ASIC
Australian Securities &
Investments Commission

ePayments Code

Effective from 2 June 2022

Document control

Document ownership

The Australian Securities and Investments Commission (ASIC) is responsible for the development of this Code.

Document history

This Code is effective from 2 June 2022.

Previous versions:

- ePayments Code, issued 20 September 2011 and amended October 2011. Effective 1 July 2012 and amended 29 March 2016.
- EFT Code, effective 1 April 2001 and amended 18 March 2002, 1 November 2008 and 1 July 2012. Superseded by ePayments Code on 20 March 2013.

Document location

The ePayments Code can be downloaded from the ASIC website.

Contents

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

(a) before the change takes effect, and

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

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

Tailored requirements for low value facilities

4.16 Clauses 4.12–4.15 do not apply to changes to terms and conditions for low value facilities. Instead, a subscriber must give holders advance notice of changes to terms and conditions for low value facilities:

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

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

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

Note 1: Subscribers must provide a process (such as a website) for users to check the balance on low value facilities: see clause 5.9.

Note 2: Clauses 4.16(b)–4.16(c) set out the specific obligation on a subscriber to give holders advance notice of changes to terms and conditions where the subscriber does not know the identity and contact details of the holder. This is different from clause 4.18, which sets out how a subscriber who does not know the identity or contact details of a holder can comply with the other obligations under clause 4.

Exception

4.17 A subscriber is not required to give advance notice of:

(a) the reduction or cancellation of daily card limits for cash withdrawals, purchases and transfers using electronic and telephone banking by holders or users, or

(b) other changes to terms and conditions,

required to immediately restore or maintain the security of a system or an individual facility, including the prevention of systemic or individual criminal activity, including fraud.

Tailored requirements for low value facilities

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

5 Receipts

Receipt requirements

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

Note: This clause does not apply to transactions performed using telephone banking or low value facilities: see clauses 5.8–5.9. In some instances, it may not be reasonable to offer receipts—for example, for direct debit arrangements, where it is clearly identifiable on a statement.

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

(a) amount,

(b) date,

(c) transaction type,

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

(e) information to enable the subscriber to identify the holder and the transaction (such as a reference code or number).

5.3 A receipt must not include certain information where doing so would increase the risk of unauthorised transactions, such as:

(a) a complete identifier, or

(b) an expiry date for a device.

Note: The *Payment Card Industry Data Security Standard* (PCI DSS), issued by the PCI Security Standards Council, sets out minimum requirements for the masking of a card's 'Primary Account Number' when displayed. This Code does not specify any minimum identifier-masking requirements and is not intended to operate inconsistently with the PCI DSS. Subscribers, in applying this Code's requirements in clause 5, may be guided by the PCI DSS and any other more onerous legal or contractual receipt content requirements.

5.4 The requirement in clause 5.3(a) to not include a complete identifier on a receipt does not apply to receipts generated for pay anyone banking facility transactions or transactions from one bank account of the user to another bank account of the same user within the same ADI.

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

(a) time, and

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

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

(a) the name of the merchant, or

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

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

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

Telephone banking

5.8 Clauses 5.1–5.7 do not apply to transactions performed using telephone banking. Instead, a subscriber must take reasonable steps to offer users the following information, at the time of a telephone banking transaction:

(a) receipt number,

(b) transaction amount,

(c) transaction type, and

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

Tailored requirements for low value facilities

5.9 Clauses 5.1–5.8 do not apply to transactions performed using a low value facility. Instead, the subscriber must give users:

(a) a process for users to check the balance on the facility, and

(b) either:

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

(ii) a process for users to check their transaction history. Details of transactions must be available for a reasonable period, taking into account general industry practice for similar facilities.

Subscribers must not charge for receipts

5.10 A subscriber must not charge users for giving:

(a) a receipt under clause 5.1,

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

(c) information about transactions performed using a low value facility under clause 5.9.

Use of equipment or systems that do not belong to a subscriber

5.11 Where a user does not use a subscriber's equipment or systems, and does not communicate with the subscriber or anyone acting on its behalf, the subscriber must use its best endeavours to comply with clauses 5.1–5.10.

6 Fees charged by ATM provider

ATM fees

6.1 A subscriber that is an ATM provider must disclose the amount of any fee or charge for using an ATM it provides that will be directly passed on to a user who:

(a) is a customer of the subscriber, or

(b) is not a customer of the subscriber.

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

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

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

(a) the ATM provider must disclose the amount of any fee charged for using its ATM that will be directly passed on to a customer who is not otherwise a customer of the ATM provider,

(b) the information in clause 6.4(a) must be disclosed before the user completes the transaction, and

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

7 Statements

Subscribers must give statements

7.1 A subscriber must give holders a statement of transactions performed through a facility at least every 6 months, unless the facility:

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

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

7.2 A subscriber must also give holders the option of receiving statements more frequently than every 6 months, and bring this option to the holder's attention when the holder first uses the facility.

7.3 A subscriber must also give holders statements on request.

Statement requirements

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

(a) amount,

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

(c) transaction type,

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

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

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

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

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

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

Tailored requirements for low value facilities

7.7 Clauses 7.1–7.6 do not apply to a low value facility.

Note: When providing a low value facility, subscribers must give users a process to check the balance of the facility and either a receipt or a mechanism for users to check their transaction history: see clause 5.9.

Tailored requirements for anonymous facilities

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

8 Mandatory consumer warning

8.1 If:

(a) a passcode is required to perform transactions, and

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

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

Chapter C: Liability

Key points

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

- unauthorised transactions, and
- system or equipment malfunction.

9 Scope

9.1 This Chapter applies in addition to, and is separate from, any other processes or rights available through a card scheme's chargeback rules.

Transactions not authorised by a user

9.2 This Chapter applies to unauthorised transactions.

9.3 An unauthorised transaction does not include any transaction that is performed by a user themselves or by anyone who performs a transaction with the knowledge and consent of a user.

Tailored requirements for low value facilities

9.4 This Chapter does not apply to a low value facility.

Note: A subscriber that provides a low value facility must tell users whether the subscriber provides a process to report the loss, theft or misuse of a device or breach of passcode security: see clause 4.8.

10 When holder is not liable for loss

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

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

(b) a device, identifier or passcode that is forged, faulty, expired or cancelled,

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

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

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

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

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

10.4 In a dispute about whether a user received a device or passcode:

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

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

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

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

11 When holder is liable for loss

11.1 If clause 10 does not apply, a holder may only be made liable for losses arising from an unauthorised transaction regulated by this Code in the circumstances specified in clause 11.

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

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

(b) the holder is not liable for the portion of losses:

(i) incurred on any one day that exceeds any applicable daily transaction limit,

(ii) incurred in any period that exceeds any applicable periodic transaction limit,

(iii) that exceeds the balance on the facility, including any pre-arranged credit, or

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

Note: A breach of the passcode security requirements in itself is not sufficient to make a consumer liable for loss from an unauthorised transaction. The subscriber must prove on the balance of probability that the user's breach *contributed* to the loss.

11.3 Where:

(a) more than one passcode is required to perform a transaction, and

(b) a subscriber proves that a user breached the passcode security requirements in clause 12 for one or more of the required passcodes, but not all of the required passcodes,

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

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

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

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

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

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

(ii) when the security compromise was reported to the subscriber, but

(b) is not liable for any portion of the losses:

(i) incurred on any one day that exceeds any applicable daily transaction limit,

(ii) incurred in any period that exceeds any applicable periodic transaction limit,

(iii) that exceeds the balance on the facility, including any pre-arranged credit, or

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

Note: A holder may be liable under clause 11.5 if they were the user who contributed to the loss, or if a different user contributed to the loss.

Effect of charges

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

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

Other situations—Limited liability

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

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

(b) the balance of the facility or facilities that the subscriber and the holder have agreed can be accessed using the device and/or passcode, including any prearranged credit, or

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

Proof that a user contributed to losses

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

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

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

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

Discretion to reduce liability

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

(a) prevailing industry practice regarding reasonable transaction limits,

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

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

Relationship to credit card, scheme debit card and charge card schemes

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

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

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

12 Passcode security requirements

Passcode security

12.1 Clause 12 applies where one or more passcodes are needed to perform a transaction.

12.2 A user must not:

(a) voluntarily disclose one or more passcodes to anyone, including a family member or friend,

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

(i) carried with a device, or

(ii) liable to loss or theft simultaneously with a device,

unless the user makes a reasonable attempt to protect the security of the passcode, or

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

Note: If a user discloses a passcode under clause 12.2(a), without having the benefit of an exception in clause 12.8 or 12.9, and the subscriber can prove on the balance of probability that the consumer contributed to a loss by breaching the passcode security requirements, the subscriber is not required under this Code to indemnify the user for that loss. See clause 11.

12.3 For the purpose of clauses 12.2(b)–12.2(c), a reasonable attempt to protect the security of a passcode record includes making any reasonable attempt to disguise the passcode within the record, or prevent unauthorised access to the passcode record, including by:

(a) hiding or disguising the passcode record among other records,

(b) hiding or disguising the passcode record in a place where a passcode record would not be expected to be found,

(c) keeping a record of the passcode record in a securely locked container, or

(d) preventing unauthorised access to an electronically stored record of the passcode record.

This list is not exhaustive.

12.4 A user must not act with extreme carelessness in failing to protect the security of all passcodes where extreme carelessness means a degree of

carelessness that greatly exceeds what would normally be considered careless behaviour.

Note 1: An example of extreme carelessness is storing a user name and passcode for internet banking in a diary, computer or other personal electronic device that is not password protected under the heading 'Internet banking codes'.

Note 2: For the obligations applying to the selection of a passcode by a user, see clause 12.5.

12.5 A user must not select a numeric passcode that represents their birth date, or an alphabetical passcode that is a recognisable part of their name, if a subscriber has:

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

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

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

(a) at the time of selecting a passcode,

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

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

12.7 The onus is on the subscriber to prove, on the balance of probability, that it has complied with clause 12.6.

12.8 Where a subscriber expressly authorises particular conduct by a user, either generally or subject to conditions, a user who engages in the conduct, complying with any conditions, does not breach the passcode security requirements in clause 12.

12.9 Where a subscriber expressly or implicitly promotes, endorses or authorises the use of a service for accessing a facility (for example, by hosting an access service on the subscriber's electronic address), a user who discloses, records or stores a passcode that is required or recommended for the purpose of using the service does not breach the passcode security requirements in clause 12.

12.10 For the purposes of clause 12.9, a subscriber is not taken to have implicitly promoted, endorsed or authorised the user's use of a particular service merely because the subscriber has chosen to use the service for its own purposes or has not actively prevented a user from accessing a service.

Note 1: For example, if a subscriber permits users to give their passcode(s) to an account aggregator service offered by the subscriber or an associated company, a user who discloses their passcode(s) to the service does not breach the passcode security requirements in clause 12.

Note 2: For example, if a subscriber permits the storage of passcodes in an electronic folder in the user's computer, a user who stores their passcode(s) in this way does not breach the passcode security requirements in clause 12.

13 Passcode security guidelines

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

13.2 Guidelines under this clause must:

(a) be consistent with clause 12,

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

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

Note: Subscribers must provide a process for users to report the loss, theft or misuse of a device or passcode: see clause 17. Subscribers must include on or with statements, at least annually, a summary of the passcode security guidelines under clause 13: see clause 8.

14 Liability for loss caused by system or equipment malfunction

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

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

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

(a) correcting any errors, and

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

15 Network arrangements

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

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

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

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

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

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

15.3 Where a merchant acquirer:

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

(b) forms the view,

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

15.4 A subscriber that is informed of an incorrect transaction under clause 15.3 must investigate the report and make any correction to a facility it considers appropriate.

15.5 A subscriber that makes a correction under clause 15.4 must:

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

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

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

16 Audit trails

Subscribers must be capable of producing audit trails

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

17 Reporting and investigating unauthorised transactions, loss, theft, etc.

Process for reporting unauthorised transactions, loss, theft, etc.

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

(a) unauthorised transactions,

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

(c) breach of passcode security.

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

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

17.3 A subscriber must accept a report under this Code of an unauthorised transaction if it receives the report within 6 years from the day that the user first became aware, or should reasonably have become aware, of the unauthorised transaction.

Note: The limitation period relating to reporting unauthorised transactions under Chapter C of this Code applies separately to any limitation periods for reporting disputed transactions under a card scheme's chargeback rules. A subscriber cannot refuse to investigate an unauthorised transaction just because the time limit for requesting a chargeback has expired.

17.4 If a user reports the loss, theft or misuse of a device or breach of passcode security, the liability of the holder for unauthorised transactions is limited by Chapter C of this Code.

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

Note: If a user cannot access the process for reporting unauthorised transactions, loss or theft due to an issue within the user's control, this clause does not apply. For example, if a user cannot access the process because they run out of credit on their mobile phone, this clause does not apply.

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

(a) does not have to be in writing, but

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

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

Process for investigating a report of an unauthorised transaction

17.7 If a user reports an unauthorised transaction, the subscriber must make reasonable efforts to obtain from the user the following information:

(a) the type of facility,

(b) where relevant, an identifier,

(c) the type of device and/or passcode used to perform the transaction,

(d) the name and address of the holder,

(e) the name of other user(s),

(f) whether a device used to perform the transaction was signed by the user,

(g) whether a device was lost, stolen or misused or the security of a passcode was breached, and if so:

(i) the date and time of the loss, theft or misuse of the device, or breach of passcode security,

(ii) the date and time the loss, theft or misuse of the device, or breach of passcode security, was reported to the subscriber, and

(iii) the date, time and method of reporting the loss, theft or misuse of the device, or breach of passcode security, to the police,

(h) where one or more passcodes were required to perform transactions, whether the user recorded the passcode(s), and if so:

(i) how the user recorded the passcode(s),

(ii) where the user kept the record, and

(iii) whether the record was lost or stolen, and, if so, the date and time of the loss or theft,

(i) where one or more passcodes were required to perform transactions, whether the user had disclosed the passcode(s) to anyone,

(j) details of where and how the loss, theft or misuse of a device, or breach of passcode security, occurred (for example, housebreaking, stolen wallet),

(k) details of the transaction to be investigated, including:

(i) a description,

(ii) the date and time,

(iii) the amount, and

(iv) the type and location of electronic equipment used,

(l) details of any surrounding circumstances,

(m) any steps taken by the user to ensure the security of any device or passcode(s) needed to perform transactions that the user considers relevant to the liability of the holder, and

(n) details of the last authorised transaction performed using the facility.

17.8 A subscriber that is subject to Appendix A to this Code must comply with clause 17.7 only to the extent that the information required under that clause is relevant and available.

17.9 Where a subscriber that is subject to Appendix A to this Code has made reasonable efforts to obtain from a user the information set out in clause 17.7, and the user has not cooperated, a subscriber is entitled to use the fact that the user has not cooperated as a relevant fact in any decision.

17.10 A subscriber must respond to requests for information from other subscribers within 15 days unless there are exceptional circumstances.

18 Timeframes and the subscriber's response

Timeframes

18.1 Within 21 days of receiving a report of an unauthorised transaction, a subscriber must:

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

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

18.2 Unless there are exceptional circumstances, a subscriber must complete its investigation within 45 days of receiving the report of an unauthorised transaction.

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

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

Explaining the outcome of a report of an unauthorised transaction

18.4 A subscriber must tell a user who reports an unauthorised transaction:

(a) the outcome of the report, and

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

18.5 Where a subscriber is subject to Appendix A to this Code and decides that a user is partly or wholly liable for a transaction under Chapter C of this Code, the subscriber must:

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

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

18.6 If a report of an unauthorised transaction is settled to the complete satisfaction of a user and the subscriber within 5 business days, the subscriber is not required to advise the user in writing of the outcome of the report, unless the user requests a written response.

18.7 If a report of an unauthorised transaction is not settled to the complete satisfaction of a user and the subscriber within 5 business days, the information in clause 18.4 must be given in writing.

Note: Chapter F and Appendix A to this Code set out requirements relating to subscribers' handling of 'complaints'. For the avoidance of doubt, reports of unauthorised transactions under this Code and disputed transactions under a chargeback process are not 'complaints' for the purposes of Chapter F and Appendix A to this Code: see ASIC Regulatory Guide 271 *Internal dispute resolution* (RG 271) at RG 271.33(d). However, a 'complaint' is made if the user raises separate issues related to the transaction that meet the definition of a complaint, or expresses dissatisfaction with the outcome or handling of the unauthorised or disputed transaction.

19 Tailored requirements for disputed transactions covered by card scheme rules

19.1 If a subscriber decides to resolve a report of a disputed transaction relating to a credit card, scheme debit card or charge card by exercising its rights under the rules of the card scheme:

(a) the timeframes under the rules of the scheme apply instead of the timeframes in clauses 18.1–18.2,

(b) clause 17.10 does not apply—rather, if the subscriber is not able to resolve the disputed transaction within 60 days, it must give the user:

(i) the reason for the delay,

(ii) updates on progress with the disputed transaction once every 2 months, and

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

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

(i) the relevant timeframes, and

(ii) when the user can reasonably expect a decision, and

(d) the subscriber must:

(i) suspend the holder's obligation to pay any amount that is the subject of the disputed transaction and any credit and other charges related to that amount, until the disputed transaction is resolved, and

(ii) inform the holder of this.

Chapter D: Conduct

Key points

This Chapter requires subscribers to:

- comply with minimum expiry date requirements for products that have expiry dates,
- ensure the security of deposits, and
- prohibit the merchant from holding a user's passcode as part of a book up arrangement.

This Chapter also:

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

20 Minimum expiry dates

Minimum expiry dates

20.1 If a facility:

(a) is not reloadable, and

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

the expiry date must be at least 12 months from the date the user activates the facility, unless the holder is entitled to a refund of the funds or value remaining on the facility at the expiry date.

20.2 If a facility:

(a) is reloadable, and

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

the expiry date must be at least 12 months from the date the user last reloads the facility, unless the holder is entitled to a refund of the funds or value remaining on the facility at the expiry date.

Note 1: For example, a Christmas Club account does not have to comply with clause 20.1 if the subscriber refunds the balance of the account to the holder when the account is closed.

Note 2: Facility expiry dates must comply with the Australian Consumer Law, where applicable. This means, for example, that some facilities may be required to be redeemable for at least 3 years. (See Division 3A of the Australian Consumer Law in Schedule 2 to the *Competition and Consumer Act 2010*.)

Conditions

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

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

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

20.4 If a device is needed to perform transactions:

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

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

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

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

21 Deposits using electronic equipment

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

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

22 Book up arrangements

22.1 If a subscriber and a merchant have a merchant agreement, the agreement must prohibit the merchant from holding a user's passcode as part of a book up arrangement.

23 Electronic communication

23.1 If this Code requires a subscriber to give a user any information under this Code, the subscriber can give the information electronically by:

(a) sending the information by a form of electronic communication nominated by the user,

(b) notifying the user that the subscriber has made the information available electronically, or

(c) another manner agreed with the user,

if the following conditions are met:

(d) the subscriber must provide an effective and convenient process for users to update their contact details,

(e) it must be easy for users to retrieve, read and store the information,

(f) if information is given by notifying a user that the information is available electronically:

(i) the information must be available electronically in that manner (***relevant electronic manner***) for a reasonable period,

(ii) unless the user has agreed to receive information, or information of that type, in that manner—the subscriber must have given the user at least 7 days' notice that it may use the relevant electronic manner to make the information, or information of that type, available to the user unless the user elects, by a means reasonably specified in the notice, not to receive information in that manner, and

(iii) the user must not have made an election referred to in clause 23.1(f)(ii), and

(g) the user must be able to request a paper copy of the information for 7 years from the time the information is given.

23.2 If a subscriber provides a facility designed exclusively for electronic use, and this Code requires the subscriber to give a user any information under this Code, the subscriber can give the information electronically by:

(a) sending the information using electronic communication,

(b) using electronic communication to notify the user that the information is available electronically, or

(c) another manner agreed with the user,

if the following conditions are met:

(d) the subscriber must clearly disclose the following matters before the user first performs a transaction using the facility:

(i) that information will be given electronically and paper copies will not be available, and

(ii) if clause 23.2(a) or 23.2(b) applies, that the subscriber will use that method of communication,

(e) it must be easy for users to retrieve, read and store the information,

(f) the information must be made available electronically by the subscriber for a reasonable period, and

(g) the subscriber must provide an effective and convenient process for users to update their contact details.

24 Privacy

24.1 The following guidelines are provided to help a subscriber interpret the Australian Privacy Principles, or any statutory privacy principles that replace the Australian Privacy Principles in the future, and apply them to transactions:

(a) Where a subscriber may use a surveillance mechanism (for example, visual or sound recording) to monitor transactions, the subscriber must notify users before the commencement of each transaction or session of transactions that the transaction(s) may be recorded by a surveillance mechanism, and explain the nature of the surveillance.

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

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

(i) a complete identifier, or

(ii) a user's name or address.

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

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

(ii) give the privacy policy to users on request.

Note: For example, a subscriber can comply with clause 24.1(d) by putting its privacy policy on its website.

Chapter E: Additional conduct requirements for ADIs

Key points

This Chapter explains the procedures for:

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

25 Scope and definitions

Scope

25.1 This Chapter applies to subscribers that are authorised deposit-taking institutions (ADIs) except ADIs that are providers of purchased payment facilities as designated by the Australian Prudential Regulation Authority.

Definitions

25.2 In this Chapter:

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

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

direct entry means a direct debit or direct credit as defined in the BECS Procedures

direct entry user means a person who issues credit or debit payment instructions using the BECS Procedures

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

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

Note: The definition of mistaken internet payment is intended to relate to typographical errors when inputting an identifier or selecting the incorrect identifier from a list. It is not intended to cover situations in which the user transfers funds to the recipient as a result of a scam.

periodical payments means 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

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

- the facility is purchased by a person from another person,
- the facility can be used to make payments up to the amount that from time to time is available for use under the conditions that apply to the facility,
- those payments are to be made by the provider of the facility or by a person acting under an arrangement with the provider (rather than by the user of the facility), and
- the facility is not covered by a declaration under subsection 9(3) of the *Payment Systems (Regulation) Act 1998*.

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

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

regular payments means direct debit arrangements, direct credit arrangements and periodical payments

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

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

26–36 Mistaken internet payments

26 Disclosure

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

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

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

27 On-screen warning

27.1 A subscriber must clearly warn users to check that the BSB number or identifier are correct, and include a warning to the effect that:

(a) if the user enters or selects an incorrect BSB number or identifier, funds may be sent to the wrong account and it may not be possible to recover funds from an unintended recipient, and

(b) if the subscriber does not match account names and identifiers to process payments, the names and identifiers will not be matched, verified or checked.

27.2 The warning required under clause 27.1 must, where practicable, be delivered:

(a) on-screen,

(b) when a user is performing a transaction using a pay anyone banking facility involving the use of a BSB and account number, and

(c) before the transaction is finally confirmed, at a time when the user can cancel the transaction or correct the error.

Note: Clause 27.2(b) limits the application of the requirements in clause 27.1 to transactions using pay anyone banking facilities involving the use of a BSB and account number. The requirements in clauses 27.1 and 27.2 do not apply to transactions using a pay anyone banking facility involving the use of a PayID.

28 Reporting

28.1 A subscriber must have an effective and convenient process for users to report mistaken internet payments.

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

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

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

29 ADIs must investigate

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

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

(a) the sending ADI must, as soon as reasonably possible and by no later than 5 business days from the time of the user's report of a mistaken internet payment, send the receiving ADI a request for the return of the funds, and

(b) the receiving ADI must within 5 business days of receiving the sending ADI's request:

(i) acknowledge the request by the sending ADI for the return of funds, and

(ii) advise the sending ADI whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

Note: Industry best practice on what amounts to 'as soon as reasonably possible' (in clause 29.2(a)) is for the sending ADI to commence the process within 2 business days. However, the precise duration of 'as soon as reasonably possible' will vary from case to case depending on the circumstances of the mistaken internet payment.

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

29.4 Both the sending ADI and receiving ADI must keep records that are sufficient to demonstrate the steps they took to comply with the mistaken internet payment obligations in this Code.

Note 1: The purpose of the record-keeping obligation in clause 29.4 is to ensure that adequate records (to the extent permitted by law and other frameworks, such as the external dispute resolution scheme's terms of reference) are available to:

(a) the external dispute resolution scheme when considering a dispute relating to the sending ADI's conduct, and

(b) ASIC, should it exercise its monitoring powers under clause 45.1 of this Code.

Note 2: ASIC expects that ADIs will be guided by the mistaken internet payments obligations in this Code in determining what records to create and maintain.

Note 3: Subscribers also have obligations under the *Privacy Act 1988*, which affect what information about individuals they can collect, how they can collect that information, how long that information can be retained and what information they can disclose.

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

30.1 The process in clauses 30.2–30.4 applies where a user reports a mistaken internet payment within 10 business days of making the payment, and the sending ADI is satisfied that:

(a) a mistaken internet payment has occurred, and

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

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

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

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

31 Process where sufficient funds are available and report is made between 10 business days and 7 months

31.1 The process in clauses 31.2–31.6 applies where a user reports a mistaken internet payment between 10 business days and 7 months after making the payment, and:

(a) the sending ADI is satisfied that a mistaken internet payment has occurred, and

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

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

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

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

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

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

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

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

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

32.1 The process in clauses 32.2–32.4 applies where a user reports a mistaken internet payment more than 7 months after making the payment, and:

(a) the sending ADI is satisfied that a mistaken internet payment has occurred, and

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

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

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

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

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

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

33 Relationship with Code of Operation for recovery of debts from customer nominated bank accounts

33.1 Where the unintended recipient of a mistaken internet payment is receiving Services Australia income support payments or Department of Veterans' Affairs payments, the receiving ADI must recover the funds from the unintended recipient in accordance with the *Code of Operation: Recovery of debts from customer nominated bank accounts in receipt of Services Australia income support payments or Department of Veterans' Affairs payments* (Code of Operation).

34 Process where sufficient funds are not available

34.1 Clause 34.2 applies where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient funds available at that time in the account of the unintended recipient to the full value of the mistaken internet payment.

34.2 The receiving ADI must exercise discretion, based on an appropriate weighing of interests of both the sending consumer and unintended recipient and information reasonably available to it about the circumstances of the mistake and the unintended recipient, in deciding whether it should:

(a) pursue the return of funds to the total value of the mistaken internet payment,

(b) pursue the return of funds representing only a partial amount of the total value of the mistaken internet payment, or

(c) not pursue any return of funds (whether partial or total).

Note 1: The receiving ADI's discretion is not unfettered but, rather, is to be guided by the receiving ADI's consideration of a range of relevant factors that assist the receiving ADI in appropriately and reasonably weighing the interests of the sending consumer against those of the unintended recipient. ASIC expects an overarching factor in this exercise of discretion will be that it should generally be accepted that an unintended recipient should not consider themselves entitled to funds that are not theirs.

Note 2: The receiving ADI is not permitted to exercise discretion under clause 34.2 if its investigations show that the total amount of the mistaken internet payment is available at the time in the unintended recipient's account. In such cases, the procedures in clauses 30, 31 and 32 apply.

34.3 The same processes set out in clauses 30, 31 and 32 apply (as the case may be, depending on how much time has elapsed between the mistaken internet payment and the consumer's reporting of it) to instances in which there are not sufficient funds in the unintended recipient's account, as if any reference in those clauses to the availability of sufficient funds were to be read as insufficient funds.

34.4 If, in response to the report of a mistaken internet payment, the receiving ADI determines it is necessary to exercise its discretion in accordance with clause 34.2(a), the receiving ADI must use reasonable endeavours to retrieve the funds from the unintended recipient for return to the holder (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

34.5 Factors that may guide the receiving ADI's exercise of discretion in clause 34.2 may include, but are not limited to:

(a) the financial impact of a return of funds on the unintended recipient,

(b) whether the return of funds would result in an overdrawing of the unintended recipient's account where the recipient's account was not overdrawn before the mistaken internet payment),

(c) the perceived likelihood of ever successfully achieving a return of the total amount of funds,

(d) the desire for all parties (that is, the sending consumer, the receiving ADI and the unintended recipient) to have certainty about timing for conclusion of the process,

(e) the impact that the passage of time has had on the receiving ADI's ability to distinguish the mistakenly paid funds from funds to which the unintended recipient is entitled,

(f) whether the return of some or all of the funds would be inconsistent with any other Commonwealth, state or territory laws, and

(g) the need to limit excessive interaction with the unintended recipient.

Note 1: The factors in clauses 34.5(a)–34.5(g) are intended as guidance only. They are neither an exhaustive list nor a 'safe harbour' for the subscriber and are not necessarily required in each case. Nor do they necessarily have standing in isolation from other factors. Relevant factors required for the receiving ADI's consideration in exercising its discretion will depend on the individual circumstances of each case.

Note 2: Examples relevant to clause 34.5(a) include, but are not necessarily limited to, whether the return of funds would be inconsistent with provisions in the *Social Security (Administration) Act 1999* or with the Code of Operation or would put the unintended recipient into a position of financial hardship that they were not in before the mistaken internet payment.

34.6 Factors that may guide the receiving ADI in knowing whether it has used reasonable endeavours under clause 34.4 may include, but are not limited to and are not necessarily required to include (depending on the individual circumstances):

(a) whether the unintended recipient is responsive to contact from, and requests made by, the receiving ADI,

(b) how many times the receiving ADI has attempted to make contact with the unintended recipient, and through which channels,

(c) how many times the receiving ADI has attempted to recover the funds,

(d) whether the unintended recipient is willing and able to commit to a practical repayment plan, if required,

(e) whether the unintended recipient's account is closed, and

(f) the desire for all parties (i.e. the sending consumer, the receiving ADI and the unintended recipient) to have certainty about timing for conclusion of the process.

Note 1: Relevant factors for clauses 34.5–34.6 will likely differ from case to case depending on the particular circumstances.

Note 2: The factors in clauses 34.6(a)–34.6(f) are intended as guidance only. They are neither an exhaustive list nor a 'safe harbour' for the subscriber and are not necessarily required in each case or have standing in isolation from other factors. Relevant factors required for the receiving ADI's consideration in determining whether it has made reasonable endeavours will depend on the individual circumstances of each case.

35 Sending ADI must inform user of outcome and right to complain

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

(a) in writing, and

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

35.2 The sending ADI's written communication under clause 35.1(a) must include details of the consumer's right to complain to the sending ADI about how the report of the mistaken internet payment was dealt with.

36 Complaints about mistaken internet payments

36.1 A user who reports a mistaken internet payment can complain to the sending ADI about how the report is dealt with, including that the sending ADI:

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

(b) has not complied with the processes and timeframes set out in clauses 26–35.

36.2 A sending ADI that receives a complaint under clause 36.1:

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

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

Note: Subscribers cannot require a user who is their customer to raise a complaint with another party to a shared electronic payments network: see clause 15.2.

36.3 If the user is not satisfied with the outcome of a complaint under clause 36.1, the user must be able to complain to AFCA about the sending ADI.

36.4 Both the sending ADI and the receiving ADI must cooperate with AFCA, including complying with any decision of AFCA (for example, about whether a mistaken internet payment did in fact occur).

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

36.5 Non-cooperation by the receiving ADI or the unintended recipient is not a relevant consideration in assessing whether the sending ADI has complied with its obligations under this Code.

37 Listing and switching

Listing service—Current ADI

37.1 A holder seeking to switch to a different ADI can ask their current ADI to provide a listing service.

37.2 If a holder requests a listing service under clause 37.1, their current ADI must give the holder lists of their:

(a) direct debit arrangements,

(b) direct credit arrangements, and

(c) periodical payments

for the previous 13 months.

37.3 The lists of direct debit arrangements and direct credit arrangements under clauses 37.2(a)–37.2(b) must include all of the following information:

(a) the direct entry user identity,

(b) the name of the direct entry user,

(c) the name of the remitter,

(d) the unique lodgement reference,

(e) the last payment date,

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

(g) the amount of the transaction.

37.4 The list of periodical payments under clause 37.2(c) must include all of the following information:

(a) the BSB (if applicable) 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.

37.5 Where, for a periodical payment, a duplicate lodgement reference is used for the same direct entry user identity, the list of periodical payments under clause 37.2(c) must include the most recent payment date for the arrangement.

37.6 If a holder requests a listing service under clause 37.1, their current ADI must give the holder instructions to help the holder identify their own pay anyone banking facility payments.

37.7 Subscribers must give the lists and information under clauses 37.2–37.6 as soon as practicable, and no later than 5 days after the request.

37.8 An ADI that provides a listing service under clause 37.2 must, if relevant, advise the holder that:

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

(b) some cancelled arrangements may appear on the lists.

Switching service—New ADI

37.9 When opening a personal transaction account for a holder who is seeking to switch from another ADI, an ADI must give the holder relevant information to help them make the switch, including informing the holder of their ability to assist in the switching process.

37.10 An ADI must assist a holder who is switching from another ADI. This assistance must include, if requested by the holder, a customised switching service, which must incorporate an industry standardised 'change of account' letter template for the holder to give to organisations with which they have arrangements for direct debits, direct credits or periodical payments.

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

37.12 If a holder requests a switching service under clause 37.11, their new ADI must:

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

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

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

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

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

Listing and switching services

37.15 A holder seeking to switch to a new ADI may ask the new ADI to obtain from their current ADI a list of all the holder's:

(a) direct debit arrangements,

(b) direct credit arrangements, and

(c) periodical payments currently in effect

for the previous 13 months.

Note: This listing service does not apply to scheme credit arrangements, scheme debit arrangements, BPAY transactions and pay anyone banking facility transactions.

37.16 If a holder requests a listing service under clause 37.15, the new ADI must give the holder information to help the holder identify their own BPAY payments, pay anyone banking facility payments, and any scheme debit card or scheme credit card arrangements.

37.17 The list of direct debit arrangements and direct credit arrangements provided by a current ADI under clauses 37.15(a)–37.15(b) must include all of the following information:

(a) the direct entry user identity,

(b) the name of the direct entry user,

(c) the name of the remitter,

(d) the unique lodgement reference,

(e) the last payment date,

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

(g) the amount of the transaction, and

(h) the frequency (if known).

37.18 The list of periodical payments under clause 37.15(c) must include all of the following information:

(a) the BSB (if applicable) 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.

37.19 Where, for a periodical payment, a duplicate lodgement reference is used for the same direct entry user identity, the list of periodical payments under clause 37.15(c) must include the most recent payment date for the arrangement.

37.20 Within 3 business days of receiving a request under clause 37.15, the new ADI must request the list of regular payments from the current ADI. If it is satisfied as to the identity of the requesting holder, the current ADI must provide the list of regular payments to the new ADI within 5 business days of receiving the request from the new ADI. A current ADI, acting with due care and skill, is not liable to the holder in relation to the failure to provide a list of all regular payments.

37.21 Within 5 days of receiving the holder's list of regular payments from the current ADI, the new ADI must:

(a) provide the list to the holder,

(b) offer to assist the holder to identify which of the direct debit arrangements and direct credit arrangements on the list they wish to transfer to the new ADI,

(c) after receiving the holder's consent, notify the relevant direct entry user's ADI of the changed account details within 2 business days of the holder's instruction in clause (b),

(d) offer to assist the holder to identify whether they wish to cancel any of the regular payments on the list, and

(e) after receiving the holder's consent, notify the relevant direct entry user's ADI of the cancellation within 2 business days of the holder's instructions in clause (d).

Note: The switching service in clause 37.21does not apply to periodical payments.

37.22 When a direct entry user's ADI receives information about a holder's changed account details from a new ADI, the ADI must forward the relevant information to the direct entry user within 3 business days. The direct entry user's ADI must take reasonable steps, such as through its contractual arrangements with the direct entry user, to ensure the direct entry user:

(a) processes the changed details promptly, and

(b) notifies the customer that the notice of changed details has been processed.

37.23 An ADI that provides this listing and switching service must advise the holder that:

(a) 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),

(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 banking facility payments, scheme debit card arrangements and scheme credit card arrangements,

(g) the holder is responsible for switching their own pay anyone banking facility payments by re-entering their payments into their new online banking account, and

(h) the 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.

Chapter F: Complaints

Key points

This Chapter:

- requires subscribers to maintain internal dispute resolution procedures that comply with Australian Standard AS/NZS 10002:2014 *Guidelines for complaint management in organizations* consistent with RG 271,
- imposes a limitations period for complaints and timeframes for resolving complaints,
- sets out procedures for dealing with complaints, and
- includes tailored requirements for complaints about a subscriber that is not required to comply with RG 271 and complaints about credit cards, scheme debit cards and charge cards.

38 Scope and definitions

Scope

38.1 A subscriber that is an Australian financial services licensee, unlicensed product issuer, unlicensed secondary seller, Australian credit licensee or credit representative must comply with this Chapter.

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

(a) is not required to comply with this Chapter, and

(b) must comply with Appendix A to this Code.

Definitions

38.3 In this Chapter:

complaint means an expression of dissatisfaction made to or about an organisation, related to its products, services, staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.

Note 1: This is the definition given in AS/NZS 10002:2014 and used in RG 271.

Note 2: Chapter F and Appendix A to this Code set out requirements relating to subscribers' handling of 'complaints'. For the avoidance of doubt, reports of unauthorised transactions, reports of mistaken internet payments under this Code and disputed transactions under a chargeback process are not 'complaints' for the purposes of Chapter F and Appendix A to this Code. (See RG 271.33(d).) However, a 'complaint' is made if the user raises separate issues related to the transaction that meet the definition of a complaint, or expresses dissatisfaction with the outcome or handling of the mistaken internet payment or unauthorised or disputed transaction.

Note 3: Chapter C of this Code sets out the required timeframes for subscribers' investigations into unauthorised transactions and disputed transactions.

39 Compliance with RG 271

39.1 A subscriber that is an Australian financial services licensee, unlicensed product issuer, unlicensed secondary seller, Australian credit licensee or credit representative must have internal dispute resolution procedures that comply with RG 271.

40 Other matters

Limitations period

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

Compensation for non-compliance with this Code

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

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

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

the subscriber, or an external dispute resolution scheme, may decide the subscriber must pay part or all of the amount of a disputed transaction, as compensation, even if the subscriber or external dispute resolution scheme decide the subscriber is not liable under Chapter C.

Note: A decision about a complaint that is neither in favour of nor against the user is not a decision that falls under clause 40.2.

40.3 The amount of any award in favour of a user under clause 40.2 is a matter for the senior management of the subscriber or the external dispute resolution scheme, taking into account all the circumstances.

Note: For example, where a subscriber does not obtain the information required under clause 17.7 or analyse it in accordance with Chapter C, an award of part or all of the disputed amount to the holder may be justified—to compensate the holder for the inconvenience and expense caused to them.

Providing information to external dispute resolution schemes

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

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

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

Chapter G: Administration

Key points

This Chapter:

- sets out when this Code commences,
- gives ASIC a general power to modify the application of this Code,
- requires subscribers to report information about unauthorised transactions, and
- requires ASIC to monitor compliance with this Code and review this Code every 5 years.

41 Transition and commencement

41.1 Subscribers must comply with this Code from 20 March 2013, or from the date they first subscribe if that date is after 20 March 2013.

41.2 A subscriber can choose to comply with this Code at a date earlier than 20 March 2013 that they nominate in writing to ASIC.

41.3 An entity must not describe itself publicly as a subscriber to this Code until it is complying with this Code.

42 Subscription

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

43 Interpretation

43.1 ASIC may issue guidelines interpreting this Code.

43.2 The headings and notes to clauses in this Code do not form part of the Code but may be used to interpret the Code.

44 Modification

Exemptions and declarations by ASIC

44.1 ASIC may, by written instrument:

(a) exempt a subscriber or a class of subscribers from specified clauses of this Code, or

(b) declare that this Code applies to:

(i) a particular transaction or type of transaction,

(ii) a particular facility or class of facility, or

(iii) a subscriber or class of subscribers,

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

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

44.3 Before making an exemption or declaration, ASIC must consult with stakeholders, taking into account practicality.

44.4 Before making an exemption or declaration, ASIC must consider the following:

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

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

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

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

45 Monitoring and periodic review

Compliance monitoring

45.1 ASIC or its agent may undertake targeted monitoring or surveillance of:

(a) subscribers' compliance with specific obligations under this Code, and

(b) matters relevant to subscribers' activities relating to electronic payments.

The focus of compliance monitoring may change from time to time. A subscriber may be required to report information about compliance with specific clauses of this Code as part of targeted compliance monitoring activities.

Note: Clause 45.1(b) is designed to allow ASIC to monitor or exercise oversight in relation to matters regarding a subscriber's activities, other than compliance with Code provisions, to facilitate ASIC's understanding of, for example, emerging trends and adaptation of this Code as necessary.

45.2 ASIC must consult with subscribers before appointing an agent to perform compliance monitoring under clause 45.1.

Review of this Code

45.3 ASIC or its agent must commence a review of this Code within 5 years of the conclusion of each preceding review.

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

(a) subscribers, industry associations and peak representative groups,

(b) federal, state and territory government agencies,

(c) consumer representatives, and

(d) external dispute resolution schemes.

45.5 ASIC must consult with stakeholders before appointing an agent to perform a review of this Code under clause 45.3.

Appendix A: Complaints procedures for subscribers not covered by Chapter F

A1 Scope

A1.1 A subscriber that is an Australian financial services licensee, unlicensed product issuer, unlicensed secondary seller, Australian credit licensee or credit representative must comply with RG 271 and Chapter F of this Code.

A1.2 Other subscribers must instead comply with this Appendix.

A2 Limitations period

A2.1 A subscriber must accept a complaint if it receives the complaint within 6 years from the day that the user first became aware, or should reasonably have become aware, of the circumstances giving rise to the complaint.

A3 Timeframes

A3.1 Within 21 days of receiving a complaint, a subscriber must:

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

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

A3.2 Unless there are exceptional circumstances, a subscriber must complete its investigation within 45 days of receipt of the complaint.

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

A3.3 If a subscriber cannot resolve a complaint within 45 days, it must:

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

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

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

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

A3.4 Where a subscriber is a member of an external dispute resolution scheme, and the rules of the scheme provide that it can accept a complaint if a subscriber has not made a decision within a specified time period, the subscriber must inform the user that they can complain to the scheme on this basis. The subscriber must provide this information no more than 5 business days after the user can complain to the scheme on this basis.

Note 1: Chapter F and Appendix A to this Code set out requirements relating to subscribers' handling of 'complaints'. For the avoidance of doubt, reports of unauthorised transactions and reports of mistaken internet payments under this Code and disputed transactions under a chargeback process are not 'complaints' for the purposes of Chapter F and Appendix A to this Code. (See RG 271.33(d).) However, a 'complaint' is made if the user raises separate issues related to the transaction that meet the definition of a complaint, or expresses dissatisfaction with the outcome or handling of the mistaken internet payment or unauthorised or disputed transaction.

Note 2: Chapter C of this Code sets out the required timeframes for subscribers' investigations into unauthorised transactions and disputed transactions.

A4 Australian standard on complaints handling

A4.1 A subscriber must adopt the definition of complaint under Australian Standard AS/NZS 10002:2014 *Guidelines for complaint management in organizations* (AS/NZS 10002:2014), which is:

> An expression of dissatisfaction made to or about an organization, related to its products, services, staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.

A4.2 A subscriber must have internal dispute resolution procedures that comply with AS/NZS 10002:2014, or its successor, to the extent required by RG 271.

A5 Disclosure

A5.1 A subscriber must explain the procedure for making complaints:

(a) in the terms and conditions for facilities,

(b) in its general documentation, and

(c) on request.

A5.2 If a complaint is not settled to the complete satisfaction of a user and a subscriber within 5 business days, a subscriber must advise the user in writing of its complaints handling procedures.

A6 Complaints procedures

A6.1 A decision about a complaint must be made on the basis of all relevant established facts and not on the basis of inferences unsupported by evidence.

A7 Cooperation between subscribers

A7.1 A subscriber must respond to requests for information from other subscribers within 15 days, unless there are exceptional circumstances.

A8 Explaining the outcome of a complaint

A8.1 A subscriber must tell a user who makes a complaint:

(a) the outcome of the complaint, and

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

A8.2 If a complaint is settled to the complete satisfaction of a user and a subscriber within 5 business days, the subscriber does not have to advise the user in writing of the outcome of the complaint, unless the user requests a written response.

A8.3 If a complaint is not settled to the complete satisfaction of a user and a subscriber within 5 business days, the information in clause A8.1 of this Appendix must be given in writing.

A8.4 If a complaint is not resolved completely in favour of a user, the subscriber must also:

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

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

This information must be in writing.

A8.5 If a subscriber decides that a facility has been incorrectly debited or credited, it must:

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

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

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

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

A9 Compensation for non-compliance with this Code

A9.1 Where a subscriber, its employees or agents do not comply with this Code, and this contributes to:

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

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

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

A9.2 The amount of any award in favour of a user under clause A9.1 is a matter for the senior management of the subscriber or the external dispute resolution scheme, taking into account all the circumstances.

Note: For example, where a subscriber does not obtain the information required under clause 17.7, or analyse it in accordance with Chapter C, an award of part or all of the disputed amount to the holder may be justified—to compensate the holder for the inconvenience and expense caused to them.

A10 Providing information to external dispute resolution schemes

A10.1 Where an external dispute resolution scheme asks a subscriber for information to help it resolve a complaint and the subscriber does not provide the information:

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

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