customer of the ATM provider.

See clause 6.1

8.1. Disclosure requirements

Disclosure must be provided at a time which allows the user to cancel the ATM transaction without cost (i.e. before the user completes the transaction).

See clause 6.2 and 6.3

8.2. Agreements with suppliers

Your institution must ensure that any agreement it enters into with another ATM provider contains the following:

- the ATM provider will disclose the amount of any fee charged for using its ATM which will be directly passed on to a user who is not a customer of the ATM provider,
- the information will be disclosed before the user completes the transaction, and
- after receiving the information, the user will be able to cancel the transaction at no cost.

See clause 6.4

9. Account statements

The ePayments Code requires your institution to provide account holders with periodic account statements in respect of accounts to or from which electronic transactions can be made.

Some exceptions apply.

See clause 7.1

9.1. Frequency of statements

The Code requires that an account statement be provided at least every 6 months.

See clause 7.1

However, account holders are entitled to request more frequent statements. The ability to make such a request must be notified to an account holder prior to, or at the time, they uses their facility for the first time.

See clause 7.2

9.1.1. Statements on request

The Code permits an account holder to request an account statement on demand.

See clause 7.3

A statement issued on request must include as much as possible of the information required for an account statement (see ¶9.3 below).

See clause 7.4

There is nothing to prevent your institution from charging a fee for providing additional account statements on demand. However, such a fee must have been properly disclosed to the customer, and it must be reasonable having regard to the cost of generating the statement (i.e. fees associated with producing additional statements must not be structured to avoid the obligation to provide such statements.)

9.2. Exceptions

9.2.1. Passbook accounts

Your institution is not required to provide an account statement for a passbook account. This exception only applies where:

- the account holder is able to:
  - have their passbook updated manually, or
  - check their account balances and activity electronically, and
- your institution imposes no charge for doing so.

See clause 7.1(a)

9.2.2. No transactions during statement period

Your institution is not required to provide an account statement for a facility:

- that has a zero balance, and
- on which no transactions were made during the statement period.

See clause 7.1(b)

9.3. Content of account statements

The Code requires account statements to include the following information:

9.3.1. Transaction details

For each transaction that has occurred since the previous statement, the statement must include:

- the amount of the transaction,
- the date the transaction was debited or credited to the account,
- the type of transaction, and
- the receipt number, or other means, which will enable the account entry to be reconciled with a transaction receipt.

See clause 7.4 (a) – (d)

9.3.2. Fees and charges

The statement must set out any charges imposed for performing a transaction regulated under the Code. These charges must be listed separately from other charges.

See clause 7.4(e)

Where practicable the statement should include the amount of each fee or charge imposed for a transaction using an ATM provided by a different ATM provider.

See clause 7.5

The format of statement disclosure will necessarily vary according to the fee structure of the account. An example of a possible disclosure format is as follows:

Transaction Type	No. of transactions	Free	Transactions charged for	Cost per transaction	Total charged
Own bank ATM withdrawal/inquiry	4	2	2	65c	$1.30
Other bank ATM withdrawal/inquiry	1	1	0	$1.50	$0.00
EFTPOS withdrawal	4	0	4	50c	$2.00

See also: For further information about good practice in relation to fees and charges disclosure on account statements, refer to ASIC Regulatory Guide 40.

9.3.3. Contact details

The statement must include the address, telephone number or other contact details that an account holder should use to make inquiries concerning their account, or to report any errors in the account statement.

See clause 7.4(f)

9.3.4. Statement warning

An account statement should include a notice suggesting that all entries on the statement be checked by the account holder and that any apparent error or possible unauthorised transaction should be promptly reported to your institution.

See clause 7.4(g)

FOR EXAMPLE	"You should check all entries on this statement immediately. Any apparent error or possible unauthorised transaction should promptly be reported to our Security Hotline - 1800 111111."

9.3.5. Security guidelines

At least once a year, your institution must include on or with its account statements a clear, prominent and self-contained notice that summarises pass code security guidelines.

These guidelines must be consistent with the terms of the Code. This means that they must:

- differentiate the recommended practices from the practices which are required under the Code, and
- advise that an account holder's liability for unauthorised transactions will be determined in accordance with the requirements of the Code rather than your institution's guidelines.

See clauses 8.1, 12 and 13.2

9.4. Other laws

Other laws contain requirements for material to be included in statements, as well as the frequency and method of delivery. When issuing account statements your institution must ensure all relevant laws are complied with, such as:

- the National Consumer Credit Protection Act and National Credit Code
- the Corporations Act
- Industry Codes of Practice such as the Customer Owned Banking Code of Practice and the Banking Code of Practice.

Note that interchange agreements, card schemes and similar arrangements may also have their own requirements.

10. Electronic communication of information

The Code allows your institution to give account users any information required to be given under the Code electronically, subject to certain conditions being met.

See clause 21, Electronic Communication

Information required to be given under the Code includes – terms and conditions, information about changes to terms and conditions, receipts, account statements, and mandatory consumer warnings.

See Part B: Disclosure Obligations

10.1. Relation to ASIC guidance on facilitating digital disclosure

On 29 March 2016, the Code was amended to align Clause 21, Electronic Communication, with ASIC's approach to the electronic provision of mandatory disclosures under Chapter 7 – Financial Services, Corporations Act. This approach, revised in July 2015, is set out in in Regulatory Guide 221, *Facilitating digital financial services disclosures (July 2016)*.

See ASIC 16-095MR ASIC facilitates easier electronic disclosure under the ePayments Code

According to ASIC, the general guidance under RG 221 is relevant to interpreting Clause 21 of the Code. As such, that guidance is referred to in this Chapter.

See ASIC RG 221.5(e) and Note, RG 221.71

See also: ¶10.7 (Obligations under other regulatory regimes).

10.2. How information may be provided electronically

Subject to the conditions referred to in ¶10.3 and ¶10.4 of this Chapter, your institution can provide information to an account user electronically under the Code by:

- Sending the information to the user by a form of electronic communication nominated by the account user, or
- Notifying the user that the information is available electronically, or
- Another manner agreed with the user.

See clause 21.1(a) – (c)

10.2.1. Sending information by a form of electronic communication nominated by user

An account user may nominate how they wish to receive information in a variety of ways, including by selecting from a tick box list on an application form.

ASIC's RG 221 guidance also indicates that a nomination may often be able to be inferred simply on the basis of contact details (e.g. email address) provided by the account user. According to ASIC:

- in most instances it will be clear from the context whether an electronic address has been nominated by the user for the purpose of receiving information from your institution;
- if a user has recently provided their email address as contact information as part of an application for a product, your institution may generally provide disclosures for that product via that email address:
  - even if the user has also provided a postal address—i.e., you do not have to use the postal address in preference
  - even if the user has not given express consent for the address to be used for the purpose of delivering or notifying disclosures
  - even if email is not the usual means of communication with the user

See ASIC RG 221.19 - 20

10.2.2. Notifying user that information is available electronically

ASIC calls this the "publish and notify" method in RG 221. The information is published electronically, and the account user is then notified that the information is available and how they can access it.

As regards the "publish and notify" method, RG 221 notes:

- On each occasion when information is published, the user must be notified that it is available.
- The user can be notified using any means the user has provided for the purposes of receiving information from your institution.
- Each notification must contain details of how to access the new information.
- Where the information being provided includes personal information (as defined under the Privacy Act), it must be adequately secured, such as by password protection.
- At the same time, the information must still be accessible and readily retrievable (e.g. passwords or user names should be able to be updated or retrieved immediately without requiring the user to contact your institution by telephone or email).
- The information must remain available at the access point notified for a reasonable period [see also ¶10.4].

See ASIC RG 221.33, RG 221.42 - 48

See also: ¶10.6 *Electronic disclosure – good practice*

As discussed at ¶10.4, before your institution can use the "publish and notify" method it must, under the Code, either:

a) obtain the account user's agreement to provide information in the manner proposed, or

b) advise the account user that it intends to make information available in a particular manner, and give them seven days to opt-out of receiving information in that manner.

See clause 21.1(f)

10.2.3. Another manner agreed with the account user

This means a separate, additional option for delivery, beyond the sending of disclosures to electronic addresses.

See ASIC RG 221.27

10.3. Electronic provision – general conditions

Under the Code, your institution may only provide information electronically to an account user if:

- It provides an effective and convenient process for account users to update their contact details, and
- It is easy to retrieve, read and store the information, and
- A paper copy of the information is available for seven years from the time the information is given. [This requirement does not apply to facilities designed exclusively for electronic use: see ¶10.5.]

See clause 21.1(d), (e), (g)

See also: ¶10.6 *Electronic disclosure – good practice*

10.4. Additional conditions if using publish & notify method

Under the Code, your institution may only provide information by notifying the user that the information is available electronically [see ¶10.2] if, in addition to meeting the conditions referred to in ¶10.3:

- Your institution makes the information available in the manner notified (***relevant electronic manner***) for a reasonable period, AND
- EITHER:
  - the user has agreed to receive information, or information of that type, in the relevant electronic manner, OR
  - your institution has given the user at least seven days' notice that it may use the relevant electronic manner to make information available to them; and the customer has not elected, by a means reasonably specified in the notice, not to receive information in that manner.

See clause 21.1(f)

In the case of facilities designed exclusively for electronic use, see ¶10.5.

10.4.1. Making information available for a reasonable period

According to ASIC's RG 221 guidance:

- As a matter of good practice, two years is a reasonable period for continuing to make most information available, unless the information has become out of date, etc.
- If it is not possible to continue to make the disclosure available from the specified link, web address or digital facility for a two-year period, good practice would be to make it easy for the account user to request a digital copy of the information at no cost (e.g. by providing a toll-free number or electronic address or request button account users can use).

See item 5, Table2, ASIC RG 221.108

10.4.2. Customer agrees to receive information

The customer's agreement can be sought in any way—such as orally, in person or over the telephone, by using a tick box form, or by SMS. Agreement could be sought as part of the application process.

See ASIC RG 221.41

10.4.3. Customer does not elect not to receive information, having been given seven days' notice

The seven days' notice should:

- Be provided using the existing method of communication with the account user.
  - For example, if an account holder has previously received their statements through the post they should be notified *by post* that their future statements will be provided electronically (and how this will be done unless they opt out of electronic delivery).
- Clearly state that the account user can opt out of the new form of delivery (i.e. request an alternative form of delivery).
- Clearly state how the account user can do this.

See ASIC RG 221.66, 221.68

As this method allows your institution to start providing information electronically without first obtaining the customer's agreement (i.e. it does not require the customer to 'opt-in'), it is most likely to be useful when your institution wants to start using the "publish and notify" method for existing customers.

See ASIC RG 221.42

10.5. Facility designed exclusively for electronic use

If your institution provides a facility designed exclusively for electronic use, any information required to be given under the Code may be given by any of the methods referred to in ¶10.2—namely, by:

- Sending the information to the account user by a form of electronic communication nominated by the account user, or
- Notifying the account user that the information is available electronically, or
- Another manner agreed with the account user.

See clause 21.2 (a) – (c)

See also: commentary in ¶10.2 on these methods;

as long as the following conditions are met:

- Before the user performs a transaction using the facility, your institution must clearly disclose that information will be given electronically, and paper copies will not be available, and
- Before the user performs a transaction using the facility, your institution must clearly disclose how the information will be provided electronically, and
- It must be easy for users to retrieve, read and store the information [see ¶10.3 Electronic provision - general conditions], and
- Your institution must make the information available electronically for a reasonable period [see ¶10.4 Additional conditions if using publish & notify method], and
- Your institution must provide an effective and convenient process for customers to update their contact details [see ¶10.3 Electronic provision - general conditions]

See clause 21.2 (d) – (g)

10.6. Electronic disclosure – good practice

RG 221 includes Part D – *Good practice guidance for digital disclosure*, which provides good practice recommendations that are relevant to Clause 21 of the Code.

The recommendations discussed in Part D of RG 221 are, in summary:

- Disclosure documents should be easy to retrieve, view and understand
  - Includes – readily navigable, simple access process, clear access instructions (e.g. not enough to provide link to generic website), electronic address or link to beginning of the document
- Disclosures should not distract or divert customers from relevant information
- Customer should be able to identify the whole disclosure

- Institutions should use their reasonable efforts to ensure customers receive a copy of the disclosure
  - Includes – using alternative means to provide disclosure if your institution receives undeliverable email notice
- Customers should be able to keep a copy so they can access the disclosure in the future
  - Includes – inviting customers to save or print copy, ensuring information continues to be available for a "reasonable period" (2 years suitable for most disclosures)
- Customers should be able to prove which version of the disclosure they relied on
  - Includes – keeping copy of all versions for at least 7 years, or as required by law & making it clear to customers that they can request copy at no cost during this period
- Customers should be able to opt out of digital disclosure
  - Includes – giving customers a clear option of opting out of electronic disclosure at any time and at no cost - not required in case of fully electronic products [see ¶10.5]
- Disclosure documents should be delivered in a way that does not unreasonably expose customers to security risks (e.g. phishing or identity theft).
  - Includes – password protection where disclosure contains personal information, in the case of generic disclosure by email with a hyperlink to the disclosure the email should state that the customer will not be asked to provide personal financial details online (e.g. to access the disclosure)

See Table 2, ASIC RG 221.108

10.7. Obligations under other regulatory regimes

As noted at ¶10.1, the regulation of electronic communications under the Code has been aligned with requirements applying in relation to financial products and services regulated under the Corporations Act. Note, however, that other regulatory regimes remain to be similarly aligned:

10.7.1. National Credit Act

Previously, electronic communication of all information required to be provided under the National Consumer Credit Protection Act ['**NCCPA'**] (including the provision of account statements), required the written ('opt-in') consent of the consumer party.

See Part 3, regulation 10 Electronic Transactions Regulations 2000

In July 2020 the Commonwealth Attorney-General remade the Regulations under the Electronic Transactions Act 1999 ['**ETA**'] "to ensure that the

exemptions to the operation of the Act remain relevant in light of current and emerging digital channels and consumer and business preferences".

The Electronic Transactions Regulations 2020 replace the Electronic Transactions Regulations 2000.

The Electronic Transactions Regulations 2020, among other things, removes a layer of procedural prescription (including the requirement for *written consent*) which previously applied under the 2000 Regulations when a credit provider sought to send (non-exempt) notices or other documents electronically to a debtor, mortgagor, or guarantor under the NCCPA. In consequence, credit providers no longer need to comply with these requirements when giving or sending NCCPA statutory documents (including Credit Code documents) electronically unless the NCCP regime itself requires them to do so.

Although a layer of prescription has been removed from the Electronic Transactions Regulations, credit providers must still observe the procedural requirements of the ETA itself when giving or sending documents electronically. In particular, they must still obtain the intended recipient's consent [just consent, not written consent] to electronic provision, although that consent may now be "reasonably inferred". In addition, the information to be provided electronically must be sent in a form that is "readily accessible so as to be useable for subsequent reference" by the recipient. These requirements are set out in section 9 of the ETA.

This legislative change prompts the question of whether it opens the way for credit providers to use 'opt-out' rather than 'opt-in' processes in obtaining customers' consent to the provision of Credit Code documents (including account statements) electronically. In our view, in the absence of any legislative protection (such as ASIC Instrument 2015/647 which facilitates electronic delivery of financial services disclosures), proceeding on the basis that the customer's consent could be reasonably inferred would involve a level of regulatory uncertainty that many institutions would not find acceptable from a risk perspective. Further reform is needed to give lenders certainty.

For more information, see Chapter 33, Managing a Consumer Credit Contract, of GRC Solutions' National Credit Act and Code Compliance Manual suite and recent Compliance Notes from GRC Solutions.

10.7.2. Customer Owned Banking Code of Practice [COBCOP]

COBCOP allows electronic communication about products and facilities unless another law prohibits it. This can be done:

- by sending the information using a form of electronic communication nominated by the customer,
- by notifying the customer that the information has been made available electronically (e.g. on a website) and how the customer may retrieve the information, or
- in another manner agreed with the customer.

When communicating with customers electronically, COBCOP also requires its subscribers to ensure that:

- The customer can readily access, read, print and store the information,
- The information is available for a reasonable period, if it is required to be retrieved, and
- There is an effective and convenient process if the customer needs to update their electronic address.

When communicating with customers electronically, COBCOB subscribers need to adopt practices that take appropriate account of online security risks and that are consistent with ASIC regulatory guidance on online disclosure.

See clause D18, COBCoP

10.7.3. Banking Code of Practice

The Banking Code of Practice allows communications with customers to be made electronically, subject to other laws.

See clauses 18-20, Banking Code of Practice

Part C –Liability: General

11. Overview of liability regime

Chapter C - Liability of the Code sets out a comprehensive regime for determining, as between your institution and the account holder, who is liable for unauthorised transactions. This regime overrides any terms and conditions your institution may impose in relation to its account facilities[6]. In other words, liability must always be determined in accordance with the Code in the event of inconsistency.

11.1. Regime only applies to unauthorised transactions

The Code's liability regime only applies to transactions that are unauthorised. This means it does not protect account holders in circumstances where a transaction has been carried out with the knowledge and consent of the account holder or any authorised user.

See clause 9.1

FOR EXAMPLE	An account holder may query a transaction on their account which they are unaware of. However, if this transaction was carried out by an authorised user (albeit without the account holder's specific knowledge or consent) it will not be an unauthorised transaction.

11.2. Allocation of loss

The Code's liability regime is very specific about the circumstances and extent to which loss may be allocated to an account holder. The liability allocation provisions can be broadly summarised into three categories.

11.2.1. Situations in which account holder cannot be made liable

Under the Code, an account holder can never be made liable in circumstances where it is clear that they have not contributed to the loss that occurred. These include (but are not limited to) situations where:

- the loss occurred as the result of fraudulent conduct by your institution's employees,
- the loss occurred before the access method was received by the user,
- the loss occurred after your institution was notified of the loss or breach of security of the access method.

See also: The situations in which an account holder can have no liability for losses under the Code are considered further in Chapter 12.

11.2.2. Situations in which account holder can be made liable

Liability may be allocated to an account holder where your institution can prove, on the balance of probability, that a user has breached certain

[6] Section 4.2 of the Code prohibits subscribers from having terms and conditions that create liabilities and responsibilities that exceed those set out in the Code. Such terms and conditions also arguably constitute misleading and deceptive conduct in breach of sections 12DA and 12DB of the ASIC Act 2001.

requirements of the Code leading to an unauthorised transaction loss occurring. These requirements cover situations where:

- the user has wilfully or carelessly disclosed their access code in one or more of the ways prescribed in the Code, or
- the user has unreasonably delayed notifying your institution of either the loss of their access device or a breach of the security of their access code.

In order to make the account holder liable, your institution must be able to prove both that the account user has acted in one of the prescribed ways, and that this has contributed to the loss which resulted.

See also: The circumstances giving rise to account holder liability for losses are considered in Chapter 13.

11.2.3. Situations where account holder can be made liable for a limited amount

Quite frequently it will not be possible to determine whether or not the user contributed to the loss in breach of a Code requirement or not. In such situations, your institution may apply the so-called 'no-fault' provisions of the Code's liability regime.

Put simply, the no-fault provisions allow a generally small portion of the loss ($150 maximum) to be allocated to the account holder without the institution having to prove the account holder or an authorised user acted in breach of the Code. The remainder of the loss must be absorbed by the institution in these circumstances.

See also: The no-fault liability provisions and situations in which they may be applied are considered in further in Chapter 14.

11.3. General principles for determining liability

Decisions regarding liability must be made on the basis of established facts and not on the basis of inferences unsupported by evidence.

All reasonable explanations for the fact that the disputed transaction(s) occurred should be considered. For each explanation, an assessment as to the degree of likelihood of each explanation in light of the established facts should be made.

See clause 11.8(a)

11.3.1. Balance of probability

The Code requires your institution to prove an account holder's liability on the balance of probability. In order for something to be proven on the balance of probability it must be shown to be more probable than not. In most cases there will always be a measure of doubt as to whether a user has contributed to their loss, particularly in circumstances where a code has been used to make an unauthorised transaction.

See clause 11.2

However, suspicious circumstances alone are not a sufficient basis for allocating liability to an account holder. Rather, your institution must be able to *show* that it is more likely than not that:

- a user acted in a way which allows liability to be imposed under the Code, and
- that action contributed to the unauthorised transaction resulting in a loss occurring.

11.3.2. Causal connection

Before an account holder can be held liable, your institution must show a causal connection between the user's actions and the consequent loss that occurred.

CASE EXAMPLE	In a case considered by the Financial Ombudsman Service (FOS), AFCA's predecessor, an account holder reported a number of unauthorised ATM and EFTPOS transactions made in New Zealand with a lost debit card. The account holder acknowledged disclosing her PIN number to her husband. However, she also provided evidence to show that neither she, nor her husband had been in New Zealand at the time of the transactions. While the financial institution suspected that the transactions were made by someone known to the account holder (or her husband) they were not able to prove this on the balance of probability. The FOS therefore formed the view that the account holder could not be held liable for the losses on the basis that she had disclosed her PIN as this had no verifiable connection with the unauthorised transactions.

11.4. Loss caused by third party

Your institution cannot avoid liability simply because the loss in question has been caused by the failure of another party to the EFT (electronic funds transfer) system, such as: a retailer or other merchant, a communications service provider, or another account institution.

See clause 15.2

This means that where your institution's account holder has not contributed to the loss, your institution must reimburse the account holder. It is then up to your institution to take appropriate action to recover the amount from the party that is ultimately responsible for the loss.

FOR EXAMPLE	Your institution cannot seek to avoid liability simply because a loss arose due to an equipment malfunction at another institution's ATM. Your institution must repay the account holder the lost amount and then take the appropriate action to recover this amount from the other institution.

12. Situations in which an account holder cannot be made liable

This Chapter considers the various situations where an account holder may not be made liable in part or whole for an unauthorised transaction loss under the Code.

12.1. Where account holder/user is clearly not at fault

There is an overriding principle under the Code (which in turn reflects general law principles) that an account holder cannot be made liable for any loss where it is clear that the account holder or other authorised user did not contribute to the loss.

See clause 10.3

12.2. System or equipment malfunction

An account holder has no liability for losses that are caused by a system or equipment malfunction.

See clause 14.1

Your institution will be responsible for any losses (including consequential damages) that an account holder or authorised user suffers as a result of the failure by your institution's system or equipment to complete a transaction in accordance with their instructions.

See clause 14.2

However, where the user should have been aware that the system or equipment was unavailable or malfunctioning, your institution's liability may be limited to the correction of any errors and the refund of any charges or fees imposed.

See clause 14.3

12.3. Fraudulent or negligent conduct of employees or agents

An account holder has no liability where the loss has been caused by the fraudulent or negligent conduct of your institution's employees or agents.

See clause 10.1(a)

An account holder will also have no liability for losses which are caused by the fraudulent or negligent conduct of:

- other companies involved in networking arrangements,
- merchants who are linked into the EFT system, or
- the agents or employees of merchants.

See clause 10.1(a)

12.4. Forged, faulty, expired or cancelled access method

An account holder has no liability for losses related to an unauthorised transaction effected by means of a device, identifier or pass code which is forged, faulty, expired or cancelled.

See clause 10.1(b)

12.5. Losses occurring prior to receipt of access method

An account holder has no liability for losses that arise from transactions that occur before the holder (or an authorised user) receives any device or pass code required to make electronic transactions (including any reissued device or pass code).

See clause 10.1(c)

FOR EXAMPLE	Your institution sends a new EFTPOS card to an account holder in the mail. A number of unauthorised transactions are made using the card, which the account holder claims never to have received. The account holder will not be liable for these losses (unless your institution can prove on the balance of probability they did in fact receive the card prior to the date of the transactions in question).

In any dispute concerning the receipt of a device or pass code, the Code presumes that the item in question was not received. Essentially, this means that your institution cannot simply rely on the fact that the device or pass code was delivered to the person's correct address.

See clause 10.4

12.5.1. Obtaining acknowledgement of receipt

In order to rebut the above-mentioned presumption, it is recommended that your institution obtain a person's confirmation of receipt. A device or pass code will be deemed to have been received by a user if they provide acknowledgement of receipt. Accordingly, your institution should require users to provide some form of receipt acknowledgement for each device and pass code it sends.

FOR EXAMPLE	In the case of a payment card that uses a PIN, your institution could do the following: • if the card and the PIN are to be sent in the mail, ask the applicant to complete and return an acknowledgment advice confirming that both the card and PIN have been received, or • if the card and the PIN are to be collected in person, ask the applicant to complete an acknowledgment advice confirming that both the card and PIN have been received.

12.5.2. Prohibition of deemed receipt

Your institution is prohibited from including a term in its terms and conditions documents which deems a device or passes code sent to a user's correct address as having been received by that user.

See clause 10.5

12.6. Incorrect double debit transactions

An account holder has no liability for losses caused by the same transaction being incorrectly debited to their account more than once.

See clause 10.1(d)

12.7. Transactions occurring after notification of problem

An account holder has no liability for unauthorised transactions that occur after your institution has been notified that:

- a device has been misused, lost or stolen, or
- the security of a pass code has been breached.

See clause 10.1(e)

12.8. Transactions made using an identifier

An account holder has no liability for losses arising from an unauthorised transaction made using an identifier only.

Where a transaction is made using a device and an identifier (but does not require a pass code) the account holder is liable only if a user unreasonably delays reporting the loss or theft of the device.

See clause 10.2

This provision is also applicable to transactions such as:

- online shopping and other card-not-present transactions; and
- contactless card (MasterCard PayPass or Visa payWave) transactions where the transaction is authorised simply by passing the user's card incorporating radio frequency [RF] technology close to an RF-equipped reader, with no PIN or other access code being required

For further information about these types of transactions refer to Chapters 20 and 21.

13. Situations in which an account holder can be made liable

This Chapter looks at the acts/inaction of account holders and users which trigger your institution's right to make the account holder liable under the Code.

13.1. Liability only in situations specified in Code

Under the Code, an account holder may be held liable for unauthorised transactions occurring as a result of the specific types of careless or wilful conduct on the part of the account holder, or an authorised account user, as discussed in the following sections of this Chapter.

Only limited specified acts/ inaction by the account holder/user give Code subscribers the right to make the account holder liable. In other words, even if the account holder or user was at fault in some other way, unless one of the specific types of act/inaction set out in the Code and summarised in this Chapter applies, the account holder may not be made liable for the resulting loss, which your institution will be required to absorb.

See clause 11.1

13.2. Fraudulent activity

An account holder will be liable for losses that arise due to fraudulent activity conducted or participated in by the account holder or an authorised user.

See clause 11.2

13.3. Voluntary disclosure of code

The Code provides that an account holder may be liable for their loss if they or an authorised user voluntarily disclose their access code to anyone else, including a family member or a friend.

See clause 11.2 and 12.2(a)

CASE EXAMPLE	Mr P gave his debit card to one of his daughters, Ms B, so that she could withdraw cash at an ATM for him. Ms B was accompanied on this occasion by Mr S, who observed the PIN being entered by Ms B. Mr S stole Mr P's card and used it to make a number of unauthorised transactions. The FOS held that Mr P was liable for his losses as there was sufficient linkage between his voluntary disclosure of his PIN to Ms B and the fact that Mr Shad gained knowledge of the PIN to make transactions.

In order for an account holder to be held liable there has to be an intention to disclose the code to another person. There are a number of situations where disclosure will not be deemed to be voluntary. These are outlined below.

13.3.1. Disclosure under duress

A user will not be taken to have voluntarily disclosed their access code if they have been coerced into giving this information by force, duress, intimidation or threat.

FOR EXAMPLE	A person has not voluntarily disclosed their access code if they have been threatened with violence at an ATM if they do not hand over their debit card and disclose their PIN.

13.3.2. Mistaken disclosure

A user will not be taken to have voluntarily disclosed their access code if they have mistakenly provided it to a person they reasonably thought they were authorised or required to disclose it to.

FOR EXAMPLE	A person has not voluntarily disclosed their code if they are contacted by a person pretending to be from your institution who asks for their access code in order to authorise a pending transaction or check for unauthorised activity on their account.

Whether a person's belief that disclosure was permitted was reasonable will be influenced by the educational activities your institution has undertaken in relation to code security. In this respect, your institution should consider providing customers with periodic reminders about the importance of not disclosing their codes to anyone, including staff from your institution.

See FOS Policies and Procedures Manual

13.3.3. Unknown disclosure

A user will not be taken to have voluntarily disclosed their access code if, when using the code, it is unknowingly seen a bystander. This is so even if the user has failed to take steps to protect the secrecy of its use.

For example, a person enters their PIN number at an ATM in order to make a withdrawal. They will not be taken to have disclosed their code simply because they failed to take steps to protect the secrecy of their PIN (such as by covering it with their hand) and it was subsequently observed by the person standing behind them. This is sometimes called "shouldering".

CASE EXAMPLE	FOS, AFCA's predecessor, decided a dispute about "shouldering" at a night club in the applicant's favour and ordered his missing funds be reimbursed. The applicant reported four unauthorised transactions after visiting a nightclub when he was overseas. The applicant had a Visa card and an account with the FSP (financial services provider), as well as a second Visa card (Card A) with another FSP. In July 2016, he said he went to the nightclub with about six other people and made only two low-value transactions, using Card A. He did not authorise

	any transactions using the first Visa card. The applicant discovered the disputed transactions and contacted the FSP later that day to report the disputed transactions, which totalled almost $15,000. The FSP said the applicant did not comply with the terms and conditions of the account because he failed to keep the card secure. It also said that if the applicant did not intend to use the first Visa card while overseas, he should have left it at home or securely in a hotel safe. FOS found that the applicant had transferred funds from his first Visa card to Card A about one week before the nightclub visit and intended to use Card A to meet his expenses overseas. Also, it was not uncommon or unreasonable for customers to carry several cards overseas in case of an emergency. The applicant provided an email from an FSP confirming that the transactions made with Card A were authorised using a PIN. EFTPOS receipts showed that he used Card A at the venue the same night, before the disputed transactions occurred. FOS said it was possible that a third party 'shouldered' him – that is, observed him entering the correct PIN. It was reasonable for the applicant to assume that his PIN was not visible to third parties when he entered it into the EFTPOS machine. People experienced in shouldering a victim could have obtained the PIN without the applicant's knowledge, FOS found. The FSP said the applicant was liable for the disputed transactions because he used the same PIN on all his devices. FOS found, however, that it was not uncommon for people to do this so that they could recall their PIN and, by itself, did not mean the applicant acted with extreme carelessness. The applicant said the first Visa card was not lost or stolen during the night of the disputed transactions and said it must have been taken out of his wallet. FOS found that the card was probably used without the applicant's knowledge, but this was not sufficient to establish that he contributed to the loss. It was reasonable for the applicant to keep the card in his wallet and believe it was safe there. FOS determined that it was appropriate for the FSP to be liable for the full amount of the disputed transactions (together with any interest and fees associated with them) because it did not establish that the applicant breached the security requirements under the ePayments Code. See FOS Annual Review 2016-17

13.3.4. Disclosure to aggregation services, etc

There is lack of clarity in the ePayments Code about the liability of a user who voluntarily discloses their access code to a third party financial services provider. These providers include aggregation services that offer to centrally manage all financial details of the user by requiring disclosure of their code so that statements can be aggregated. Other examples include affordability verification services for various loans providers.

Arguably, the disclosure of a password/PIN to such a third party breaches the ePayments Code prohibition and makes the loan applicant liable for any unauthorised transaction losses resulting from the disclosure. However, AFCA may consider this an unacceptable outcome from a consumer perspective, given that the third party has encouraged or required the applicant to provide their code as part of its services.

The risk for the institution that subscribes to the ePayments Code is that if the source of a compromise cannot be identified, it may be forced to bear the loss.

ASIC is aware of the issue and will consider the matter at the time the next update to the ePayments Code is undertaken. In the meantime, institutions that subscribe to the ePayments Code should consider addressing this matter in their Terms and Conditions. In addition, customer communications could periodically remind users not to disclose codes to a third party such as an aggregation service. Such action may help the subscribing institution if a dispute is taken to AFCA.

The Consumer Data Right in Open Banking goes some way to address this problem by allowing a customer to direct their institution to give personal information to a third party without needing to disclose their password/PIN. See the GRC Solutions Australian Privacy Principles Compliance Manual for more information about Open Banking.

13.4. Keeping a record of code

The Code does not prohibit an account holder or authorised user making a record of the code linked to their device. However, an account holder may be liable for unauthorised transactions if they fail to make a reasonable attempt to protect the security of a code record.

See clause 11.2 and 12.2

Making a reasonable attempt to protect the security of a code record includes:

- a reasonable attempt to disguise the code within the record, and/or
- reasonable steps to prevent unauthorised access to the code record.

See clause 12.3

The requirement to make a reasonable attempt to protect the security of a code record applies to both records of codes that are used in conjunction with a device (such as a PIN) as well as standalone codes (such as an internet banking password).

13.4.1. Reasonable attempts to disguise a code

Previously FOS developed guidance around what it considered to be a reasonable attempt to disguise a code. Since AFCA has not provided new guidance on this matter and the FOS guidance appears to be still relevant, we summarise below the FOS guidance.

Attempts that the FOS considered reasonable include:

- concealing the code's identity within the record by altering the code, such as by:
  - re-arranging the order of the numerals or letters, or
  - substituting other numerals, letters or symbols.
- concealing the code's identity within the record without altering the code:
  - making it appear as another type of word or number, or
  - surrounding the code with other numerals, letters or symbols.
- hiding or disguising the code record among other records or in places where a code record would not be expected to be found, such as in a cook book.

On the other hand, attempts that the FOS considered unreasonable include:

- recording the code as a series of numbers with any of them marked or circles or highlighted which would indicate them as a code,
- recording the code with surrounding information that makes it stand out from its context, such as a 4-digit telephone number in a list of 8-digit phone numbers,
- recording the code as a birth date, postcode or first or last part of a telephone number without additional features of disguise.

The reasonableness of a disguise attempt should be assessed from the point of view of the reasonable user. This may include consideration of any directions your institution has widely publicised or otherwise provided to the person about unreasonable forms of disguise.

The fact that a code disguise failed to prevent unauthorised transactions does not make a person's attempt to disguise a code unreasonable.

See FOS Bulletin No. 37 (March 2003)

FOS COMMENT: "REASONABLE DISGUISE"	*"In the recent experience of Financial Ombudsman Service, many cardholders attempt to 'disguise' their PIN by writing it down as the last or first four digits of an 8-digit phone number. As the PIN is usually in its correct sequence, we do not usually consider that such a 'disguise' is reasonable. In some circumstances we might accept that the attempt to disguise was reasonable if the phone number was buried among a long list of names, addresses and phone numbers. But even here, a cardholder can negate their attempt to disguise if they list the disguised PIN under a name that draws attention to the likelihood of a PIN record being present. As an example, we have seen a recent dispute about a card branded with the name of a prominent retailer where the 'disguised' PIN was part of a phone number listed in an address book under the same name as the retailer. We could not accept that this was a reasonable attempt to disguise the PIN record or to prevent unauthorised access to the PIN record."* FOS Banking & Finance Bulletin 59, p.6 (September 2008)

13.4.2. Reasonable attempts to prevent unauthorised access

The Code provides that reasonable steps to prevent unauthorised access may involve:

- hiding the record among other records,
- hiding the record in places where a code record would not be expected to be found,
- keeping a record of the code in a securely locked container, or
- preventing unauthorised access to an electronically stored record of the code.

See clause 12.3

The FOS has observed that a code record contained in an address book, diary personal organiser carried along with a device in a handbag, backpack, etc does not constitute a place where a record would not be expected to be found. Similarly, codes for internet or telephone banking kept in a folder with other banking records would not be an unexpected place. However, consideration should still be given as to whether the code record was reasonably disguised or hidden amongst the other records.

An electronic record could be stored in a program on a personal computer, hand-held organiser or mobile phone. In considering whether reasonable steps have been taken to prevent unauthorised access to an electronic record, the FOS has noted the following should be considered:

- whether the information was freely available by mere possession of the equipment,
- whether the electronic equipment required a password to gain access and if so whether password access was turned on,

- whether the information was stored under an immediately recognisable menu item, such as "bank passwords" or "access codes".

See FOS Bulletin No. 37 (March 2003)

13.4.3. Record kept with access device

Where a code is used in conjunction with a device an account holder will be liable for loss if they or an authorised user keep an unprotected record of their code either:

- on the outside of the relevant access device, or
- on an article that is liable to loss or theft simultaneously with the device.

See clause 12.2(b)

The FOS has stated that a simultaneous loss or theft of a code record and a device occurs when they are kept:

- in the same receptacle that itself can be lost or stolen, such as a wallet, handbag, briefcase or suitcase,
- in the same location within the same room (for example on the same desktop or tabletop, or in the same drawer or box) so that the device and code record can be seen together and taken in the same instance,
- in the same vehicle, even if they are located in different compartments of that vehicle (such as where the device in the centre console and the record in the glove box).

See FOS Policies and Procedures Manual

An account holder will only be liable if your institution can prove that a user knowingly (or recklessly) kept a record of their code on or with an article that was liable to simultaneous loss as their access device.

CASE EXAMPLE	Mr G has a debit card with a system-generated PIN. Mr G's house was broken into and among other items his debit card stolen. A number of unauthorised ATM withdrawals were subsequently made with the correct PIN being used on the first attempt. Although Mr G denied keeping a record of the PIN, the FOS accepted that in the circumstances it was likely that knowledge of the PIN could only have been gained from a record of the PIN. However, as it appeared every room in the house had been entered during the burglary, there was insufficient information to state on the balance of probability that this record had been kept on an article that was liable to loss with the debit card.

13.4.4. Use of a single pass code for multiple accounts

As account holders typically have multiple accounts or facilities, many will use the same PIN or other pass code to protect/access multiple accounts. Doing so does not breach any Code requirement. The FOS previously expressed the following view of this practice:

FOS COMMENT:	*While having the same self-selected PIN for multiple cards is not a perfect solution to PIN security, as long as that PIN is not voluntarily disclosed to anyone the Financial Ombudsman Service considers that it is a preferable strategy to keeping written records of a multiplicity of PINs. Ideally, the self-selected PIN should be constructed in such a way that the cardholder never needs to make a record of it.* See FOS Banking & Finance Bulletin 59, p. 6 (September 2008)

13.5. Extreme carelessness in protecting codes

The Code provides that an account holder may be liable if they act with extreme carelessness in failing to protect the security of their access codes.

The concept of "extreme carelessness" involves subjective judgements. The Code attempts to explain it as meaning a degree of carelessness with the security of the codes, which greatly exceeds what would normally be considered careless behaviour.

See clause 12.4

FOR EXAMPLE **FOS COMMENT:**	Storing the user's username and password for Internet banking in a diary or personal organiser or computer (not locked with a PIN) under the heading "Internet Banking Codes". The Financial Ombudsman has stated that it has only ever used 'extreme carelessness' as a reason for allocating liability to an account holder "*in circumstances that closely equate*" to the above circumstances; noting that "*it is difficult to envisage circumstances where 'extreme carelessness' might be relevant to the allocation of liability for a PIN-authorised card transaction because the [Code] already has provisions about disclosure, keeping a record of, and self-selection of a PIN*". See FOS Banking & Finance Bulletin 59, p. 6 (September 2008)

CASE EXAMPLE	Mr Swed was careful to ensure that his wife did not see his PIN because he knew she had a gambling problem. When money was taken from his bank account by his wife, the bank tried to show that Mr Swed had exercised "extreme carelessness" in his attempts to protect the PIN.

	However, Judge Davies found that Mr Swed had not acted with "extreme carelessness": *In relation to his PIN Mr Swed gave evidence that if he used the ATM when Mrs Swed was with him he made her stand a metre or a metre and a half away so that she would not be able to see what he entered on the key pad. Mrs Swed's evidence was that she was able to look around him to the side and see the number he entered…* *All the evidence suggests that Mr Swed did what he could to keep both his password and his PIN secret from Mrs Swed in particular. There is no other evidence of how Mrs Swed could have obtained his PIN. Her evidence of how she managed to see it is not so fanciful that it cannot be believed. It is possible for persons to observe the entry of a PIN because of where the keypad is located. Mrs Swed is a clever woman and one who appears to have perfected deception in various guises to feed her gambling habit. I consider that her evidence of how she came to know Mr Swed's PIN should be accepted.* *I do not consider, however, that this conclusion means that Mr Swed acted with extreme carelessness in relation to the entry of his PIN. Both his evidence and that of Mrs Swed was that he did what he could to prevent her being able to see what he was doing at the ATM. If he did not realise that she was closer than he thought, that cannot be characterised as extreme carelessness.* See National Australia Bank Ltd v Swed (No.2) [2015] NSWSC 1322

13.6. Selection of prohibited code

The Code allows your institution to prohibit a user from selecting one of the following pass codes:

- a numeric code which represents the user's birth date, or
- an alphabetical code which is a recognisable part of the user's name.

In the event that a user selects a prohibited pass code, the account holder may be held liable for any losses that arise due to a breach of the code's security.

See clauses 11.2 and 12.5

Note that the selection of the name or date of birth of another person, such as a spouse/partner, parent or child, does not contravene the Code.

13.6.1. Need for warning

An account holder will only be liable if, immediately before selection of the code, your institution:

- specifically instructed them not to select a prohibited code, and
- warned them of the consequences of such a selection.

See clauses 12.5 and 12.6(a)

The onus is on your institution to prove that it gave the required instruction and warning at the time of selecting a code. Such proof might be in the form of a signed acknowledgement by the user.

See clauses 12.6(a) & 12.7

The warning must be designed to focus the user's attention on the instruction and the consequences of breaching the warning.

See clause 12.6(b)

Your institution must consider the user's capacity to understand the warning and ensure it is provided in a way they are likely to understand. This includes taking into account the user's level of literacy and understanding of English.

See clause 12.6(c)

13.6.2. FOS's views on warning requirement

FOSconsidered that:

- a provision about self-selection in a terms and conditions document does not in itself constitute a sufficient instruction given immediately before selection.
- where selection of the code is done in branch in the presence of a staff member, the instruction and warning should be given orally,
- where selection of a code is done through an ATM, computer, telephone or other electronic terminal, a prominent instruction and warning should appear on screen at the point of selection.

See FOS Bulletin No. 37 (March 2003)

13.6.3. Restriction on other codes not permitted

Your institution can ask or encourage users not to select other easily-guessed codes, such as a part of their telephone number, driver's licence, etc. However, it cannot make the account holder liable if a user does select one of these codes. To do so would be to impose liability in circumstances which the Code does not recognise, and this would breach clause 4.2(b) of the Code (see Chapter 5).

13.7. Delay in notification

The Code provides that an account holder may be liable for unauthorised transactions where it appears that a user has unreasonably delayed notifying your institution that:

- their access device has been misused, lost or stolen, or
- the security of their access code has been breached.

See clause 11.5

13.7.1. Lost or stolen device

An account holder's liability when an access device is lost or stolen commences from the time that the user "should reasonably have become aware" that the device was lost or stolen.

See clause 11.5(a)

The time at which a user should have become aware that a device has been lost or stolen arises when a reasonable user would have checked on the presence of the device. This may arise:

- in the course of the user's actual pattern of card use, or
- when something has occurred which should put the user on notice to check that the card is still in their possession - for example a reasonable user would be expected to check on the location of their device where:
  - there has been a burglary in their home,
  - there is evidence that their home office has been rifled, or
  - there has been an attempted pick-pocketing.

The test of when a user should have checked the whereabouts of their device is subjective. It does not impose an obligation on users to regularly check their device. Instead it will depend on their regular pattern of usage.

It is not unreasonable for a user to take some time to ensure that the card has not been misplaced or to search for the card if it cannot be initially located. It is also not unreasonable for a user to take time to notify the police or some other security officer before notifying your institution.

The FOS has noted that the extent of delay that is reasonable will depend on factors such as:

- whether the user has grounds for doubting the card had been lost or stolen as opposed to simply being misplaced,
- how long the delay was – e.g. 5 minutes, 3 hours, a day.

See FOS Bulletin No. 37 (March 2003)

CASE EXAMPLE	After receiving his account statement on 27 November, Mr T reported a number of unauthorised transactions on his account. The transactions in question took place on 15 – 17 November. He stated that he had lost his wallet (in which his credit card was stored) on the 15th November, although up until the time he received his statement he believed he had simply misplaced the wallet somewhere in his home. FOS was of the view that Mr T was obligated to conduct a reasonable search for his wallet when he realised it was missing rather than just assume it was somewhere in his house. This would have revealed his wallet and credit

	card were lost. He should therefore have reasonably become aware his credit card was missing on 15 November and was liable for all transactions which occurred after this date.

13.7.2. Misused device/breach of code security

An account holder's liability when there has been a misuse of their access device or a breach of the security of an access code commences from the time they become aware that this has occurred.

See clause 11.5(a)

For a user to be regarded as having become aware of a security compromise more than a mere doubt or suspicion is required. In most cases, a person will only become aware that someone else has misused their access device or gained knowledge of their code when they review a copy of their account statement and notice one or more unauthorised transactions or that their balance is significantly less than expected.

Note, however, that the mere fact an account statement has been sent to the account holder does not in itself establish that the account holder has become aware of an unauthorised transaction that may be apparent from the statement. For instance, it is possible that they may not review their statement until sometime after it has been sent by your institution.

CASE EXAMPLE	Mr M's card was used to make unauthorised transactions between 10:58pm on 13 March and 8:55am on 14 March, as well as between 6:13pm and 7:24pm on 14 March. The card was not lost or stolen and there was no information to identify the person who used the card or how they got knowledge of the PIN. In a statement Mr M noted that he became aware of the misuse of his card about 10:30am on 14 March - after he went online to transfer funds by internet banking. However, he did not report the transactions to his financial institution until 7:34pm on 14 March. FOS found that as there was 6 hours delay between when Mr M had become aware of the unauthorised transactions and when he reported them, he had unreasonably delayed notification. He was therefore liable for the transactions which occurred during the delay period.

13.7.3. Effect of charges

In determining whether a user has unreasonably delayed notification, the effect of any charges your institution imposes for services such as providing notification or replacing a lost device will be taken into account.

See clause 11.6

The extent of the cost imposed, as well as the general state of the user's finances, will need to be considered in determining whether the delay that occurred was reasonable in the user's particular circumstances.

FOR EXAMPLE	It would not be unreasonable for a user to delay reporting the loss of their ATM card while they attempted to look for it in order to try to avoid unnecessarily incurring a significant cost their financial institution imposed for providing a replacement card.

13.7.4. Interaction with chargeback rights

FOS has provided the following guidance on the interaction of the Code requirements and account institutions' chargeback rights in the context of delayed reporting of unauthorised transactions:

FOS COMMENT: INTERACTION WITH CHARGEBACK RIGHTS	*"If a cardholder did not become aware for some months that an unauthorised PIN@POS transaction had been made, for example after a family member had misused the card and returned it to the cardholder, the account holder would not be liable because of that delay for unauthorised transactions that were made before the cardholder became aware. The fact that the card-issuing account institution had lost its right to chargeback the disputed transaction to the merchant's account institution would not be relevant to the allocation of liability because the [Code] has no provision that links unreasonable delay to loss of chargeback rights. The practical outcome is that there are likely to be many circumstances where a card-issuing institution will receive a dispute about an unauthorised PIN@POS transaction that has not been lodged in time for a chargeback right to be exercised. It will be important in these circumstances that the card-issuing institution is not unduly influenced by the loss of chargeback rights when it is making a decision about the allocation of liability. Rather, the allocation of liability for unauthorised PIN@POS transactions should always be made by reference to the [Code] if the unauthorised transaction cannot be charged back."* See FOS Banking & Finance Bulletin 59, p. 6 (September 2008)

13.8. Card left in ATM

The Code provides that an account holder will be liable for losses arising from unauthorised transactions that occur because a user left a card in an active ATM.

However, this provision only applies if the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM. These include:

- ATMs that capture cards that are not removed after a reasonable time, and
- ATMs that require a user to swipe and then remove a card in order to commence a transaction.

See clause 11.4

FOR EXAMPLE	A user performs a balance enquiry, takes their balance enquiry receipt and walks away leaving their card in the ATM. The ATM remains active with an on-screen message asking whether or not the user wants to make another transaction. An unknown person approaches the machine shortly after and withdraws cash from the user's account. As there is no evidence that the ATM failed to meet reasonable standards for mitigating the risk of the user leaving their card in the ATM, the user will be liable for this withdrawal under clause 11.4. See FOS Circular Issue 9, Autumn 2012, p. 16

13.9. Liability is generally for full amount

Generally, if the account holder or authorised user acts or fails to act in one of the ways prescribed by the Code, as described in this Chapter, the account holder can be made liable for the full amount of the resulting loss suffered by your institution.

This is the case even if there were other factors that contributed to the loss for which the account holder/user was not responsible. In other words, no apportionment of liability is envisaged by the Code where the account holder or other authorised user breaches one of the liability triggers considered in this Chapter.

Note, however, that:

- the imposition of full liability is subject to daily and other periodic transaction limits, account balance limits and other restrictions
- an account holder may not be made liable under the Code for a greater amount than they would be liable for under the card scheme chargeback rules, where these are applicable.

See also: Chapter 15 - *Further limits on account holder liability* & Chapter 16 - *Transaction limits and liability* discuss these additional limits on account holder liability.

14. Situations in which account holder can be made liable for a limited amount

In certain situations, the Code allows the apportionment to the account holder of a limited amount of liability (up to $150 only) without your institution having to prove any fault on the part of an account user. The provisions which allow for this limited apportionment are sometimes referred to as the "no-fault liability regime".

See clause 11.7

The circumstances in which, and the extent to which, subscribing institutions make use of the no fault liability regime in practice vary greatly from institution to institution.

14.1. When can no fault liability be applied?

The no fault liability provisions of the Code can only be applied if the following two conditions are satisfied:

14.1.1. It is unclear how transaction occurred

The no fault provisions can only be applied when it is not clear that the account holder or authorised user *did not* contribute to the loss, but your institution cannot prove on the balance of probability that the account holder or authorised user *did* contribute to the loss.

FOR EXAMPLE	A number of allegedly unauthorised ATM withdrawals are made from a customer's account. Your institution is not able to determine the identity of the person who conducted the transactions, nor the means by which knowledge of the PIN was gained. The account holder or other authorised user may have been involved, or they may not have been. In such cases, while your institution cannot make the customer liable for the total amount lost, it does have the option of making them liable for the first $150 (assuming more than $150 was lost, and subject to applicable transaction limits: see ¶14.2 below).

14.1.2. Use of a Code

The no fault regime only applies where a pass code was required to perform the unauthorised transaction.

FOR EXAMPLE	An unauthorised purchase is made over the internet using the account holder's card number and card expiry date. As this transaction only involved the use of identifiers (i.e. no access code was required) it is not possible to apply the no-fault liability regime to the transaction.

FOR EXAMPLE	An unauthorised contactless card transaction is made (i.e. a PayPass or payWave transaction). As the transaction is authorised just by holding the account holder's card against a reader terminal with no PIN or other access code access code being used, it is not possible to apply the no-fault liability regime to the transaction.

14.2. Amount of liability

In situations where the no-fault liability requirements can be satisfied, your institution may hold an account holder liable for the lesser of the following:

- $150 (or such other lower amount as may be set by your institution),
- the balance of the account from which funds were transferred,
- the actual loss which has occurred (excluding any portion of the loss which exceeds any applicable daily transaction or other periodic transaction limit).

See clause 11.7

Online scams

There are situations where an external dispute resolution scheme will find in favour of a customer who falls victim to an online scam

CASE EXAMPLE	FOS, AFCA's predecessor, found in favour of a customer who mistakenly disclosed passcodes in a scam transaction. An applicant, Mr H, disputed liability for transactions totalling more than $5,000 after falling victim to a scam. Mr H received an email about taking part in an online cash survey using an enclosed weblink. He clicked on the link to complete the survey. He entered his credit card account information as part of the survey. By entering his number, or by clicking on the link, this information was remotely accessible on his computer. It transpired that fraudsters asked him to enter one-time PINs that the FSP (financial services provider) sent to his mobile number after he entered his credit card details. Mr H entered the one-time PINs, not realising they were secret passcodes. He thought they were required to complete the survey to win cash. The resulting transactions were to offshore merchants, from whom Mr H received no goods or services. Mr H lodged a dispute with FOS, saying that he did not authorise the transactions. Under the ePayments Code, if a customer disputes liability for an electronic payment, the FSP bears the onus of proving: • the customer authorised the transaction by performing it, or by a third party performing it with the customer's knowledge or consent, or

	• if the customer did not authorise the transaction, the customer breached certain security provisions of the Code and is liable for the transaction. In the June 2018 determination, FOS said that Mr H did not voluntarily disclose the one-time PINs, as argued by the FSP, or breach the passcode security requirements in the ePayments Code. The passcode sent to the applicant did not also say that it was to be kept a secret and not disclosed to anyone. FOS found Mr H did not know the one-time PINs were, in fact, secret passcodes and that he did not intend to disclose them and thought he was responding only to a survey. As a result, FOS found that he did not voluntarily disclose the one-time passcodes and therefore had not contributed to his loss under the ePayments Code. FOS said the FSP must compensate Mr H for his financial loss, after allowing for his limited liability of $150 under the Code. Further, the FSP must pay $250 non-financial loss for stress and inconvenience caused because the FSP sent him several text messages after the FOS dispute was lodged about his 'liability' for the transactions. See FOS Annual Review 2017/2018

15. Further limits on account holder liability

As discussed in ¶13.9, generally if an account holder can be made liable for an unauthorised transaction, they will be liable for the full amount of the loss.

See clause 11.2(a)

Qualifying this, however, the Code also includes a number of additional rules which govern the amount of liability that can be allocated to an account holder. These rules apply even where fault on the part of the account holder or an authorised user has been established under the Code.

15.1. Amounts for which account holder has no liability

The Code provides for certain amounts for which an account holder is not liable.

See clause 11.2(b)

15.1.1. Loss in excess of transaction limit

An account holder is not liable for losses incurred which exceed a set transaction limit. A transaction limit may apply to:

- the amount that can be withdrawn/transferred from an account,
- the amount which can be withdrawn/transferred in any one transaction,
- the amount which can be withdrawn by a particular authorised user,
- the amount which can be withdrawn by a particular access method, or
- a combination of these.

In general, transaction limits will apply on a daily basis. However, other periodic limits may be agreed between your institution and the account holder.

See also: Chapter 16 *Transaction limits and liability*

FOR EXAMPLE	A customer may be limited to making no more than $1,000 worth of transactions on their account in any one day. In the event that $1,200 worth of unauthorised transaction were made on their account in a day they would not be liable for the $200 loss which is over and above their daily transaction limit.

15.1.2. Loss in excess of account balance

An account holder is not liable for losses that exceed the balance of their account (including any prearranged credit amount).

See clause 11.2(b)(iii)

15.1.3. Loss when notification facility unavailable

An account holder is not liable for any losses when your institution's notification facility is not available.

Where notification facilities are not available during a particular period, any losses occurring during this period that would otherwise be attributed to a user due to non-notification are deemed to be your institution's responsibility. (However, a user must provide notification within a reasonable time of the facility again becoming available or they may be liable for further losses.)

See clause 17.4

See also: Chapter 17 – *Reporting unauthorised transactions*.

15.1.4. Loss on non-EFT accounts

An account holder is not liable for any loss that occurs on an account which your institution and the account holder have not agreed could be accessed using the device or pass code used to perform the transaction.

See clause 11.2(b)(iv)

FOR EXAMPLE	An elderly customer of a financial services provider lodged a complaint with the FOS after being taken advantage of by a long-standing acquaintance who had withdrawn $175,000 from the customer's account without his knowledge. Having obtained the customer's telephone banking password, which the customer used in the acquaintance's presence, the acquaintance was able to change the customer's address for account statements. She then established internet banking and used this channel to withdraw $5000 per day from the customer's account for just over a month. Even though the customer had disclosed his telephone banking password to the acquaintance, FOS found that liability for the unauthorised payments lay with the financial services provider rather than the customer on the basis that the customer had not agreed to the access method (internet banking) by which the transactions were made. Adapted from *FOS 2013/14 Annual Review* case study (p. 67)

15.2. Effect of chargebacks

Put simply, a chargeback is a right to transfer responsibility for a card transaction from the cardholder's financial institution to the merchant's institution. Both VISA and Mastercard have formulated rules that govern chargeback rights. These include aspects such as the time limits within which a cardholder's institution must exercise its rights.

A failure to exercise chargeback rights has implications under the Code. Specifically, the Code provides that your institution cannot hold an account

holder liable for any unauthorised transactions that could have been charged back under the rules of the relevant card scheme at the time the complaint was made.

See clause 11.10

This principle applies even if the account holder otherwise contributes to the loss, such as by keeping a record of the relevant PIN with the card in their wallet.

FOR EXAMPLE	Mr A was approached by a business associate (Mr B) for help with a temporary lack of funds. Mr A agreed to help and rang a number of firms and authorised the use of his credit card to make a number of one-off payments on Mr B's behalf. Mr B was present in the room during the phone calls. Subsequently, Mr B used his knowledge of Mr A's card details to charge a further $54,000 to the card on 12 separate occasions between January and March. Mr A first realised that Mr B had made an unauthorised transaction when he received his January statement. His first action was to confront Mr B, who promised to pay him back. However, cheques provided by Mr B bounced. Mr A finally informed the card issuer about the unauthorised transactions at the end of March. The card issuer's initial response was that it was his problem, not theirs, and that he would have to sort it out with Mr B. However, after a dispute was lodged with the FOS the card issuer charged back $40,000 worth of transactions. As the remaining transactions were phone-based MOTO transactions (see Chapter 20 for the meaning of MOTO transactions), they came within the coverage of the Code. The FOS issued a finding that it was satisfied that the card issuer did have a right to charge back the remaining transactions when it was notified that they were unauthorised at the end of March. Consequently, clause 11.10 operated to prevent the card issuer from allocating liability for those transactions to the disputant. The FOS ordered the card issuer to refund $14,173 to the disputant plus the subsequent interest charges on that amount.

15.2.1. Inability to exercise chargeback

Chargeback rights usually only remain in place for three to four months after making a transaction. However, your institution cannot impose a time limit on account holders to detect unauthorised transactions regulated by the Code within the available chargeback timeframe.

While the Code does impose liability on a cardholder if they unreasonably delay notification of an unauthorised transaction, liability only commences

from the time they become aware of the transaction. The Code has no provision that links reasonableness (or otherwise) of a notification to your institution retaining a chargeback right.

FOR EXAMPLE	If a family member takes and uses a card without permission and returns it to the cardholder, the cardholder may not become aware of the unauthorised transaction(s) for some months. The fact the card holder's financial institution has lost its right to chargeback the disputed transaction is not relevant to allocation of liability.

16. Transaction limits and liability

The Code does not seek to restrict the daily and other transaction limits that institutions set. However, if a transaction limit is found to be unreasonably high, the institution's liability in the event of an unauthorised transaction may be impacted.

16.1. Types of transaction limits

In general, a transaction limit will be based on a particular periodical amount of time, such as a daily basis. However, your institution can also impose a transaction limit by reference to:

- a particular access method,
- a particular account, or
- the institution equipment used.

Often the applicable transaction limit will be based on a combination of these factors.

FOR EXAMPLE	The most common transaction limit that applies in Australia is a maximum daily cash withdrawal using a card and PIN at an ATM. Each financial institution applies their own chosen limit, which can be varied depending on the customer.

16.2. Effect on liability

Your institution should carefully consider whether it will apply a transaction limit to a particular customer or account, as this may have a bearing on questions of liability.

16.2.1. Transactions above daily limit

An account holder will have no liability for amounts that exceed a daily or other periodical transaction limit attached to their account. This applies whether or not they may otherwise have some responsibility for the loss.

FOR EXAMPLE	An account may have a $1000 daily transaction limit. The account holder will not have any liability for any unauthorised transaction(s) which occur in a single day above this limit.

16.2.2. No reasonable limit

While the Code does not require your institution to apply any transaction limit, AFCA may, in certain circumstances, consider reducing an account holder's liability if no reasonable transaction limit has been applied.

In general, the extent to which an account holder's liability may be reduced will depend on:

- the reasonableness of the limit applied to their account having regard to prevailing industry practice, and
- the security and reliability of the means your institution uses to verify that a transaction was authorised by the user (in the absence of the protection that would have been provided by a reasonable transaction limit)

See clause 11.9

The more secure and reliable the EFT facility (i.e. the more the account holder is protected from losses), the more reasonable it will be to apply a higher transaction limit.

FOS EXAMPLE	A thief stole a debit card and gained knowledge of the PIN in circumstances that were unclear. The account institution that issued the card applied a daily limit of $1,000 to withdrawals at ATMs but applied a separate daily limit of $8,000 to EFTPOS transactions. The thief purchased high value electronic equipment to the value of $40,000 over a five day period before the cardholder became aware that his card was missing. The FOS surveyed a number of account institutions about the limits that might apply to EFTPOS transactions and concluded that $8,000 was not a reasonable daily limit having regard to prevailing industry practice. In addition, as EFTPOS transactions required no authorisation apart from production of the card and entry of correct PIN, the FOS also concluded that there were no secure and reliable means in place to protect the account holder from losses in the absence of a reasonable daily limit. Accordingly, FOS was of the view that the account institution should reimburse the account holder in full. See FOS Banking & Finance Bulletin 59, p.13 (September 2008)

16.3. Modification of transaction limits

Your institution may modify the type and extent of transaction limits it applies over time. The Code requires that your institution provide account holders with 20 days prior notice of such changes.

See clause 4.11(d)

Where the modification involves the removal or increase of an existing limit, your institution must provide account holders with clear and prominent advice that this may increase their liability in the event of an unauthorised transaction.

See clause 4.12

17. Reporting unauthorised transactions

Your institution must provide users with an effective and convenient method by which they can report that:

- a device has been lost, stolen or misused,
- the security of a pass code has been breached, and
- an unauthorised transaction has occurred.

See clause 17.1

17.1. Method of notification

Your institution may provide more than one method of notification. Most retail banking institutions provide a telephone hot line for this purpose.

17.1.1. Availability

At least one facility should be available to users at all times. Where notification facilities are not available during a particular period, any losses occurring during this period (that would otherwise be attributed to a user due to non-notification) are deemed to be your institution's responsibility.

However, a user must provide notification within a reasonable time of the facility again becoming available or they may be liable for further losses.

See clause 17.4

17.1.2. Acknowledgement

Your institution must implement procedures for acknowledging receipt of notifications. Such acknowledgments need not be in writing although they must provide a means by which:

- users can verify that they provided notification, and
- when such notification was made.

See clause 17.5

FOR EXAMPLE	If notification is provided over the telephone, your institution may give the user a reference number to verify that a report has been made.

17.2. Charges for notification

The process by which a user can make a report must be free, or for the cost of a local call only.

See clauses 17.2 and 26.2

It is generally recommended that no charges be imposed for use of a notification method. Such fees may impact on a user's liability for delaying notification under the Code.

Part D – Liability: Specific Cases

18. ATM/EFTPOS transactions using PIN

This Chapter provides a summary of the various issues your institution should take into account when determining liability for unauthorised ATM and EFTPOS transactions made using a personal identification number (PIN). The Chapter should be read in conjunction with the general discussion of liability under the Code in Part C of this Manual.

18.1. What is an ATM/EFTPOS transaction?

Most ATM and EFTPOS transactions are made using a card (either debit or credit) with authorisation for the transaction provided by way of a personal identification number (PIN) which the user enters on a terminal pad. Accordingly, for the purposes of the Code, such transactions require the use of both a device (card) and code (PIN).

Contactless card EFTPOS transactions differ from other EFTPOS transactions, however, in that such transactions require a device (card) only, with no PIN required. Contactless card transactions are not further considered in this Chapter. See Chapter 20 for a summary of the issues related to contactless card transactions.

18.2. Liability for forged ATM/EFTPOS cards

It is quite common for an unauthorised transaction to occur as a result of the user's card being skimmed and a fake or forged card being created. Skimming refers to the process by which a user's card details (including PIN number) are unknowingly obtained and used to make a duplicate copy of the user's card.

Where a user maintains that they were in possession of their ATM/EFTPOS card at the time the unauthorised transaction(s) were made, consideration should be given to whether there is any evidence that the user's card has been skimmed.

Information that supports a conclusion that a card has been skimmed includes:

- the user used their card at the site of a known attack (e.g. ATM or EFTPOS terminal) prior to the unauthorised transactions commencing,
- there is evidence of two cards being used at different locations at or around the same time,
- attempts to make transactions continue after the card is reported as having been compromised and stopped by your institution, and
- the pattern of transactions indicates a person trying to withdraw the maximum amount in the shortest possible time.

Where the evidence suggests that a user's card has been skimmed, it is clear that the user has not contributed to the loss in any way. As such, the account holder must be exempted from all liability. This rule applies even if there is evidence that the user was careless in the use of their card, such as by failing to take steps to obscure the entry of their PIN, or failing to notice a skimming device.

See also: Part C, Chapter 12.

18.3. Liability for misuse of ATM/EFTPOS card

It is possible that a user's card may be unknowingly used by someone else. This will generally be someone close to the user, such as a friend, family member or employee.

Your institution will be liable for such unauthorised transactions unless it can prove on the balance of probability that a user has contributed to the loss by:

- failing to protect the secrecy of their PIN, or
- unreasonably delaying notifying your institution that their card has been misused and/or their PIN security has been breached.

See also: Part C, Chapter 11 – 13.

18.3.1. Failing to protect PIN secrecy

Your institution will be able to hold an account holder liable for any unauthorised transactions which occur as a result of a user failing to properly protect the secrecy of their PIN.

To do so, the Code requires that your institution must show that the user has:

- voluntarily disclosed their PIN to another person,
- kept a record of their PIN on or with their ATM/EFTPOS card, or
- kept a record of their PIN in another location that was not reasonably hidden, disguised or otherwise protected.

See also: Part C, Chapter 13.

Use of correct PIN

The fact that an account has been accessed with the correct PIN, even on the first attempt, will not of itself constitute sufficient proof that a user has either disclosed or kept an unprotected record of their PIN. In other words, your institution will need to have some additional evidence in order to prove the user has breached the security requirements that make them liable under the Code.

Use of prohibited PIN

The fact that an account has been accessed with the correct PIN may suggest that a user has selected a PIN which is easily guessable. Your institution should enquire as to whether the user has selected a PIN which represents their birth date.

If so, an account holder will be liable for the unauthorised transactions, as long as your institution can also establish that prior to PIN selection it provided the user with adequate instruction not to select their birth date as a PIN, and warned them of the consequences of such a selection. (Other easily guessed PINs do not relieve your institution of liability.)

18.3.2. Delay in notification

Liability may also be allocated to an account holder when your institution can prove on the balance of probability that the user has unreasonably delayed notifying your institution of their card's misuse.

In such instances, your institution is entitled to hold the account holder liable (subject to relevant daily and other transaction limits: see Chapters 15 & 16) for any unauthorised transactions that have occurred between when:

- the user became aware that their card had been misused and/or PIN security had been breached (i.e. became aware that an unauthorised transaction had occurred on their account), and
- the user provided notification to your institution.

See also: Part C, Chapters 12 & 13.

18.4. Liability for lost or stolen ATM/EFTPOS card

A user's card may be lost or stolen and subsequently used by someone to make unauthorised transactions. Your institution will be liable for such transactions unless it can prove on the balance of probability that a user has contributed to the loss by:

- failing to protect the secrecy of their PIN, or
- unreasonably delaying notifying your institution that their card was lost or stolen.

See also: Part C, Chapters 12 & 13.

18.4.1. Failing to protect PIN secrecy

Your institution will be able to hold an account holder liable for unauthorised transactions made with a stolen card that occur as a result of a user failing to properly protect the secrecy of their PIN.

In order to do so, your institution must be able to show that the user has:

- kept a record of their PIN on or with their ATM/EFTPOS card, or
- kept a record of their PIN in another location that was not reasonably hidden, disguised or otherwise protected.

The fact that an account has been accessed with the correct PIN, even on the first attempt, will not of itself constitute sufficient proof that a user has either disclosed or kept an unprotected record of their PIN. In other words, your institution will need to have some additional evidence in order to prove the user has breached the security requirements triggering liability under the Code.

The fact that an account has been accessed with the correct PIN may suggest that a user has selected a PIN which is easily guessable. Your institution should enquire as to whether the user has selected a PIN which represents their birth date of birth.

If so, an account holder will be liable for the unauthorised transactions, provided that your institution can also establish that prior to PIN selection it

provided the user with adequate instruction not to select their birth date as a PIN, and warned them of the consequences of such a selection.

See also: Part C, chapters 12 & 13.

18.4.2. Delay in notification

Liability may also be allocated to an account holder when your institution can prove on the balance of probability that the user has unreasonably delayed notifying your institution that this card was lost or stolen.

In such instances your institution is entitled to hold the account holder liable for any unauthorised transactions that have occurred between when:

- the user should have become aware that their card was lost or stolen, and
- the user provided notification to your institution.

18.4.3. Where access method not received

It is possible that a card may be stolen on route to the user. An account holder will have no liability for any unauthorised transactions that are made before they received both their card and PIN.

It is up to your institution to prove that both the card and PIN were in fact received. This is generally achieved by requiring some form of acknowledgement from the user at the time of receipt.

18.5. Chargeback rights

Where an unauthorised EFTPOS transaction has been conducted on a scheme debit or credit card, your institution may have potential chargeback rights.

Your institution should investigate whether any chargeback rights exist and if so, take the appropriate action.

Under the Code, your institution cannot hold an account holder liable for any unauthorised transactions that it could have been charged back.

See also: Chapter 15.2, *Effect of Chargeback*

19. Online banking transactions

This Chapter provides a summary of the various issues your institution should take into account when determining liability for unauthorised online banking transactions.

What is an online banking transaction?

For the purposes of this Manual an online banking transaction refers to a transaction that is made over the Internet via an internet banking facility.

To make an online banking transaction, a user will generally require:

- a customer identification number (identifier) and
- password (code).

However, some organisations also require the use of an additional security token. This is typically a device which generates a onetime pass code, which must be entered in conjunction with the user's identification number and individual password.

19.1. Liability for not protecting password secrecy

It is possible that a user's online banking facility may be unknowingly used by someone else. This will generally be someone close to the user, such as a friend, family member or employee.

Your institution will be able to hold an account holder liable for any unauthorised transactions which occur as a result of a user failing to properly protect the secrecy of their password.

However, to do so the Code requires that your institution must show that the user has:

- voluntarily disclosed their password to another person, or
- kept a record of their password in a location that was not reasonably hidden, disguised or otherwise protected.

19.1.1. Use of correct password is not enough

The fact that an account has been accessed with the correct password, even on the first attempt, will not of itself constitute sufficient proof that a user has either disclosed or kept an unprotected record of their password. In other words, your institution will need to have some other evidence in order to prove the user has breached the security requirements that make them liable under the Code.

19.1.2. Where a prohibited password is used

The fact that an account has been accessed with the correct password may suggest that a user has selected a password which is easily guessable. Your institution should enquire as to whether the user has selected a password which represents their birth date or a recognisable part of their name.

If so, an account holder will be liable for the unauthorised transactions, provided that your institution can also establish that prior to password

selection it provided the user with adequate instruction not to select a recognisable part of their name as a password, and warned them of the consequences of such a selection.

19.1.3. Where password obtained by spyware

A password that is obtained by spyware would not be deemed to be voluntarily disclosed for the purposes of the Code.

However, your institution may be able to hold the user liable if it can prove on the balance of probability that they knew that the spyware was present on their computer or were recklessly indifferent to its presence.

19.1.4. Where a token is used

If your institution requires that a user provide both their individual password and a token-generated pass code in order to make a transaction, an account holder will only be liable for a user failing to protect their password secrecy when your institution can show that this was the dominant cause of the loss. In other words, the consumer cannot be made liable for the loss where the dominant cause of the loss was a failure to protect the token.

19.1.5. Delay in notification

Liability may also be allocated to an account holder when your institution can prove on the balance of probability that the user has unreasonably delayed notifying it that their password security has been breached.

In such instances, your institution is entitled to hold the account holder liable for any unauthorised transactions that have occurred between when:

- the user became aware that their password security has been breached (i.e. that an unauthorised transaction has been made on their account), and
- the user provided notification to your institution.

19.2. Liability for lost or stolen token

If your institution requires a token to be used in order to conduct online banking transactions, a user may be liable for unauthorised transactions if they fail to notify your institution after their token has been lost or stolen.

Liability may also be imposed on an account holder when your institution can prove on the balance of probability that the user has unreasonably delayed notifying your institution that their token was lost or stolen.

In such instances your institution is entitled to hold the account holder liable for any unauthorised transactions that have occurred between when:

- the user should have become aware that their token was lost or stolen, and
- the user provided notification to your institution.

19.2.1. Where token not received

It is possible that a token may be stolen on route to the user. An account holder will have no liability for any unauthorised transactions that are made before they have received their token.

It is up to your institution to prove that the token has been received. This will generally require some form of acknowledgement from the user.

20. Card not present transactions

This Chapter highlights the very limited circumstances in which your institution will be able to assign liability to the account holder in situations involving a disputed card-not-present payment transaction.

20.1. What is a card not present transaction?

In simple terms, a card not present transaction is a transaction that is conducted by use of a credit/debit card where the card holder is not present at the merchant when the transaction is concluded.

Originally card not present transactions were limited to mail order and telephone order or 'MOTO' transactions. However, these days a majority of card not present transactions are made over the Internet. Indeed, the online channel is now the dominant means of making purchases and paying remotely.

Where a consumer card not present transaction is conducted through electronic equipment, such as a telephone or internet, it will be regulated by the Code.

A card not present transaction does not require the use of a PIN. Instead, such transactions are processed by way of 2 or more (non secret) identifiers such as:

- the card number,
- the card expiry date, and
- in some cases the 3-digit card verification value ('CVV') that is usually printed on the reverse of the card.

20.2. Liability for unauthorised card not present transactions

Under the Code:

- an account holder **cannot** be made liable for a loss arising from an unauthorised transaction made using one or more (non-secret) identifiers only (i.e. where neither a PIN or other pass code, or card or other device, is required).
- where a transaction can be made using a device, or a device and an identifier, but does not require a PIN or other pass code, the account holder can be made liable **only** if the user unreasonably delays reporting the loss or theft of the device.

See clause 10.2

Although a card not present transaction requires valid debit/credit card details in order to take place, a debit/credit card is not considered to be a device for the purpose of such transactions as the card itself is not required to complete the transaction.

Thus, because no device or code is generally (see exception below at ¶20.3) used to complete a card not present transaction, your institution will generally

be unable to allocate liability to an account holder for such transactions under the Code if they are disputed as unauthorised.

In relation to such transactions, any coincidental disclosure of a PIN or other pass code, or delay in notifying the loss or theft of a card or other device, will be causally irrelevant as neither the code nor the device was required to make the unauthorised transaction.

Similarly, where no code or device is required to perform the transaction the provisions of the no-fault liability regime do not apply.

In short, by providing payment facilities that allow online and other remote forms of payment (such as telephone and mail order) to be conducted by account holders, financial institutions assume a high risk of bearing the losses associated with disputed transactions.

CASE EXAMPLE	On 31 October 2017, four charges totalling $93,380 were debited to the customer's card. The customer said the disputed charges were made without her consent and were unauthorised. Each disputed charge was a MOTO transaction, carried out using non-secret information visible on the face and the back of the card. FOS said that under Code clause 10.2, unless there is an unreasonable delay in reporting a card's loss or theft, the account holder is not liable for unauthorised transactions that can be made with information visible on the card's face and/or back. There was no unreasonable delay because the customer brought the disputed charges to the attention of a relationship manager on 1 November 2017, the day after they appeared on the card's account statements. FOS found in favour of the customer and required the Financial Services Provider to refund the customer. See FOS Case No: 520361

20.3. Liability for verified card not present transactions

A number of card issuers have implemented verification methods for online purchases. These include Verified by Visa and MasterCard SecureCode.

When an account holder shops at a participating online store, they are required to enter a password before the purchase can be finalised. Additional card holders are also required to register separately and create their own password.

Because this means a secret code is required for such purchases, they will be covered by the Code. In particular, an account holder may be held liable when:

- they disclose their password to someone else, or
- unreasonably delay notifying your institution that the security of their password has been breached.

In addition, the provisions of the no-fault liability regime may be applied to such transactions.

21. Contactless card transactions

This Chapter provides a summary of the various issues your institution should take into account when determining liability for unauthorised contactless card transactions.

21.1. What is a contactless card transaction?

Most MasterCard and Visa cards issued in Australia now generally incorporate radio frequency (RF) technology enabling transactions to be authorised automatically by holding a card against an RF-equipped reader terminal. These services are called *MasterCard PayPass* and *Visa payWave*.

PayPass and *payWave* reader terminals are typically found in stores processing lower value transactions, including supermarkets, cafes and convenience stores, and service stations. Transactions, typically up to $100, can be processed using the technology.

Contactless card transactions differ from other EFTPOS transactions in that the transaction is authorised simply by passing the user's card close to, or touching, the RF-equipped reader. No access code such as a PIN is required.

21.2. Liability for accidental scan

Although generally unlikely it is possible that a transaction will occur as a result of the user's card accidentally being picked up by a reader.

In such instances, it is clear that the user has not contributed to the loss in any way, and as such the account holder must be excused from all liability under the Code.

21.3. Liability for misused card

A user's card may be unknowingly used by someone else. This will generally be someone close to the user, such as a friend, family member or employee. However, it is possible that a shop assistant may also use someone else's contactless card to make unauthorised duplicate transactions.

Because no code is required to authorise contactless card transactions, the possibility of misuse is relatively high.

FOR EXAMPLE	A family member may take a user's card from their wallet and conduct a number of transactions returning it to the user's wallet without the user ever being aware it has been taken.

Your institution will generally be liable for transactions that occur in this way.

No PIN or other pass code is required to authorise contactless transactions; so, even if there was a coincidental disclosure of a PIN by the account user, that disclosure would be causally irrelevant to your institution's liability for an unauthorised contactless card transaction (although it may be relevant in relation to other PIN-enabled transactions separately undertaken by the unauthorised person). In this respect, the Code operates in relation to

unauthorised contactless card transactions similarly to the way it operates in relation to card-not-present transactions (see Chapter 20).

In the case of unauthorised contactless card transactions, however, liability **is** able to be allocated to the account holder where your institution can prove on the balance of probability that the user has unreasonably delayed notifying your institution of the card's loss or misuse. This is because, under Clause 10.2 of the Code, where an unauthorised transaction is made using a card or other device, the account holder can be held liable for the transaction where (but only where) the user unreasonably delays reporting the loss or theft of the device.

See clause 10.2

In contrast to the card-not-present transaction discussed in Chapter 20, a card is required to effect a contactless transaction and is, therefore, causally relevant to the transaction occurring. For this reason, the account holder can be made liable under the Code if they unreasonably delay reporting a card or other device's loss or theft.

In such instances, your institution is entitled to hold the account holder liable for any unauthorised transactions that have occurred between when:

- the user became aware that their card has been misused (i.e. that an unauthorised transaction has occurred on their account), and
- the user provided notification to your institution.

21.4. Liability for lost or stolen card

A contactless card may be lost or stolen and subsequently used by someone to make unauthorised purchases.

For the reasons discussed in¶21.3, liability for transactions made with a lost or stolen card may be allocated to an account holder where (but only where) your institution can prove on the balance of probability that the user has unreasonably delayed notifying your institution that they are no longer in possession of their card.

In such instances, your institution is entitled to hold the account holder liable for any unauthorised transactions that have occurred between when:

- the user should have become aware that their card was lost or stolen, and
- the user provided notification to your institution.

21.5. Chargeback rights

Where an unauthorised contactless card transaction has been conducted on a scheme credit/debit card, your institution may have potential chargeback rights. Your institution should investigate whether any chargeback rights exist and if so, take the appropriate action. Remember, under the Code your institution cannot hold an account holder liable for any unauthorised transactions that it could have charged back.

See also: Chapter 15.2 *Effect of chargeback*

Part E – Other Conduct Matters

22. Expiry dates

The Code sets out rules for facilities that have an expiry date, such as reloadable travel cards. The expiry date is the date after which the facility cannot be used to perform transactions.

NOTE	These requirements will only be relevant to limited use, generally low value payment facilities (such as gift, travel money and other pre-paid cards). They are not applicable to account-based facilities issued by ADIs.

22.1. Minimum expiry date

22.1.1. Reloadable facility

If a facility is reloadable then the expiry date must be at least 12 months from the date the user last reloads the facility. However, this requirement does not apply if the holder is entitled to a refund of the funds or value remaining on the facility at the expiry date.

See clause 18.2

22.1.2. Non-reloadable facility

If a facility is not reloadable then the expiry date must be at least 12 months from the date the user activates the facility, unless the holder is entitled to a refund of the funds or value remaining on the facility at the expiry date.

See clause 18.1

22.2. Expiry date conditions

Your institution is prohibited from unilaterally bringing forward the expiry date on any facility it offers.

See clause 18.3(a)

Your institution must give users a way to check the expiry date (for example, using the process provided for users to check their balance).

See clause 18.3(b)

22.3. Device expiry dates

If a device is needed to perform transactions, your institution must disclose the expiry date on the device. However, if the expiry date cannot be ascertained (e.g. because it depends on the date a user activates or reloads a facility), your institution must clearly disclose on the device the period during which the facility will be able to be used to make transactions.

See clause 18.4

22.4. Regulator expectations

FOS previously provided the following commentary on its approach to dealing with disputes in relation to facilities with expiry dates. This is likely to give an indication of how AFCA may approach the matter:

In considering disputes about facilities with expiry dates, particularly with regard to any balance that is forfeited to the issuer, we will be concerned to ensure that the issuer has complied with the particular provisions in clause 18 [of the Code] about minimum expiry dates, as well as with the general disclosure requirements in clause 4 [of the Code] to prepare clear and unambiguous terms and conditions for facilities. There is clearly an obligation on subscribers to ensure that their customers are fully informed about both the advantages and the disadvantages (including forfeiture of an unclaimed balance) of a facility with an expiry date.

See FOS Circular – e-Payments Code (Issue 9 – Autumn 2012), p. 15

In October 2014, ASIC undertook a review of travel money and similar reloadable card products "with a particular focus on identifying any unfair contract terms or deficient disclosures". As a result, customers whose reloadable cards had expired were able to reclaim leftover funds.

In response, travel money card issuers made improvements, including:

- Improved disclosure about how customers can reclaim funds after expiry.
- Removal or reduction of fees, including inactivity fees.
- Improved communication at card expiry to remind customers of their available balance and explain how funds can be accessed.

See ASIC 14-262MR *ASIC concerns see CBA release $2.2 million for 45,000 travel card customers* (8 October 2014) and ASIC 15-220MR *Consumers can reclaim funds on expired travel money cards following ASIC action* (25 August 2015)

23. Deposits by electronic equipment

The Code sets out some guidelines that apply to a transaction that consists of a deposit of funds to an account.

23.1. Discrepancies

Your institution must notify an account holder as soon as possible of any discrepancy between:

- the amount of the deposit recorded by the electronic equipment or device, and
- the amount recorded by your institution as having been actually received.

When providing this notification your institution must advise the account holder of the actual amount that has been credited to the nominated account.

See clause 19.2

23.2. Security of deposits

Under the Code the security of a deposit or payment into a facility received by your institution's equipment or device is the responsibility of your institution from the time the transaction is completed by the user.

FOR EXAMPLE	Where a customer deposits money at an ATM, responsibility for the security of the deposit belongs to the account institution who owns the ATM from the time the transaction is completed.

This is subject to verification of the amount(s) deposited.

See clause 19.1

24. Privacy

The Code provides some examples of how the Australian Privacy Principles may apply to electronic transactions.

See clause 22.1

It should be noted that the guidance provided in the Code is limited to a number of specific applications only. Additional privacy obligations will apply to your institution's provision of electronic payment facilities; and your institution must ensure it is fully compliant with all of the requirements of the Privacy Act (including the Australian Privacy Principles).

See also: For further information about the requirements of the Privacy Act, refer to GRC Solutions' Australian Privacy Principles Compliance Manual.

24.1. Surveillance of EFT transaction

Your institution must notify users if a surveillance device may be used to monitor a transaction. A surveillance device includes:

- visual recording, such as a camera;
- sound recording, such as a tape recorder; and
- data recording, such as a log in an ATM.

Notification must be provided before the commencement of the transaction (or each session of related transactions).

The notice should state that the transaction may be recorded by a surveillance device and describe the nature of the surveillance.

See clause 22.1(a)

FOR EXAMPLE	Some ATMs have cameras installed. Where a camera is installed, the Code requires you to notify the user they may be photographed. The following would be appropriate notification: • a sticker or sign on the outside of the ATM that indicates "You may be photographed while using this ATM", and • a message on the screen before the commencement of the transaction that indicates "You may be photographed while using this ATM." In practical terms, your institution will have control over this only where your institution owns and/or operates the ATM. Other ATM operators should comply with the requirements of the Code on their own.

24.2. Restriction on information given by systems

Your institution needs to ensure that no electronic equipment it controls or provides will provide information about an account unless the correct access method for that account is used.

See clause 22.1(b)

An exception applies where your institution's employee or agent is the one operating the equipment.

FOR EXAMPLE	An employee servicing an ATM that sees information about an account will not breach this provision.

24.3. Privacy policies on web site

Where transactions can be conducted through your institution's electronic address (e.g. website), your institution should ensure that clear privacy policies are made available to the user.

Privacy policies may be available:

- at that electronic address, or
- through that electronic address (for example by hyper-linking to a further site).

See clause 22.1(d)

Part F – Mistaken Internet Payments

25. Scope and disclosure requirements

The Code sets out a regime for dealing with mistaken internet banking payments. Account institutions were required to comply with this regime from the date they first subscribed to the Code.

25.1. What is a mistaken internet payment?

The Code applies to electronic payments that are:

- made by an account user through a 'Pay Anyone' internet banking facility,
- processed through direct entry using the BECS (Bulk Electronic Clearing System) Procedures, and
- paid into the account of an unintended recipient because the account user selected or entered the wrong:
  - account number, or
  - some other identifier used to process the transaction.

A mistaken internet payment may arise as a result of:

- the account user's error, or
- the account user being advised of the wrong BSB number and/or identifier.

See clause 23.2

25.1.1. Includes incorrect details

The mistaken internet payments provisions of the Code apply where the account user has selected an incorrect payee account from their payee list, as well as where the user has entered incorrect account details.

There had been some uncertainty regarding this; however an agreed interpretation encompassing incorrect selection from the payee's list was settled by ASIC, the Financial Ombudsman Service and the Australian Payments Clearing Association (now AusPayNet) and reflected in an APCA Operational Memorandum of 24 April 2013. As part of this agreement, financial institutions whose systems did not allow the institution to apply the Code regime in cases of incorrect selection from a payee list were given until 31 December 2013 to make the necessary changes.

See GRC Solutions Compliance Note 2013.063 which attaches a copy of Operational Memorandum CS2/genl/020.13 (24 April 2013)

25.1.2. Exemption - BPay

The mistaken internet payment provisions of the Code are expressly stated to not apply to payments made using BPAY (which has its own well-established regime for addressing mistaken payments).

See clause 23.2

25.2. Disclosure requirements

The terms and conditions for accounts that enable account users to make a payment through a 'Pay Anyone' internet banking facility must set:

- the circumstances in which your institution can freeze funds or withdraw them without the account holder's consent (if satisfied that a mistaken internet payment has occurred),
- what an account user must do if they think they have made a mistaken internet payment, and
- the circumstances in which your institution will not be able to recover funds when the account user has made a mistaken internet payment.

See also: For further information refer to Chapter 26.

25.3. On-screen warning

Your institution must provide account users with an on screen warning in relation to making internet payment. This warning should:

- clearly warn account users about the importance of entering the correct details and the risks of mistaken internet payments, including that:
  - the funds may be credited to the account of an unintended recipient if the BSB and account number (and/or other identifier used) do not belong to the named recipient, and
  - it may not be possible to recover funds from an unintended recipient.

See clause 25.1

The warning should also advise account users that the account name will not be validated against the account number when the payment is processed.

See Australian Payments Network (AusPayNet) Guidelines for Mistaken Payments

FOR EXAMPLE	An example of the warning: It is important you check that the BSB number and account number you have entered are correct because payments are processed using these details and without checking the account name. Funds may be credited to the account of an unintended recipient if the BSB number and account number are not correct. It may not be possible to recover funds from an unintended recipient.

The warning must be delivered each time an account user is performing a transaction using a 'Pay Anyone' internet banking facility.

Where practicable it should also be delivered:

- on-screen, and

- before the transaction is finally confirmed, at a time when the account user can cancel the transaction or correct the error.

See clause 25.2

26. Recovery procedures

The Code sets out the procedures that subscribing institutions must put in place to investigate and recover mistaken internet payments.

The obligations vary depending on whether your institution is:

- the **sending ADI** (the institution whose customer has made the internet payment), or
- the **receiving ADI** (the institution whose customer has received the internet payment).

26.1. Obligations of sending ADIs

In general, a sending ADI is required to take steps to assist its account users to recover payments they have made by mistake. The obligations imposed under the Code include:

26.1.1. Acknowledge user reports

A sending ADI must have an effective and convenient process for account users to report mistaken internet payments. The process must be free, or for the cost of a local call only.

See clause 26.1

The sending ADI must acknowledge every report that a mistaken internet payment has occurred. The acknowledgment does not have to be in writing, but must enable account users to verify that they have made a report and when it was made.

See clause 26.3

26.1.2. Request return of funds

The sending ADI is required to make a request to the receiving ADI for return of funds. This request should be completed using the AusPayNet Request for Return of Mistaken Internet Payment Form (A30).

The request should be made within a reasonable time of receiving the account user's report that a mistaken internet payment has occurred. A sending ADI should aim for a turn-around of two business days, unless it is necessary to make enquiries to investigate the report.

See AusPayNet Guidelines for Mistaken Payments

26.1.3. Investigate payment

It is recommended that as a sending ADI, your institution conduct a preliminary investigation as to whether or not a mistaken internet payment has occurred before making a return request. This is partly because under the BECS Procedures a sending ADI can be held liable in respect of wrongly returned funds.

The extent of the investigation will depend on the circumstances. For example:

- if the account user claims to have entered the wrong BSB or account number, you should ask them what the details should have been. In most situations it should be obvious that a transposition or other clerical error has occurred.
- if the account user has selected the wrong payee from their list of existing payees, you should ask them for details as to who the intended payee was, what the payment was made in relation to, etc. In some situations, it may be prudent to obtain a statutory declaration from the account user.

If, on completion of the investigation, your institution is satisfied that a mistaken internet payment has occurred it must send the receiving ADI a request for the return of the funds.

See clause 27.2

If your institution is not satisfied that a mistaken internet payment has occurred, it is not required to take any further action.

See clause 27.3

The Code does not prescribe any timeframes for investigation. However, as a sending ADI is required to provide a final report to the account user within 30 days of their report, it is generally recommended that your investigation be conducted as soon as possible.

See also: For more information about providing a final report see ¶26.1.4 below.

26.1.4. Notifying account user of outcome

Your institution must provide an account user with a written notice that sets out the result of the investigation into their mistaken internet payment report. Depending on the outcome this may include:

- whether or not your institution concluded that a mistaken internet payment occurred,
- whether or not the receiving ADI concluded that a mistaken internet payment occurred,
- whether or not there were sufficient funds in the mistaken recipient's account,
- whether or not the funds have been returned to the account user's account, and
- what further action the account user may take in relation to the matter (such as taking the matter to AFCA).

This notification must be provided within 30 business days of the day on which the account user's report was made.

See clause 33.1

26.2. Obligation as a receiving institution

26.2.1. Acknowledge request

A receiving ADI must acknowledge all requests for return of funds received from a sending ADI within 5 business days.

See clause 27.2

This does not mean that your institution (as a receiving ADI) is required to confirm by this date whether or not it believes a mistaken internet payment has occurred. It must simply note that it has received the request.

When providing its acknowledgement, your institution must also advise the sending ADI whether or not there are sufficient funds in the account of the supposed unintended recipient to cover the mistaken internet payment.

See clause 27.2(b)(ii)

Note that the receiving ADI should not provide the account balance, but merely state whether there are sufficient funds in the account. Doing so would breach the APPs and the banker's duty of confidentiality.

The Australian Payment Network's Request for Return of Mistaken Internet Payment Form (A30) provides a check box that can be used by receiving ADIs to acknowledge the sending ADI's return request.

26.2.2. Investigate payment and return funds

On receipt of a return request from a sending ADI, your institution must use reasonable endeavours to assess whether or not a mistaken internet payment has occurred.

At a minimum, your institution should:

- compare the original direct entry (DE) file against its own records – if the account name and/or number do not match, it can generally be assumed that it is a mistaken payment, or
- where the payment resulted from the user selecting the wrong payee from a list of payees, accept an indication from the sending ADI that the user wrongly selected the payee and made a mistaken payment.

See AusPayNet Guidelines for Mistaken Payments

Additionally, your institution may also wish to:

- compare the intended payment account details against the original DE file – if the account name remains the same and the account number differs it can generally be assumed it is a mistaken payment,
- request additional information from the sending ADI, and
- request additional information from the intended receiving ADI (for example to ascertain the validity of the intended payee account details).

See AusPayNet Guidelines for Mistaken Payments

If satisfied that a mistaken internet payment has occurred, your institution must take steps to return the funds. The required actions are set out in the

table below and vary depending on when the user made their report and the availability of funds in the unintended recipient's account.

Time of user's report	Obligations
Within 10 days of the transaction	Investigate whether a mistaken internet payment has occurred and if satisfied, withdraw the funds from the unintended recipient's account. This process must be completed within 5 business days (or 10 business days if further information is required from the sending ADI).
Between 10 days and 7 months of the transaction	Complete investigation as to whether a mistaken internet payment has occurred within 10 business days. If so, freeze funds to the value of the transaction and notify the unintended recipient that it will withdraw these funds in 10 days unless they can establish an entitlement to the funds. If no substantiated entitlement established - return the funds to the sending ADI within 2 days of the expiry of the notification period (or as the circumstances may allow - for instance where the unintended recipient consents to the return).
More than 7 months after the transaction	Complete investigation as to whether a mistaken payment has occurred and seek the consent of the unintended recipient to return the funds. No timeframe is specified in the Code for either of these actions but they should be done as soon as reasonably practicable. If the unintended recipient consents to the return, funds must be returned to the sending ADI within 2 business days of that consent. If the unintended recipient does not consent or respond, no further action is required.

Where a receiving ADI is not satisfied that a mistaken internet payment has occurred it may either do nothing, or at its discretion it may seek the consent of the unintended recipient to return the funds.

See clause 29.5

26.2.3. Where insufficient funds exist

Where there are insufficient funds in the unintended recipient's account to complete a return of funds, your institution must use reasonable endeavours to retrieve the funds from the unintended recipient overtime, such as by facilitating the repayment of funds through instalments.

See clause 32.1

Insufficient funds exist where the account balance of the unintended recipient is less than the value of the mistaken internet payment. Note that insufficient funds will also exist where recovery would place the unintended recipient's account into overdraft.

See AusPayNet Guidelines for Mistaken Payments

26.2.4. FOS's approach to mistaken internet payment issues

The Financial Ombudsman Service provided the following commentary on its approach to the obligations of the receiving institution under the Code in a mistaken internet payment context. This is an indicator of AFCA's likely approach:

> *The provisions for automatic return of funds where a report is made within 10 business days of the transaction and the funds remain in the account of the unintended recipient give additional certainty for subscribers about their mutual obligations (over and above their rights and responsibilities as members of the Australian Payments Clearing Association). They also ensure that the payer will have their funds returned within a reasonably short period of time. While the unintended recipient may feel aggrieved about a unilateral reversal of a mistaken payment, they will not have suffered any compensable loss if they were not entitled to the funds in the first place.*
>
> *The most important aspect of the provisions regarding cases in which a report is made between 10 business days and 7 months and there are sufficient funds in the account is that the receiving ADI is obliged to prevent the unintended recipient from withdrawing the funds during the 10 business days the unintended recipient has to establish an entitlement to the funds. This provision allows an unintended recipient to seek to establish an entitlement to the funds, but also prevents them from trying to frustrate the recovery process by unilaterally withdrawing the funds once notified of a disputed payment. The requirement to establish entitlement within 10 business days, failing which the funds will be returned, also ensures that the recovery process is relatively brief.*
>
> *We may receive complaints about the actions of the receiving ADI from unintended recipients who are aggrieved by the return process. However, they would have to establish to our satisfaction that they had an entitlement to the funds, and that they had provided that information to the receiving ADI within 10 business days, before we could find that they had suffered a compensable loss.*
>
> *When dealing with individual disputes, we will have regard to:*
>
> - *the prominent warnings routinely given on internet banking screens which alert the sender of a mistaken internet payment that the*

sending ADI places no reliance on the name entered and will transfer the funds by reference to the BSB/account number only, and

- *whether the process for retrieval provided by the Code has been followed.*

As we may only consider a dispute that arises from or relates to the provision of a financial service by the FSP to the applicant, we cannot accept a dispute from a sender about the receiving ADI, unless the sender had attempted to send funds to their own account held with the receiving ADI.

FOS Circular – e-Payments Code (Issue 9 – Autumn 2012), p.12

26.2.5. Relationship with the Centrelink Code

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.

See clause 31.1

This means that in the event there are insufficient funds in the unintended recipient's account, a receiving ADI can only take up to 10% of any social security payments to repay the mistaken funds.

A receiving ADI may take a higher percentage of the unintended recipient's social security payment if they have agreed to this occurring. This agreement must be in writing.

See clause 31.1

27. Mistaken internet payment - complaints

This Chapter sets out the circumstances in which a complaint may be made under the Code in relation to a mistaken internet payment issue. This Chapter should be read in conjunction with *Part H – Complaints Handling*, which details the Code's general requirements in relation to complaints handling.

27.1. Complaints about your institution

An account user who reports a mistaken internet payment can complain about how their report is dealt with, including that:

- your institution has determined that a mistaken internet payment did not occur,
- your institution has not complied with the processes and timeframes set out in the Code.

See clause 34.1

Your institution must attempt to resolve the complaint under its internal dispute resolution procedures.

See clause 34.2

27.2. Complaints about other institution

An account user may also make a complaint to your institution about how their report was dealt with by the receiving institution.

See clause 34.1

The Code requires your institution to deal with complaints made about the actions of the receiving institution under its own internal dispute resolution procedures. It must not require the account user to complain to the receiving institution.

See clause 34.2(b)

27.3. External dispute resolution

The Code states that if an account user is not satisfied with the outcome of an internal investigation they are entitled to complain to AFCA. .

Both the sending ADI and the receiving ADI must cooperate with AFCA, including complying with any decision of AFCA.

See clause 34.3 and 34.4

Note that FOS previously stated that it could not accept a dispute from an account user about actions of a receiving ADI, unless the sender had attempted to send funds to their own account held with the receiving ADI. This is a likely indicator of AFCA's approach to such matters.

See FOS Circular – Autumn 2012

Part G – Account Switching

28. Introduction, scope, terminology

28.1. Overview

The Code sets out obligations that require subscribers who are ADIs to assist account holders who wish to switch their transaction accounts from one ADI to another.

On request, subscribing ADIs must assist account holders to:

- obtain lists (called Regular Payment Lists) of their direct debit arrangements, direct credit arrangements, and other periodical payments for the previous 13 months from the institution the account holder is leaving; and
- switch their existing direct debit and credit arrangements over to the institution the account holder is going to.

See clause 35

As will be apparent, the Code's listing and switching requirements do not deal with electronic payments transfers and, as such, have little intrinsic connection with the rest of the Code. They were included in the Code as an administrative convenience (as the Code is the only ADI Code to which virtually all ADIs subscribe).

NOTE	Open Banking (which is being implemented in accordance with a staggered timetable) is likely to impact the account switching under the Code and may require changes to the Code in time.

28.2. Development of switching provisions

Listing and switching provisions were first inserted in the predecessor EFT Code of Conduct, effective 1 November 2008, following negotiations between the Government, the ADI sector and consumer representatives[7]. The 2008 provisions of the EFT Code are retained in substance as Clauses 35.1 – 35.14 of the Code.

Additional listing and switching requirements were incorporated into the Code from 1 July 2012[8]. These are set out in Clauses 35.15 to 35.23.

The 2012 requirements, which are supported operationally by an Account Switch Mail Box service developed by the Australian Payments Network [AusPayNet][9] (see section 28.6 below), are intended to make the new ADI the prime facilitator of the account switching process. Note, however, that the

[7] For background, see ASIC Media Release 08-213MR *New Account switching service* (31 October 2008), available at www.asic.gov.au
[8] For background, see ASIC Media Release 12-139MR *ASIC implements new bank account switching rules* (26 June 2012), available at www.asic.gov.au
[9] The Australian Payments Network (AusPayNet) is the industry body which manages and develops regulations, procedures, policies and standards governing payments clearing and settlement within Australia. Among other functions, AusPayNet administers payments clearing systems for direct entry payments. For more information about AusPayNet, go to www.auspaynet.com.au

2012 requirements are additional to, and do not replace, the 2008 requirements.

28.3. Application of requirements

The account listing and switching requirements of Clause 35:

- only apply in relation to transaction accounts (i.e. savings and cheque accounts) held by individual customers of ADIs,
- only apply to direct debit arrangements, direct credit arrangements, and other periodical payments associated with such accounts,
- do not apply to scheme credit arrangements, scheme debit arrangements, BPAY transactions, or internet banking 'Pay Anyone' transactions.

Clause 35 requirements apply to ADIs in their roles as:

- New ADI (i.e. the institution the account holder is switching to),
- Current ADI (i.e. the institution the account holder is switching from), and
- Direct entry [DE] User ADI (i.e. the institution of the merchant, service provider, government agency etc with an arrangement to direct credit or direct debit the account holder's account).

Note also – While the obligation to provide a listing service (i.e. a list of regular payments) applies to customer-initiated regular payment arrangements as well as direct credit and direct debit arrangements, the obligation to provide a switching service only applies to direct debit and direct credit payment arrangements.[10]

28.4. Terminology

Clause 35 uses a number of terms that are not used elsewhere in the Code. These terms are defined in Clause 23, *Scope and Definitions*, of Chapter E, Code. Terms relevant to the Chapter 35 Listing and switching requirements include:

- **Direct entry** – a direct debit or direct credit as defined in the BECS Procedures[11]
- **Direct entry user [DE User]** – a person who issues credit or debit payment instructions using the BECS Procedures[12]

[10] Customers must be advised that they will need to re-establish their customer-initiated regular payment arrangements with their new ADI themselves: see ¶30.4.2.
[11] Direct entry is an electronic payment system, administered by AusPayNet, used by sponsored businesses, government agencies and other entities (called DE Users) to collect or send regular payments from/to customers, employees, transfer recipients etc. Payments collected from customers' banking accounts are known as "direct debits". Payments sent to customers' banking accounts are known as "direct credits". For an overview of the Direct Entry system see www.auspaynet.com.au
[12] Direct entry users include: businesses that receive regular payments of utility bills, insurance premiums, loans etc via direct debit arrangements they have with their customers; and businesses, government agencies (such as Centrelink) etc that make salary, dividend and transfer payments by directly crediting their employees', shareholders', transferees' etc accounts. Direct entry users must be sponsored into the direct entry system by a BECS Participating Member financial institution.

- **Periodical payments** - recurring payments that are made daily, weekly, fortnightly, monthly, annually or at other regular intervals, but does not include direct debit arrangements or direct credit arrangements
- **Regular payments -** direct debit arrangements, direct credit arrangements and periodical payments.

28.5. AusPayNet Bulk Electronic Clearance (BECS) Procedures

The Code's obligations are supplemented by, and largely implemented in practice through, provisions contained within the AusPayNet's Bulk Electronic Clearance (BECS) Procedures.[13] Subsequent chapters of this Manual reference the provision of the BECS Procedures that interrelate with the requirements of the Code.

See Part 6 and 7 of the BECS Procedures

28.6. Account Switch Mail Box

Central to the operation of the account listing and switching arrangements is the Account Switch Mail Box [the Mail Box], an electronic mail-box and related set of procedures established and administered by AusPayNet.

The Clause 35 requirements of the Code assume the existence of, and are substantially implemented through, the Mail Box.

28.6.1. Access to the Mail Box

BECS Participating Members of AusPayNet who provide deposit accounts to their customers have access to the Mail Box in their own right. ADIs that are not themselves BECS Participating Members, including many customer-owned ADIs, must be "sponsored" into the system by their banking service provider (Cuscal, Indue, ASL), each of which is a BECS Participating Member.

28.6.2. Operation of the Mail Box

A detailed description of the rules and procedures for the AusPayNet Account Switch Mail Box is beyond the scope of this Manual. AusPayNet provides a comprehensive guide, Account Switch Mail Box – User Guide to Mail Box participants/users.[14] Readers are referred to this resource.

In brief, the Mail Box is a mechanism and set of protocols through which:

- an account holder's new ADI can request a list of the account holder's regular payments (called a Regular Payments List) associated with the account being switched from,
- the account holder's current ADI can provide a Regular Payments List to the new ADI,
- the new ADI can notify relevant DE Users' ADIs of the account holder's changed account details (the new ADI sends the DE User's ADI a

[13] A full copy of the BECS Procedures in relation to switching are available on the AusPayNet website at www.auspaynet.com.au
[14] This Guide is not publicly available.

Notice of Variation which, if accepted, is then forwarded to the DE User/ merchant or service provider to action), and

- the new ADI can notify relevant DE Users' ADIs if the account holder wishes to cancel any direct debit or direct credit arrangements with a DE User (the new ADI sends the DE User's ADI a Notice of Cancellation which, if accepted, is then forwarded to the DE User/merchant or service provider to action).

The Mail Box includes processes allowing participating institutions to:

- reject Regular Payments List Requests and Notifications (e.g. if the information provided is inaccurate or incomplete),
- cancel Requests and Notifications, and
- resubmit Requests and Notifications.

29. Obligations of current institution

29.1. Overview

This Chapter sets out your institution's obligations as the account holder's current ADI (i.e. the institution the account holder is switching from).

As a current ADI, your institution has obligations:

- to provide a list of regular payments to the account holder and/or the new ADI, and

See clauses 35.1 and 35.20

- provide the account holder with assistance in switching their direct debits and direct credits.

See BECS Procedures 6.7G and 7.12E

29.2. Obligation to provide a listing service to account holder

On request, your institution must give an account holder seeking to switch to a different ADI, lists of the account holder's direct debit arrangements, direct credit arrangements and periodical payments with your institution for the previous 13 months.

See clauses 35.1 and 35.2

The lists of direct debit arrangements and direct credit arrangements must include:

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)

g) the amount of the transaction.

See clauses 35.3 and 35.17

The list of direct debit and direct credit arrangements should be substantially in the format set out in BECS Procedure Appendix A25.

The list of periodical payments must include:

a) the BSB and identifier of the payee,

b) the name of the payee

c) a narrative

d) the payment date*, and

e) the amount of the transaction.

See clause 35.4

*For a periodical payment, where a duplicate lodgement reference is used for the same direct entry user identity, the list must include the most recent payment date for the arrangement.

See clause 35.5

As part of the listing service, your institution must also:

- give the account holder instructions to help them identify their internet 'Pay Anyone' payments.

See clause 35.6

- advise the account holder that: (a) the lists may not include one-off payments, and (b) some cancelled payment arrangements may not appear on the lists.

See clause 35.8

Lists and required information must be given as soon as practicable, and no later than 5 days, after the request.

See clause 35.7 and BECS Procedure 6.7G and 7.12E

29.3. Obligation to provide a list of regular payments to new ADI

As an alternative to directly asking your institution for a list of their regular payments (see ¶29.2), an account holder may obtain this information from your institution via the institution they are switching to. The new ADI seeks the account holder's regular payments list, and (as the current ADI) your institution provides that list, through the AusPayNet Account Switch Mail Box.

29.3.1. Content of the obligation

Under the Code, your institution must provide the account holder's new ADI with a list of regular payments (i.e., a list of the account holder's direct debit arrangements, direct credit arrangements and periodical payments with your institution for the previous 13 months) if requested to do so by the new ADI.

See clause 35.20 and BECS Procedures 6.7C and 7.12B

The list must be provided within 5 days of a request being received.

See clause 35.20 and BECS Procedures 6.7C and 7.12B

The obligation to provide a list of regular payments is subject to your institution being satisfied that the request is a valid one. That is, the request is one that:

- relates to an account covered by the switching provisions
- is made by the new ADI in writing and submitted through the AusPayNet Mail Box
- signed by the switching account holder (and any other person whose signature is required to operate on the account), and

- specifies accurate account information which corresponds with information your institution holds for the account holder, including BSB and account number and the names of persons authorised to operate the account

See BECS Procedures 1.1, 6.7C and 7.12B

Your institution is also not obliged to respond to a request for a list of regular payment details unless it is satisfied as to the identity of the requesting account holder.

See clause 35.20

As long as it acts with due care and skill, your institution is not liable to the account holder if it fails to provide a list of all regular payments in response to a request from the new ADI.

See clause 35.20

29.3.2. Implementation through AusPayNet Account Switch Mail Box

The AusPayNet Account Switch Mail Box and associated procedures provides the mechanism through which requests from a new ADI to provide a Regular Payments List [RPL] are received and responded to by your institution as the current ADI. In summary:

- On behalf of a customer who has established an account with them, the new ADI completes an AusPayNet RPL Request form which, having been executed by the customer, is sent to your institution (called the 'old ADI' by AusPayNet) via the Mail Box.
- Your institution may either accept or reject the Request. If the Request is accepted, your institution completes the appropriate RPL form and submits this to the new ADI through the Mail Box.
- If your institution rejects the Request, it must advise the new ADI, providing a reason for the rejection from a menu of 4 reasons:
  - incomplete request,
  - incorrect details,
  - account closed, or
  - other (reason to be specified).

  In response to a rejected Request, the new ADI may either resubmit the Request with completed or corrected details, or cancel the Request. The Mail Box includes processes for resubmitting and cancelling rejected Requests.

For further information and details of these procedures, including example forms, refer to the AusPayNet Account Switch Mail Box – User Guide.[15]

[15] This Guide is provided to Mail Box users through AusPayNet. It is not publicly available.

29.4. Obligation to provide switching service

29.4.1. Content of the obligation

If requested by an account holder, your institution must also assist the account holder to identify which (if any) of the direct debit and direct credit arrangements on their regular payment list they wish to transfer to their account with the new ADI.

The AusPayNet Mail Box provides the mechanism through which the switching process is conducted. Briefly summarised, the process is as follows:

- Your institution:
  - assists the customer to complete the AusPayNet Notice of Variation of Account Details form for each direct debit or direct credit that is being switched (an example of this form is set out in Appendix 29.2), and
  - your institution then forwards a copy of the completed (and signed) Notice of Variation of Account Details to the relevant DE User's ADI via the AusPayNet Mailbox within 2 business days of the customer signing it.

  See BECS Procedure 6.7G and 7.12E
- The DE User's ADI can either accept or reject the Notice of Variation. If it accepts the Notice, it will forward it to the DE User/merchant for the latter to amend the account holder's details.
- If the DE User's ADI rejects the Notice of Variation, it will advise your institution via the AusPayNet Mail Box. Your institution may then either resubmit the Notice with completed or corrected details, or cancel the Notice. The Mail Box includes processes for resubmitting and cancelling rejected Notices.

The Notice of Variation of Account Details Form is found in BECS Procedure Appendix A24.

29.4.2. Warnings to be given when providing service

When providing a switching service, it is generally recommended that your institution advise the account holder that:

- DE Users may take some time to process notifications and some require notice of a change of bank details well in advance of the billing date—if so, a switching notice given under this arrangement may not take effect until the next billing cycle,
- they should retain an adequate balance in their existing account until they are confident that all requested regular payments have been transferred to the new account,
- they are responsible for switching their internet banking 'Pay Anyone' payments, BPAY payments into their new online banking account, and

- they are responsible for switching their own scheme debit card or credit card arrangements by advising their provider or merchant of their new debit card or credit card number.

As a matter of prudent practice, the above warnings should be given in writing at the time your institution provides the account holder with the switching service.

Appendix 29.1 – Format for Regular Payment List

AusPayNet requires that ADIs provide account holders with the list of their direct credit and direct debit payments in a format that is substantially along the following lines:

[Full name of the customer]
[Address of the customer]

BSB No: XXX-XXX
Account No: XXXXXXXXX

Direct Debit and Direct Credit Arrangements for the past 13 months as at dd/mm/yyyy Page: zz9

Date	DE User ID	Name of User	Name of Remitter	Lodgement Reference	Amount
Ddmmyy	XXXXXX	XXXXXXXXX(20)XXXXXXX	XXXXX(16)XXXXXXX	XXXXX(18)XXXXXXXXX	zzzzz9.99
DEBITS					
120508	001244	xyz city council	xyz city co	0045235620201234	120.80
201107	051679	Telco Prepaid Plus	Telco Prepaid	04137778881107	100.00
140208	051679	Telco Prepaid Plus	Telco Prepaid	04137778880208	150.00
140807	051679	Telco Prepaid Plus	Telco Prepaid	04137778880807	100.00
CREDITS					
250508	017766	ABC Ltd	ABC payroll	Salary 3	1156.76
250508	005566	Telco Ltd	Telco dividend	dividends	256.76

*** END OF LIST ***

Note: Under the Account Switching Facility, any periodical payments may be included in the Regular Payments List provided to a Customer or may be provided on a separate list.

Appendix 29.2 – Example of Notice of Variation of Account Details

The following is an example of a completed Notice of Variation provided by AusPayNet. Note that (despite what the example wording says) your institution should insert its details in the section marked Incoming FI.

NOTICE OF VARIATION OF ACCOUNT DETAILS
For recurring payments only

PROMPT ACTION REQUIRED

CONFIDENTIAL COMMUNICATION:

This document is confidential and intended only for the use of the addressee. If you have received this communication in error, please notify the financial institution from which you have received it to arrange disposal. Unauthorised use of the information in this message may result in legal proceedings against the user.

This Notice of Variation of Account Details authorises [NEW FI] to notify Debit Users and Credit Users of changed account details on the Customer's behalf. [NEW FI] must send each Debit User and Credit User, through its Sponsor or User FI (as the case may be), a copy of this signed Notice, together with the particular Schedule relevant to that User. Debit Users and Credit Users are required to verify (by signature comparison or other means) that this form has been properly authorised by the Customer before making any changes to the Customer's Direct Debit or Direct Credit arrangements. ***Debit Users and Credit Users must action this request promptly and contact the Customer if there is any doubt as to the Customer's authorisation. The Customer's instruction takes effect from the date of receipt by the User, subject to the expiry of any notice period which may apply to amendments to the terms of the Customer's arrangement with the User.***

I/We have switched financial institutions and as a result my/our account details, for the purposes of Direct Debits and Direct Credits, have changed.

I/We authorise [NEW FI] to notify each Debit User and Credit User listed in the attached schedules, through its Sponsor or User FI, as the case may be, of my/our changed account details on my/our behalf.

I/we acknowledge that provision of this Notice, together with the relevant Schedule attached, to each such Debit User or Credit User will change the account details set out in my/our direct debit arrangements and direct credit arrangements with them. The other terms of my/our original Direct Debit Request and Direct Credit arrangements are not affected.

I/We instruct each such Debit User and Credit User, ***with immediate effect,*** to use the new account details provided below for my/our Direct Debits /Direct Credits.

My/Our Old Account Details:

Account Name: John Citizen

BSB: 654 - 321 **Account Number:** 987 654 321

My/Our New Account Details:

Account Name: John Citizen

BSB: 123 - 456 **Account Number:** 123 456 789

Name of Financial Institution: My New Bank

I/we confirm that I am/we are authorised to operate the account represented by the BSB and Account Number shown immediately above (my/our New Account Details).

Customer's Name(s): JOHN CITIZEN _____

(Please print)

Customer's signature(s): _____ _____

(in terms of the account authority)

Date: 1st July 2012 Contact Telephone Number: 02 9999 8888

Contact Email: MyEmail@gmail.com.au

New FI Use only

To Sponsor/User Institution: Sponsor Bank [User FI Name]

Date Sent: 3rd July 2012

SCHEDULE

My/Our Direct Debit(s)/ Direct Credit(s) with:

ABC Insurance [Name of User] 011223 [DE User ID]

My/Our Full Account Name: John Citizen

My/Our New Account Details: 123 - 456 [BSB] 123 456 789 [Account Number]

Lodgement Reference	**Name of Remitter**	**Last Payment Date**	**Amount**	**Debit/ Credit**	**Customer's identification number with the Debit User** [examples - Customer's Billing Number, Contract Number or Policy Number]
POL - 111	ABC Insurance	30/06/2012	250.00	debit	POL - 111
POL - 999	ABC Insurance	25/06/2012	100.00	debit	POL - 999

New FI Use only

To Sponsor/User Institution: Sponsor Bank [User FI Name]

Date Sent: 3rd July 2012

30. Obligations of new institution

30.1. Overview

This Chapter sets out your institution's obligations as the account holder's new ADI (i.e. the institution the account holder is switching to) under Clause 35 *Listing and Switching* of the Code.

As the new ADI, your institution has obligations:

- to inform a new account holder about the availability of listing and switching assistance;

  See clauses 35.9 – 35.10

- to provide the new account holder with a listing service, on request;

  See clauses 35.15 – 35.21

- to provide the new account holder with a switching and cancellation service, on request;

  See clauses 35.11 – 35.12 & 35.21 – 35.23

- to assist the new account holder to make their own switching arrangements, should they wish to do so.

  See clause 35.10

30.2. Obligation to inform account holder about switching assistance

When opening a personal transaction account for an account holder seeking to switch from another ADI, your institution must give the account holder relevant information to help them make the switch, including informing them of your institution's ability to assist with the switching process.

See clause 35.9

In our view, this information should:

- be provided whenever it is apparent that a new account holder is switching their account from another ADI (i.e. whether or not the account holder specifically states that they are switching);
- cover the various forms of assistance referred to in Clause 35 of the Code, including the listing and switching services required to be provided under the rules effective since 1 July 2012
- be provided to account holders in written form.

30.3. Obligation to provide a listing service

30.3.1. Content of the obligation

On the request of an account holder seeking switch to your institution, you must obtain a list of the account holder's regular payments (i.e. their direct debit arrangements, direct credit arrangements and periodical payments for the previous 13 months) from their current ADI.

See clause 35.15

This obligation does not apply to scheme credit arrangements, scheme debit arrangements, BPAY transactions and internet banking 'Pay Anyone' transactions.

See *Note*, clause 35.15

However, your institution must give the account holder information to help the account holder identify their own BPAY payments, internet 'pay anyone' payments and any scheme debit or scheme credit arrangements.

See clause 35.16

Your institution must request the list of regular payments from the current ADI within 3 days of the account holder's request being made.

See clause 35.20

Chapter 29 of this Manual sets out the information the current ADI must include in the list of regular payments. The list must be provided by the current ADI within 5 days of being requested by your institution

See clauses 35.17 - 20

As the new ADI, you must provide the list of regular payments to the account holder within 5 days of receiving it from the current ADI.

See clause 35.21(a)

30.3.2. Warning to be given when providing regular payments list

When providing the list of regular payments to the account holder, you must advise the account holder: that, while every effort is taken to ensure completeness, the list may not be complete (e.g. it may not include all regular or one-off payments); and that some cancelled arrangements may appear on the list.

See clause 35.23(a) & (b)

As a matter of prudent practice, this warning should be in writing and should be included in or with the list of regular payments.

30.3.3. Implementation through AusPayNet Account Switch Mail Box

The AusPayNet Account Switch Mail Box and associated procedures provides the mechanism through which, on behalf of a new account holder, your institution can request and receive a Regular Payments List [RPL] from their current ADI. In summary:

- On behalf of a customer who has established an account with you, your institution completes an AusPayNet RPL Request form which, having been executed by the new account holder, is sent to the current ADI (called the 'old ADI' by AusPayNet) via the Mail Box.
- The current ADI may either accept or reject the Request. If the Request is accepted, the current ADI prepares and attaches the completed RPL and submits this to your institution through the Mail Box. Your institution must then provide the RPL to the account holder.
- If the current ADI rejects the Request, it must advise your institution, providing a reason for the rejection from a menu of 4 reasons: incomplete request; incorrect details; account closed; other (reason to be specified). In response to a rejected Request, your institution may either resubmit the Request with completed or corrected details, or cancel the Request. The Mail Box includes processes for resubmitting and cancelling rejected Requests.

For further information and details of these procedures, including example forms, refer to the AusPayNet Account Switch Mail Box – User Guide[16].

30.4. Obligation to provide switching and cancellation service

30.4.1. Content of the obligation

When providing an account holder with a list of their regular payments obtained from their current ADI (see ¶30.3 above), your institution must also:

- offer to assist the account holder to identify which of the direct debit arrangements and direct credit arrangements on the list they wish to transfer to their account with your institution,[17]

  See clause 35.21(b)

- assuming assistance is sought, in respect of each direct debit and direct credit arrangement the account holder wishes to transfer to their account with your institution, notify the relevant DE User's ADI of the changed account details within 2 business days of receiving instructions to do so,

  See clause 35.21(c)

- offer to assist the account holder to identify if they wish to cancel any of the regular payments on their list,

  See clause 35.21(d)

- assuming assistance is sought, in respect of each direct debit and direct credit arrangement the account holder wishes to cancel, notify

[16] This Guide is provided to Mail Box users through AusPayNet. It is not publicly available.
[17] The list may include, as well as direct credit and direct debits, other customer-initiated periodical payment arrangements, recurring payments and internet 'pay anyone' payments. The switching obligations under the Code do not apply to these other payment arrangements. Account holders, who may wish to re-establish these other arrangements from their new account, must be advised of this: see ¶30.4.2 below.

the relevant DE User's ADI of the cancellation within 2 business days of receiving instructions to do so.

See clause 35.21(e)

30.4.2. Warnings to be given when providing service

When providing an account holder with a switching and cancellation service, your institution must advise the account holder that:

a) While every effort is taken to ensure completeness, the list of regular payments may not be complete (e.g. it may not include all regular or one-off payments)

b) Some cancelled arrangements may appear on the list

c) Direct entry users may take some time to process notifications

d) Some direct entry users require notice of a change of bank details well in advance of the billing date—if so, a switching notice given under this arrangement may not take effect until the next billing cycle

e) The holder should retain an adequate balance in their existing account until they are confident that all requested regular payments have been transferred to the new account

f) The switching service applies only to direct debit arrangements and direct credit arrangements and not to periodical payments, BPAY payments, 'Pay Anyone' payments, scheme debit card arrangements and scheme credit card arrangements

g) The account holder is responsible for switching their own internet banking 'Pay Anyone' payments into their new online banking account, and

h) The account holder is responsible for switching their own scheme debit card or credit card arrangements by advising their provider or merchant of their new debit card or credit card number.

See clause 35.23

As a matter of prudent practice, the above warnings should be given in writing at the time your institution offers to provide the account holder with a switching and cancellation service.

30.4.3. Implementation through AusPayNet Account Switch Mail Box

The AusPayNet Account Switch Mail Box and associated procedures provides the mechanism through which, if requested to do so, the new ADI notifies the DE Users' ADIs (and ultimately the DE Users/merchants that initiate direct credits to, and direct debits from, the account holder's account):

- of the account holder's changed account details (see ¶30.4.1 above); or,
- that the account holder is cancelling their direct debit or direct debit arrangement, if this is the case (see ¶30.4.1 above).

Switching Process

Briefly summarised, the AusPayNet Mail Box switching process is as follows:

- On behalf of the account holder, the new ADI completes an AusPayNet Notice of Variation of Account Details form (and schedule where required) for each of the DE Users that initiate direct credits to, and direct debits from, the switching account holder's account. This form is shown in BECS Procedure Appendix A24.
- The account holder having signed the Notice of Variation form(s), the Notice is then forwarded through the Mail Box to the appropriate DE User(s) ADI.[18]
- The DE User's ADI can either accept or reject the Notice of Variation. If it accepts the Notice, it must forward it to the DE User/ merchant for the latter to amend the account holder's details.
- If the DE User ADI rejects the Notice of Variation, it must advise the new ADI, providing a reason for the rejection from a menu of 4 reasons: incomplete request; incorrect details; account closed; other (reason to be specified).
- In response to a rejected Notice of Variation, the New ADI may either resubmit the Notice with completed or corrected details, or cancel the Notice. The Mail Box includes processes for resubmitting and cancelling rejected Notices.

Cancellation Process

Briefly summarised, the AusPayNet Mail Box cancellation process is as follows:

- On behalf of the account holder, the new ADI completes an AusPayNet Notice of Cancellation form setting out the details of the direct debit or direct credit arrangement to be cancelled. The purpose of the Notice is to inform both the DE User's ADI (called the Sponsor/User FI[19]) and the current ADI (called the Old FI) that the account holder wishes to cancel a specific direct debit or credit payment arrangement. This form is shown in BECS Procedure Appendix A21.
- The account holder having signed a cancellation request, the Notice of Cancellation is forwarded through the Mail Box to the DE User's ADI and the current ADI.
- The DE User's ADI can either accept or reject the Notice. If the DE User's ADI accepts the Notice, it must forward it to the DE User/merchant etc to cancel the direct debit or direct credit arrangement.
- If the DE User's ADI rejects the Notice, it must advise the new ADI, providing a reason for the rejection from a menu of 4 reasons:

[18] The AusPayNet regime distinguishes ADIs of merchants with an arrangement to direct debit an account holder's account (called the *Sponsor FI*) and ADIs with an arrangement to direct credit an account holder's account (called the *User FI*).
[19] The AusPayNet regime distinguishes ADIs of merchants with an arrangement to direct debit an account holder's account (called the *Sponsor FI*) and ADIs with an arrangement to direct credit an account holder's account (called the *User FI*).

incomplete request; incorrect details; account closed; other (reason to be specified).

- In response to a rejected Notice of Cancellation, the New ADI may either resubmit the Notice with completed or corrected details, or cancel the Notice. The Mail Box includes processes for resubmitting and cancelling rejected Notices.

For further information regarding the procedures for switching and cancelling regular payment arrangements, and copies of sample forms, refer to the AusPayNet Account Switch Mail Box – User Guide.[20]

30.4.4. Where accountholder has obtained regular payments list from current ADI

As discussed in ¶29.2 above, instead of obtaining a regular payments list through your institution as the new ADI, an account holder may obtain a regular payments list directly from their current ADI. The account holder may then give this list to your institution and ask it to provide a switching and cancellation service on their behalf.

Your institution must provide a switching service under the Code in these circumstances.

See clause 35.11

Your institution should follow the same process as if the list of regular payments had been obtained through your institution (rather than directly from the current ADI).

See clauses 35.11- 35.12

30.5. Obligation to assist account holder making their own switching arrangements

Instead of using your institution to facilitate the switching of their regular payment arrangements (as discussed in section 30.4 above), an account holder may seek to have those arrangements changed him or herself.

In these circumstances, if requested to do so, your institution must provide the account holder with a standardised 'change of account' letter template which they can use to give organisations with which they have arrangements for direct debits, direct credit or periodical payments.

See clause 35.10

The availability of the 'change of account' template letter should be included in the information required to be provided to individuals seeking to switch to your institution: see section 30.2 above.

See clause 35.9

The *AusPayNet Account Switch Mail Box – User Guide* includes a *Switch of Regular Payments Arrangements* form letter which your institution should

[20] This Guide is provided to Mail Box users through AusPayNet. It is not publicly available.

provide as a template to customers seeking to make their own switching arrangements.[21]

[21] This Guide is provided to Mail Box users through AusPayNet. It is not publicly available.

Appendix 30.1 – Example of Notice of Variation of Account Details

The following is an example of a completed Notice of Variation provided by AusPayNet.

NOTICE OF VARIATION OF ACCOUNT DETAILS

For recurring payments only

PROMPT ACTION REQUIRED

This Notice of Variation of Account Details authorises [NEW FI] to notify Debit Users and Credit Users of changed account details on the Customer's behalf. [NEW FI] must send each Debit User and Credit User, through its Sponsor or User FI (as the case may be), a copy of this signed Notice, together with the particular Schedule relevant to that User. Debit Users and Credit Users are required to verify (by signature comparison or other means) that this form has been properly authorised by the Customer before making any changes to the Customer's Direct Debit or Direct Credit arrangements. ***Debit Users and Credit Users must action this request promptly and contact the Customer if there is any doubt as to the Customer's authorisation. The Customer's instruction takes effect from the date of receipt by the User, subject to the expiry of any notice period which may apply to amendments to the terms of the Customer's arrangement with the User.***

I/We have switched financial institutions and as a result my/our account details, for the purposes of Direct Debits and Direct Credits, have changed.

I/We authorise [NEW FI] to notify each Debit User and Credit User listed in the attached schedules, through its Sponsor or User FI, as the case may be, of my/our changed account details on my/our behalf.

I/we acknowledge that provision of this Notice, together with the relevant Schedule attached, to each such Debit User or Credit User will change the account details set out in my/our direct debit arrangements and direct credit arrangements with them. The other terms of my/our original Direct Debit Request and Direct Credit arrangements are not affected.

I/We instruct each such Debit User and Credit User, ***with immediate effect,*** to use the new account details provided below for my/our Direct Debits /Direct Credits.

My/Our Old Account Details:

Account Name: John Citizen

BSB: 654 - 321 **Account Number:** 987 654 321

My/Our New Account Details:

Account Name: John Citizen

BSB: 123 - 456 **Account Number:** 123 456 789

Name of Financial Institution: My New Bank

I/we confirm that I am/we are authorised to operate the account represented by the BSB and Account Number shown immediately above (my/our New Account Details).

Customer's Name(s): JOHN CITIZEN _____

(Please print)

Customer's signature(s): _____ _____

(in terms of the account authority)

Date: 1st July 2012 Contact Telephone Number: 02 9999 8888

Contact Email: MyEmail@gmail.com.au

New FI Use only

To Sponsor/User Institution: Sponsor Bank [User FI Name]

Date Sent: 3rd July 2012

SCHEDULE

My/Our Direct Debit(s)/ Direct Credit(s) with:

ABC Insurance [Name of User] 011223 [DE User ID]

My/Our Full Account Name: John Citizen

My/Our New Account Details: 123 - 456 [BSB] 123 456 789 [Account Number]

Lodgement Reference	Name of Remitter	Last Payment Date	Amount	Debit/ Credit	Customer's identification number with the Debit User [examples - Customer's Billing Number, Contract Number or Policy Number]
POL - 111	ABC Insurance	30/06/2012	250.00	debit	POL - 111
POL - 999	ABC Insurance	25/06/2012	100.00	debit	POL - 999

New FI Use only

To Sponsor/User Institution: Sponsor Bank [User FI Name]

Date Sent: 3rd July 2012

Appendix 30.2 – Example of Direct Debit Cancellation Request

The following is an example of a completed Direct Debit Cancellation Request Form provided by AusPayNet.

DIRECT DEBIT CANCELLATION REQUEST

Incoming FI's/Ledger FI's Logo – Optional

Has the Customer given a signed cancellation instruction? Yes ☐ No ☐

If yes, is the signed cancellation instruction attached or included? Yes ☐ No ☐

Note: any Cancellation Request issued on behalf of a new customer under an account switching arrangement must be signed by the customer in accordance with the relevant account authority.

Date sent: 03 / 07 / 2012 Ledger Institution's Reference Number: A1122

CONFIDENTIAL COMMUNICATION:

This facsimile is confidential and intended only for the use of the addressee. If you have received this communication in error, please notify the financial institution from which you have received it, at the telephone number given, to arrange disposal. Unauthorised use of the information in this message may result in legal proceedings against the user.

To: Sponsor Bank [Name of Sponsor Institution]

B Smith Name of Sponsor Institution's Contact*

Fax number: 1234 5678 **e-mail:**

* Refer to Appendix B7 of the BECS Procedures for details of Contact and fax number / e-mail address.

CC: Old Bank [Full name and ACN/ARBN/ABN of old Ledger FI]]

A Cook Name of old Ledger FI Contact*

Fax number: 9999 8888 **e-mail:**

* Refer to Appendix B7 of the BECS Procedures for details of Contact and fax number / e-mail address.

From: New Bank [Full name and ACN/ARBN/ABN of Ledger FI]

New Bank Branch [Name of Branch or Central Point]

Fax number: 9999 6666 **e-mail:**

Contact Officer (full name) J Lee **Signature:**

We advise that our Customer(s), whose details are shown below, has/have given instructions that they wish to cancel a Direct Debit Request addressed by them to the Debit User whose name and User ID Number are also shown below.

Customer Name(s): John Citizen

Details of account debited: BSB Number: 654 - 321

Account Number: 987 654 321

Name of Debit User: ABC Insurance

Debit User ID Number: 0011233

Lodgement Reference: POL - 888

Name of Remitter: ABC Insurance

Customer's identification number(s) with the Debit User (if known) [Examples: Customer's Billing Number, Contract Number or Policy: POL - 888

Date the Customer's account was last debited: 25/06/2012

In accordance with clause 7.5 of the BECS Procedures, please PROMPTLY forward a copy of this Cancellation Request to the Debit User, who is to act promptly under clause 7.10 of the BECS Procedures in accordance with an instruction to cancel a Direct Debit Request.

I/we confirm that I am/we are authorised to operate the account represented by the BSB and Account number detailed above.

I/we authorise [Ledger FI/Incoming FI] to submit this Cancellation Notice on my/our behalf.

Customer Signature(s)

Customer Name(s) John Citizen

31. Obligations of a direct entry user's ADI

31.1. Overview

This Chapter sets out your institution's obligations as a direct entry [DE] User ADI under Clause 35 *Listing and Switching* of the Code.

As a DE User ADI, your institution has obligations:

- to forward relevant information about an account holder's changed details to the DE User;

See clauses 35.22 & 35.13

- to ensure the DE User processes the changed account details and notifies the customer promptly.

See clause 35.22

31.2. Obligation to forward changed details to DE User

31.2.1. Content of the obligation

As a DE User ADI, when your institution receives information about an account holder's changed account details from a new ADI, it must forward the relevant information to the DE User within 3 business days.

See clauses 35.22 & 35.13

Although the Code does not specifically deal with the situation where your institution (as a DE User ADI) receives information that an account holder has decided to cancel a direct debit or direct credit arrangement, it can be assumed that the obligation to forward the information to the DE User within 3 days also applies in this situation.

31.2.2. Implementation through AusPayNet Account Switch Mail Box

Briefly summarised, the AusPayNet Mail Box provides the mechanism through which a DE User's ADI may:

- receive an AusPayNet Notice of Variation of Account Details or a Notice of Cancellation from a new ADI;
- accept the Notice. If it accepts the Notice, the new ADI must then forward the Notice to the DE User within 3 business days, for the latter to amend the account holder's details;
- alternatively, reject the Notice. If the DE User's ADI rejects the Notice of Variation or Notice of Cancellation, it must advise the new ADI, providing a reason for the rejection from a menu of 4 reasons: incomplete request; incorrect details; account closed; other (reason to be specified).
- In response to a rejected Notice, the new ADI may either resubmit the Notice with completed or corrected details, or cancel the Notice. The

Mail Box includes processes for resubmitting and cancelling rejected Notices.

For further information regarding the procedures for switching and cancelling regular payment arrangements, and copies of sample forms, refer to the AusPayNet Account Switch Mail Box – User Guide[22].

31.3. Obligation to ensure prompt processing & notification by DE User

As a direct entry user ADI, your institution must take reasonable steps, such as through its contractual arrangements with the DE User, to ensure the DE User:

- processes the changed details promptly; and
- notifies the customer that the notice of changed details has been processed*.

See clause 35.22

*If your institution is a DE User making direct debits or credits on behalf of its customers, your institution must notify the originator of the debit or credit (i.e. the customer) of the changed account details.

See clause 35.14

[22] AusPayNet makes this Guide available to ADIs participating in the Mail Box system.

Part H – Complaints Handling

32. Overview

The Code sets out a number of principles that must be followed when a person raises a complaint relating to an electronic transaction or ePayment facility.

32.1. Definition of complaint

The Code defines a complaint as: *an expression of dissatisfaction made to a subscriber about a matter regulated by this Code where a response or resolution is explicitly or implicitly expected*.

See clause 2.6

This definition is based on the definition in the Australian Standard on complaints handing (AS ISO 10002–2006[23]); and is consistent with the definition adopted by ASIC in respect of its regulatory guidance on complaints handling by Credit and AFS Licensees set out in RG 165 *Licensing: Internal and external dispute resolution* (July 2020)[24].

32.2. Subject of complaints

Most complaints related to the Code concern liability for unauthorised transactions. That is, the customer complains that their account has been debited for a transaction which they did not authorise.

Another common type of complaint concerns the situation where funds were not received from an ATM or the correct amount was not received, yet the customer or customer's account has been debited.

Institutions also occasionally receive complaints that do not relate to issues of liability (i.e. the customer has not suffered any financial loss). Examples include:

- where an ATM has captured their card,
- where the user did not receive a transaction slip, or
- where an ATM would not allow the cardholder to perform the transaction which he or she required.

32.3. Timeframes for resolving complaints

Your institution should attempt to resolve all complaints as soon as possible. The Code requires that an initial response be provided to the customer within at least 21 days. This timeframe begins from the date your institution receives all relevant details from the customer.

[23] Note that the ePayments Code still refers to the 2006 version of the Australian Standard, even though it was updated in 2014 to become AS/NZS 10002:2014.
[24] RG 165 applies to complaints received by financial institutions before 5 October 2021, the date the new ASIC RG 271 *Internal dispute resolution* (RG 271) comes into effect.
ASIC RG 165 also refers to the superseded AS ISO 10002-2006 *Customer satisfaction - Guidelines for complaints handling in organizations*, while regulation 7.6.02(1) requires ASIC to take into account the current standard: AS/NZS 10002:2014 *Guidelines for complaint management in organizations* when considering whether to make or approve standards or requirements relating to internal dispute resolution. However, the new RG 271 has adopted the new standard AS/NZS 10002:2014.

Where a complaint cannot be resolved within 21 days, the Code allows your institution a further 24 days (i.e. 45 days in total) to complete its investigation, after which the customer must be advised of their right to take the complaint to external dispute resolution.

See clauses 38.4 and 38.5

32.4. Complaints involving third parties

A complaint may arise as the result of another party to the shared EFT system (such as a retailer, merchant or other financial institution) failing to meet their obligations.

Under the Code your institution is prohibited from requiring that a customer raise a complaint with any other party to the shared EFT system. This means that your institution must deal with any complaints made to it directly.

See clause 15.3

FOR EXAMPLE	If loss occurs to a user from an equipment malfunction at an XYZ Bank ATM, your institution must never direct the user to take up the dispute with XYZ Bank.

32.5. Liability if you do not follow the correct procedures

Where your institution fails to follow the complaints handling procedures set out in the Code, AFCA is entitled to hold it liable for all or part of the amount in dispute.

Liability under this rule might arise where your institution:

- fails to obtain from the user all of the prescribed information for unauthorised transaction complaints,
- fails to correctly allocate liability in accordance with the rules for allocation of liability under the Code,
- fails to adequately notify the complainant as to the reasons for its determination of liability.

Note that this requirement is about procedural compliance. As such, your institution may be made liable under this clause even if it would not ultimately be liable for the loss on the substance of the complaint.

See clause 38.10

32.6. Limitations period for lodging complaints

Your institution must accept a complaint if it receives the complaint within six years from the day that the user first became aware, or should reasonably have become aware, of the circumstances giving rise to the complaint.

See clause 38.1

32.6.1. Limitations period and chargeback rules

Card scheme chargeback rules often limit the ability of the customer to lodge a chargeback request to 120 days. ASIC has made clear that a complaint

under the Code can still be lodged even if the period for charge back requests has expired.

CASE EXAMPLE	Citibank refunded around 4,000 current and former customers more than $1 million after the bank refused their requests to investigate 'card not present' unauthorised transaction complaints because the requests to investigate were made outside the time period permitted under the Visa and MasterCard scheme chargeback rules. Citibank's customer letters over the period from 1 January 2009 to 22 July 2016 advised that, because of the customer's failure to report within the schemes' chargeback timeframes, the bank "was not required to assess the claim, and the customer's only options were to approach the merchant or a fair trading agency". The letters made no reference to the customers' rights under the unauthorised transaction provisions of the ePayments Code. As such, in ASIC's view, Citibank misled its customers (by omission) about their protections under the Code; and, in consequence, its customers "would not have had their claims properly considered in accordance with Citibank's contractual obligations with those customers" under the Code. See ASIC MR 17-376 (9 November 2017)

33. Complaints handling system

Your institution must establish and document a complaints handling system that covers all of its products and services that are regulated by the Code.

33.1. Minimum requirements

At a minimum the Code requires your institution to establish internal complaint handling procedures which comply with:

- ASIC Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (RG 165), and
- AS ISO 10002–2006[25] *Customer satisfaction—Guidelines for complaints handling in organizations* to the extent required by RG 165

See clause 37.1

Key aspects of AS ISO 10002-2006 are outlined in the remainder of this Chapter. However, your institution should ensure that it has a copy of the full standard, which can be obtained from the Standards Australia website at: www.standards.com.au.

NOTE	ASIC Regulatory Guide RG 165 will apply until 4 October 2021. It will be replaced by RG 271 from 5 October 2021. This Manual will be updated as more information is released by ASIC.

33.2. Documentation

Your institution should ensure that its procedures are adequately documented. This will help to ensure the procedures are transparent, as well as facilitating staff training and awareness.

Your institution should set out in writing matters such as the following:

- the procedure for receiving and investigating complaints,
- the means by which your institution will respond to complaints and the appropriate time frames,
- the procedure by which unresolved complaints are to be referred to an external dispute resolution scheme, and
- the types of remedies available for resolving complaints.

33.3. Accessibility

Your institution's complaints handling system must be free and accessible to customers. In this respect, the system should be reasonably accessible by all of your institution's customers, including people who do not speak English, people who have an intellectual or physical disability, and those with low levels of literacy.

[25] Note that the ePayments Code still refers to the 2006 version of the Australian Standard, even though it was updated in 2014 to become AS/NZS 10002:2014.

Your institution's complaints handling system should provide a straightforward process for resolving complaints. In general, we recommend that:

- there should be a single contact point for complainants;
- a particular employee should be nominated to deal with each complaint (as far as possible this should not be someone who is the subject of, or involved in, the complaint);
- the nominated person should have:
  - sufficient training and competence to deal with those complaints; and
  - the capacity to resolve the complaint themselves, or the ability to liaise readily with a person or persons with that authority in your organisation.

33.4. Dissemination of information

Your institution should provide a copy of its complaints handling procedures to all relevant staff.

Additionally, a simple guide to your institution's procedures should be made available:

- in Terms and Conditions booklets,
- to customers on request,
- in a relevant section of your institution's website.

33.5. Collection of statistics

Your institution should arrange to record complaints and their resolution so that aggregate data on the type, frequency and resolution of such complaints is available. This will be used for two purposes:

- to allow your institution to identify and address systematic problems.
- to allow your institution to meet its reporting obligations. Chapter 37 *Administrative requirements of Code* discusses the Code's reporting requirements.

34. Investigating a complaint

This Chapter sets out the procedures your institution should follow when a customer makes an ePayments Code related complaint.

34.1. Get complaint in writing

The first thing your institution should do is obtain details of the customer's complaint. Unless the complaint is a simple one, which can be resolved to the customer's satisfaction immediately, your institution should ensure that a written record of the complaint is made.

In general, it is good practice for a staff member of your institution to make the record having obtained details from the customer orally. However, the customer may be asked to complete a form themselves, for example where a complaint is lodged online.

It is important that your institution obtains sufficient information from customers to enable it to carry out proper investigations. Accordingly, consideration should be given to developing one or more standard documents for this purpose.

34.1.1. Duty to provide all relevant information

A customer has a duty to provide your institution with the information it requests about a dispute. Your institution is entitled to hold off investigating a dispute until all requested information has been provided.

However, a customer is not required to provide irrelevant information. As such, your institution should not delay an investigation where the outstanding information is irrelevant to the complaint or is not reasonably available.

See FOS Bulletin 37 (March 2003)

34.2. Initial response

Once sufficient information as to the substance of the dispute has been obtained, your institution should consider providing the customer with a written notice that summarises its procedures for investigating and handling complaints.

In addition to acknowledging receipt of their dispute the notice should outline the timeframes in which the customer should expect to receive a response from your institution.

FOR EXAMPLE	*"You should receive advice of our findings within 21 days of you providing us with the completed Enquiry/Complaint form. If we are unable to complete our investigation within this timeframe we reserve the right, by notifying you in writing, to extend the investigation period by up to a further 24 days."*

34.3. Unauthorised transaction disputes

Most complaints concern liability for unauthorised transactions. There are a number of specific matters that need to be considered when investigating these types of disputes:

34.3.1. Obtain prescribed information

Where a complaint concerns an unauthorised transaction, your institution must make a reasonable effort to obtain certain information prescribed by the Code.

See clause 38.2

To the extent that it is available and relevant to the complaint, the following information should be obtained:

- account type and number
- type of device and/or pass code used to perform the transaction
- name and address of the account holder
- the name of other users authorised to operate on the relevant account,
- whether a device used to perform the transactions was signed by the user,
- whether a device was lost, stolen or misused or the security of a pass code was breached. If so:
  - date and time of loss, theft or security breach
  - the date and time this was reported to your institution
  - the date, time and method it was reported to the police
  - where and how loss, theft or security breach occurred (e.g. housebreaking, stolen purse/wallet).
- where a pass code was used to make the transaction:
  - whether a record of the code was made and if so:
  - how was it recorded
  - where it was kept
  - whether the record of code was lost or stolen and if so, the date and time of the loss or theft.
  - whether the code had been disclosed to anyone else
- details of transaction to be investigated, including:
  - a general description,
  - the date, time and amount, and
  - type and location of electronic equipment used.

- any details which the user considers relevant to his/her liability in respect of the transaction, such as:
  - circumstances surrounding the loss, theft or security breach
  - the reporting of the loss, theft or security breach
  - any steps taken by the user to ensure the security of the device or pass code
- details of the last valid transaction.

Appendix 34.1 provides a template form which can be adapted in order to collect the specified information above.

34.3.2.System failure

Whenever a customer raises a complaint concerning the authorisation of a transaction, your institution should investigate whether there was any system or equipment malfunction at the time of the transaction.

Where a failure is found to have occurred, your institution will be responsible to users for any resulting unauthorised transactions. In addition, your institution may be liable for any other consequential loss a user may have suffered.

See Clause 14

34.3.3.Authorisation

In any transaction dispute, consider whether there are any reasons to suspect the transaction was authorised by the account holder or other user.

All the facts surrounding the transaction must be taken into consideration. In some situations, the weight of the information may support a conclusion that the transactions were made or authorised by a user.

The burden of establishing that a disputed transaction was in fact authorised falls on your institution. In the majority of situations the customer's complaint is likely to be legitimate.

CASE EXAMPLE	Mrs B disputed a number of ATM withdrawals made from a joint account she held with her husband. After examining all of the circumstances of the case the FOS held that on the balance of probability the transactions in dispute were not unauthorised transactions due to the fact that: • Mrs B made a number of undisputed withdrawals during the period in which the disputed transactions occurred, • the disputed and undisputed transactions were for the same amount, • the disputed and undisputed transactions were made at the same ATMs, which were all located close to Mrs B's home,

	• Mrs B was in possession of her card at all times, so in order to make both the disputed and undisputed transactions someone would have had to take it and return it to her on a number of occasions.

34.3.4. Liability

If satisfied that the transaction in dispute is unauthorised, your institution will then need to consider the provisions of the Code liability regime. Refer to details about this regime in *Part C – Liability: General* and *Part D: Liability: Specific Case*s of this Manual.

Briefly summarised:

Situations where account holder has no liability

First your institution should investigate whether the transaction is likely to be a result of any of the following:

- the fraudulent or negligent conduct of your institution's agents and employees (or those of other companies linked to the electronic funds transfer system),
- activity which occurred:
  - before the user received their access device or code - including any replacement device or code,
  - after your institution had been notified that the user's access device had been misused, lost or stolen or that the security of their access code had been breached,
- made with a component of an access method that was forged, faulty, expired or cancelled, or
- your institution's system incorrectly debiting the transaction more than once to the same account.

If so, the account holder cannot be held liable for the transaction and should be reimbursed accordingly.

Situations where account holder has liability

If none of the no-liability situations (as set out above) apply, your institution should then consider whether a user has any potential responsibility for the transaction. In this respect your institution should investigate whether there is any evidence to indicate that the transaction is the result of a user:

- voluntarily disclosing their code to someone else.
- keeping a record of their code on or with their access device.
- acting with extreme carelessness in the protection of their code(s).
- selecting a prohibited code.
- unreasonably delaying notification that:
  - their device was misused lost or stolen, or

— the security of their code had been breached.

If your institution is able to establish (on the balance of probability) that a user has committed any of these actions then the account holder may be held liable for any unauthorised transaction which occurred as a result.

However, if your institution is unable to obtain sufficient evidence to establish responsibility for the disputed transactions then the account holder may not be made liable, subject to a limited amount of liability being able to be allocated according to the no-fault liability regime (see Chapter 14).

Appendix 34.1 - EFT Transaction Enquiry/Complaint Form

The form on the following pages can be adapted by your institution to collect the information required to investigate an unauthorised transaction dispute.

EFT TRANSACTION ENQUIRY / COMPLAINT

Office Use Only
EFT Ref No:

*Credit Union/BuildingSociety/Bank:*_____

SECTION 1

Name Of User:_____

Address Of User: _____

Account Type And Number: _____

Other Users Authorised To Operate On The Relevant Account(s): _____

SECTION 2

Transaction Details Of Transaction To Be Investigated

Type Of Access Method Used:_____

Date	Time	Wdl/Dep/Other

Amount Requested: $ _____

Amount Received: $ _____

Type And Location Of Electronic Equipment Used: _____

_____

Details Of Problem: _____

_____

Details Of Last Valid Transaction: _____

_____

SECTION 3

Device Loss Circumstances

1. Was Device Signed? Yes / No

2. Was Device Lost / Stolen: _____
   Date: _____
   Time: _____
   Place: _____

3. Loss Reported To Organisation: _____
   Date: _____
   Time: _____
   Reference Number: _____

4. Loss Reported To Police / Other: _____
   Date: _____
   Time: _____
   Where: _____

Code Circumstances

5. Where Was The Code Recorded Or Kept: _____

6. Was Code Lost / Stolen: _____
   Date: _____
   Time: _____
   Place: _____

7. Loss Reported To Organisation: _____
   Date: _____
   Time: _____
   Reference Number: _____

8. Loss Reported To Police / Other: _____
   Date: _____
   Time: _____
   Where: _____

9. Has Code Been Disclosed To Anyone : Yes / No

SECTION 3 Continued

10. If Yes To Whom Has Code Been Disclosed: Spouse / Family
    Other: _____

11. How And Where Did The Loss Of The Device / Code Occur (Include Information Regarding Any Other Institutions' Cards. Include Relevant Details About Steps Taken To Ensure Security Of Device Or Codes):
    _____
    _____

12. Date Of Last Valid Transaction: _____
    Amount: $ _____

35. Timeframes for investigation

The Code sets out the timeframe in which a dispute about a Code related matter must be resolved by your institution.

These timeframes are consistent with those imposed on your institution in relation to financial services and credit products under ASIC RG 165.[26]

35.1. General timeframe

As a general rule, your institution must attempt to complete all investigations within 21 days. This timeframe begins from the date your institution receives all relevant details from the complainant.

See clause 38.4

The Code requires that your institution notify the complainant as to the outcome of its decision by the end of the 21 day period. Accordingly, your institution will need to resolve complaints internally within a shorter period (such as 14 days) in order to ensure notification reaches the customer in time.

35.2. Extended timeframe

Where a complaint cannot be resolved within 21 days, the Code allows your institution a further 24 days (i.e. 45 days in total) to complete its investigation.

35.2.1. Notification

Where the extended timeframe is to be applied, your institution must write to the complainant and advise them of the need for more time. Notification must be provided to the customer by the end of the initial 21 day period.

See clause 38.4(b)

35.2.2. Complaints beyond 45 days

All investigations must be completed within 45 days unless there are exceptional circumstances. These may include delays caused by foreign account institutions or foreign merchants being involved in the resolution process.

See clause 38.5

Where an investigation continues beyond the extended 45 day timeframe your institution must write to the customer and advise them of:

- the reasons for the delay,
- their right to take their complaint to AFCA, and
- the contact details of AFCA.

See ASIC RG 165.89

[26] Note that RG 165 will be replaced by RG 271 from 5 October 2021.

35.3. Complaints involving other institutions

Slow response times of other institutions involved in processing the disputed transaction can be a common source of delay.

To assist with this the problem the Code requires subscribing institutions to respond to requests for information from other subscribers within 15 days, unless there are exceptional circumstances.

See clause 38.6

35.4. Timeframes for disputes involving credit cards

Where a complaint is connected with a credit card transaction your institution may choose to exercise "chargeback" rights under the rules of the relevant card scheme.

In such situations, your institution may also choose to adopt any timeframes for resolution provided under the rules of the card scheme in lieu of the Code requirements.

See clause 39.1(a)

Where your institution decides to apply card scheme time limits it must comply with the following additional requirements of the Code:

35.4.1. Notification to complainant

Where your institution intends to apply card scheme's resolution procedures it must inform the customer, in writing, of the relevant time limits that will apply under the scheme rules and when they may reasonably expect a decision.

See clause 39.1(c)

35.4.2. Suspension of user's obligations

Your institution must suspend the account holder's obligation to pay any amount which is the subject of the complaint and any other charges related to that amount until the complaint is resolved.

Your institution must also inform the account holder of that suspension. This may be done at the same time as notification of the relevant time limits is provided.

See clause 39.1(d)

35.4.3. Complaints continuing beyond 60 days

If your institution is unable to resolve a complaint within 60 days, the Code requires that it write to the customer to advise them:

- of the reasons for the delay, and
- a date when a decision could reasonably be expected.

Thereafter, your institution must provide the complainant with a progress update on their complaint at least every two months.

See clause 39.1(b)

36. Resolving the complaint

After collecting and assessing all available evidence your institution should be in a position to resolve the complainant's complaint. The subsequent obligations imposed by the Code depend upon the decision your institution reaches.

36.1. Where you find wholly in favour of a customer

Your institution may decide to resolve a complaint wholly in favour of the complainant. This may be due to the nature of the evidence or the complainant's history and relationship with your institution.

FOR EXAMPLE	Your institution may consider that the actions of a user have contributed to a number of unauthorised transactions occurring. However, it may decide to find in favour of the account holder because the potential damage to the relationship does not warrant finding against the user.

Your institution should ensure that any appropriate adjustments are made to the customer's account. Adjustments should be made as soon as possible after your institution has reached its decision.

In addition, under the Code, where your institution determines a complaint wholly in favour of a customer, it must do the following:

36.1.1. Notify outcome

Your institution must provide the complainant with a written notice that sets out:

- the outcome of its investigation, and
- the reasons for its decision, including references to relevant clauses of the Code.

See clause 38.7

36.1.2. Complaints resolved within 5 days

If your institution is able to settle a complaint to the complete satisfaction of a complainant within 5 business days, it is not required to advise the complainant in writing of the outcome of the complaint, unless they specifically request a written response.

See clause 38.8

36.2. Where you find wholly or partly against a complainant

Your institution may decide to resolve a complaint wholly or partly against a complainant. In practice this will generally mean that:

- your institution has determined (on the balance of probability) that a complainant has contributed to one or more of the unauthorised transactions in dispute, or

- your institution has decided to apply the provisions of the Code's no-fault liability regime.

Under the Code, where your institution determines a complaint wholly or partly against a customer, it must provide the complainant with a written notice that sets out:

- the outcome of its investigation,
- the reasons for its decision, including references to relevant clauses of the Code,
- information about any further action the complainant can take, including their right to take their complaint to AFCA, and
- the contact details for AFCA.

See clause 38.7 and ASIC RG 165.87

Part I – Code Administration

37. Administrative requirements of Code

This Chapter sets out details of the Code's administrative arrangements (as *specified in Chapter G: Administration* of the Code). It covers:

- ASIC's powers and responsibilities as Code administrator; and
- the Code's compliance monitoring arrangements.

37.1. ASIC's powers and responsibilities

Although the Code is an industry code of conduct, unlike other financial services industry codes (such as the Customer Owned Banking Code of Practice, the General Insurance Code, and the Code of Banking Practice) the Code is administered by the financial services statutory regulator, ASIC, rather than a separately constituted industry-established body.

This is a legacy arrangement reflecting the fact that the Code is not 'owned' by any single industry sector.

As Code administrator, ASIC:

- may issue guidelines interpreting the Code

See clause 42

- may issue exemptions from specified clauses of the Code to subscribers/ classes of subscribers; subject to meeting various requirements.

See clause 43

- may declare that the Code, as modified by the declaration, applies to particular transactions/ types of transaction, facilities/ classes of facility, subscriber/ class of subscribers; subject to meeting various requirements.

See clause 43

- may undertake (or have its agent undertake) targeted compliance monitoring of specific obligations under the Code.

See clause 44

- in consultation with stakeholders, must commence (or have its agent commence) a review of the Code within 5 years of the conclusion of each preceding review.

See clause 45

37.2. Code compliance monitoring arrangements

The Code requires subscribers to:

- Annually report information about unauthorised transactions, as specified in a notice published on ASIC's website.

See clause 44.1

NOTE	ASIC has placed a temporary pause on the unauthorised transaction data report requirements. It does not require reports for the 2018, 2019 and 2020 calendar years. ASIC will provide an update about reporting requirements for subsequent years. See https://asic.gov.au/regulatory-resources/financial-services/epayments-code/

- Report to ASIC (or its agent) regarding its compliance with specific clauses of the Code, in response to targeted compliance monitoring of Code obligations.

See clause 44.2