



ASIC

Australian Securities & Investments Commission

Electronic Funds Transfer Code of Conduct

**As revised by the
Australian Securities & Investments
Commission's EFT Working Group**

**Issued 1 April 2001
Amended 18 March 2002**

Contents

Part A	4
Rules and procedures to govern the relationship between users and account institutions in electronic funds transfers involving electronic access to accounts.....	4
1. Scope and interpretation	4
2. Availability and disclosure of the terms and conditions applicable to EFT transactions	7
3. Changing the terms and conditions of use	8
4. Records of EFT transactions and notice of surcharges.....	9
5. Liability for unauthorised transactions	12
6. Liability in cases of system or equipment malfunction	17
7. Deposits to accounts by funds transfers.....	17
8. Networking arrangements.....	17
9. Audit-trails.....	18
10. Complaint investigation and resolution procedures.....	18
Part B.....	22
Rules for consumer stored value facilities and stored value transactions	22
11. Scope and interpretation	22
12. Availability and disclosure of information and terms and conditions applicable to stored value facilities	24
13. Changing the terms and conditions of use	25
14. Record of available balance.....	26
15. Rights to exchange stored value	26
16. Refund of lost or stolen stored value	27
17. System or equipment malfunction	27
18. Stored value operator's obligations	27
19. Complaint investigation and dispute resolution.....	28

Part C 29

Privacy, electronic communication, administration and review..... 29

20. Interpretation and Multiple Disclosure Obligations 29

21. Privacy 30

22. Electronic communications 30

23. Commencement and administration 32

24. Review 33

Schedule to Code 34

The EFT CODE

Part A

Rules and procedures to govern the relationship between users and account institutions in electronic funds transfers involving electronic access to accounts

1. Scope and interpretation

1.1 (a) Part A of this Code applies to EFT transactions. EFT transactions are funds transfers initiated by giving an instruction, through electronic equipment and using an access method, to an account institution (directly or indirectly) to debit or credit an EFT account maintained by the account institution. Sub clauses 1.3 and 1.4 limit the scope of application of Part A.¹

(b) Part A of the Code governs the rights and duties of account institutions and users (including account holders). It does not directly govern the rights and duties of third parties, such as issuers of access methods who are not account institutions or third parties in an EFT network such as merchants. Account institutions cannot avoid their obligations to users under the Code on the grounds that a third party has caused the failure to meet these obligations.

1.2 A funds transfer is the transfer of value to or from an EFT account (regardless of whether the EFT account has a debit or credit balance before or after the transfer) including between two EFT accounts or between an EFT account and another type of account. Without limitation, the transfer of value may be effected by one or more of the following:

- adjusting one or more account balances;
- transferring currency or a physical payment instrument;
- transferring electronic representations of value (eg digital coins or payment instruments); or
- adjusting amounts of stored value whether recorded on a card or other media (eg loading and unloading stored value).²

1.3 Transaction-type limitation

Part A of this Code does not apply to:

- (a) that part of a funds transfer which is the debiting of and transfer of value from; or
- (b) that part of a funds transfer which is the receipt of value and the crediting of that value to;

an account that is designed primarily for use by a business and established primarily for business purposes.

1.4 Exclusion of some funds transfers involving biller accounts

- (a) Except for clause 7, Part A of this Code does not apply to an account institution in respect of the receiving of value in a funds transfer for the credit of a biller account maintained by the account institution.
- (b) Part A of this Code does not apply to an EFT transaction which is a user-initiated funds transfer from a customer's biller account to the account institution to pay the account institution for goods or services (other than financial services) provided by the account institution to that customer (eg. a debit to the customer's biller account and a credit to an internal account of the account institution).³

1.5 Interpretation

In Part A of this Code:

"access method":

- (a) means a method authorised by an account institution for use by a user and accepted by the account institution as authority for it to act on an instruction given through electronic equipment to debit or credit an EFT account; and
- (b) comprises the use of one or more components including (but not limited to) devices, identifiers, codes or a combination of these; and
- (c) does not include a method requiring the user's manual signature where the comparison of the appearance of that manual signature with a written specimen signature is the principal intended means of authenticating a user's authority to give the instruction (whether or not that means is used in a particular transaction).⁴

"account access service" is a service for the purposes of which either or both of the following apply:

- (a) the user must provide one or more codes to a service provider to enable the service provider or another person to access accounts at an account institution on behalf of the user (for example, an account aggregator service); or
- (b) the user must record or store one or more codes in a manner required by the service provider to facilitate the user, the service provider or another person acting on behalf of the user to access EFT accounts at an account institution using that code or codes (for example, the service provider provides the user with a software wallet to store codes and the wallet is used to access EFT accounts by the user or the service provider).

“account institution” means an institution which:

- subscribes to this Code; and
- maintains EFT accounts for account-holders.⁵

“biller account” is an EFT account maintained by an account institution solely to record amounts owed or paid by its customer in respect of the provision of goods or services to its customer by the account institution.⁶

“code” means information:

- the content of which is known to the user and is intended to be known only to the user or only to the user and the account institution;
- which the account institution requires the user to keep secret; and
- which the user must provide (in any manner) to or through a device or electronic equipment in order to access an EFT account.⁷

“device” means a physical device used with electronic equipment to access an EFT account, for example a card, token or biometric reader.

“EFT account” means an account:

- (a) maintained by an account institution which belongs to an identifiable account holder who is a customer of the account institution; and
- (b) which the account institution permits a user to initiate a funds transfer from or to using an access method through electronic equipment (notwithstanding that there may be a delay between the use of the access method and the debiting or crediting of the account).

In the case of a stored value facility (as defined in Part B), neither the value control record in the facility nor any record held by a stored value operator of the stored value available to be transferred from that stored value facility is an EFT account.⁸

“electronic equipment” includes electronic terminal, computer, television and telephone.

“financial services” includes the lending of money, the provision of credit and a financial service as defined in s.12BA of the *Australian Securities and Investments Commission Act 1989*.

“identifier” means information:

- the content of which is known to the user but not only to the user and which the user is not required to keep secret; and
- which the user must provide (in any manner) to or through a device or electronic equipment in order to access an EFT account.⁹

“institution equipment” means electronic equipment controlled or provided by or on behalf of an account institution to facilitate EFT transactions.

“institution system” means an electronic system, communications system or software controlled or provided by or on behalf of an account institution to facilitate EFT transactions.

“user” means a person authorised by an account institution (and, if the user is not the account holder, also authorised by the account holder) to use an access method to give instructions to the account institution to debit or credit an EFT account and includes an account holder.¹⁰

2. Availability and disclosure of the terms and conditions applicable to EFT transactions

2.1 Account institutions will prepare for their users clear and unambiguous Terms and Conditions applicable to EFT transactions, which reflect the requirements of this Code. The Terms and Conditions are to include a warranty that the requirements of this Code will be complied with. The Terms and Conditions will not provide for or be effective to create liabilities and responsibilities of users, which exceed those set out in this Code.

2.2 Account institutions will provide a copy of the Terms and Conditions:

- (a) to the account holder prior to or at the time of initial use of the access method; and
- (b) at any other time when requested to do so by a user.

The availability of Terms and Conditions is to be publicised by account institutions.

2.3 Account institutions will ensure that, before an access method is used for the first time after issue, the user to whom it is issued has been provided with information on:

- (a) any charges for the issue or use of an access method, separate from activity or other charges applying to the account generally;

- (b) the nature of any restrictions imposed by the account institution on the use of the access method (including any daily transaction limit and other periodic transaction limits which apply to the access method, an account or electronic equipment) and an indication that merchants or other institutions may impose additional restrictions;
- (c) a description of the types of transactions that may be made, and of the accounts that may be accessed, with the access method;
- (d) a description of any credit facility, which may be accessed by the user through electronic equipment using the access method;
- (e) the procedure for reporting the loss, theft or unauthorised use of a device or breach of security of a code (such as a telephone number or other means of reporting outside of normal business hours); and
- (f) the means to activate complaint investigation and resolution processes (including the procedure for querying entries on a periodic statement).

3. Changing the terms and conditions of use

3.1 Account institutions wishing to vary or modify the EFT Terms and Conditions to:

- (a) impose or increase charges relating solely to the use of an access method, or the issue of an additional or replacement access method;
- (b) increase an account holder's liability for losses relating to EFT transactions (subject to the liability limits established elsewhere in this Code); or
- (c) impose, remove or adjust a daily transaction limit or other periodic transaction limit applying to the use of an access method, an account or electronic equipment;

will provide written notification to the account holder, and allow a period of notice of at least 20 days (or, where applicable legislation requires a longer notice period, that longer period) before the change takes effect.

- 3.2 (a) Account institutions will give notice of other changes at the following time:
- (i) in time to comply with any applicable legislative requirements for a particular period of notice in advance of the date the change takes effect;¹¹ or
 - (ii) where there is no such legislative requirement, in advance of the date the change takes effect.
- (b) Account institutions will provide notice of other changes in the manner required by applicable legislation, or if there are no such requirements, in a

manner which is likely to come to the attention of as many account holders as possible.

- 3.3 Advance notice need not be given when changes are necessitated by an immediate need to restore or maintain the security of the system or individual accounts.
- 3.4 Where important, or a sufficient number of cumulative changes so warrant, account institutions will issue a single document providing a consolidation of variations made to the Terms and Conditions.
- 3.5 When account institutions advise account holders of the removal of, or an increase in, a daily transaction limit or other periodic transaction limit, they should, at the same time, advise account holders that the removal of or an increase in that transaction limit may increase account holder liability in the case of unauthorised transactions. This advice is to be clear and prominent.

4. Records of EFT transactions and notice of surcharges

A Receipts

- 4.1 (a) Except where paragraph (b) applies, at the time of an EFT transaction and unless a user specifically elects otherwise, the account institution will ensure a receipt is issued containing all of the following information:
- (i) the amount of the transaction;
 - (ii) the date and time (if practicable) of the transaction;
 - (iii) the type of transaction eg, a “deposit”, “withdrawal”, “transfer”, (symbols may be used only if they are explained on the receipt and easily understood abbreviations may be used);
 - (iv) an indication of the account(s) being debited or credited;
 - (v) data that enable the account institution to identify the customer and the transaction;
 - (vi) where possible, the type and general location of any institution equipment used to make the transaction or a number or symbol that enables that institution equipment to be identified;
 - (vii) in the case of a funds transfer to a merchant in payment for goods or services, the name of the merchant to whom payment was made;
 - (viii) where possible, and where it is not likely to compromise the privacy or security of the user or the account holder, the balance remaining in the account which is debited in the funds transfer (or, in the case of a deposit, the account which is credited).¹²

- (b) If an EFT transaction is conducted by voice communications (including an automated voice response system by telephone), the account institution will ensure that the following information is provided to the user by voice communication at the time of the EFT transaction:
- (i) a receipt number;
 - (ii) the amount of the transaction;
 - (iii) the type of transaction eg. a “deposit”, “withdrawal”, “transfer”;
 - (iv) an indication of the account(s) being debited or credited;
 - (v) in the case of a funds transfer to a merchant in payment for goods or services, the name of the merchant to whom the payment was made;
 - (vi) where possible, and where it is not likely to compromise the privacy or security of the user or the account holder, the balance remaining in the account which is debited in the funds transfer (or, in the case of a deposit, the account which is credited).

Account institutions may choose to provide users with the option to specify at the time of each transaction that a receipt is not required.¹³

- (c) A charge may not be imposed on a user or an account holder for the issuing of a receipt under sub-clauses (a) and (b).
- (d) In an EFT transaction where the user does not use institution equipment or an institution system and does not communicate with the account institution or a person acting on its behalf, the account institution is only obliged to use its best endeavours to meet its obligations under paragraphs (a) and (b).¹⁴

B Periodic statements

- 4.2 (a) Except for those passbook accounts covered by sub-clause (b), for an account to or from which EFT transactions can be made, the account institution will provide a record of account activity at least every six months. Account holders are also to be offered the option of receiving more frequent periodic statements. That option is to be brought to the attention of the account holder at the time the access method is first issued. As well, statements are to be available at the request of the account holder.
- (b) Passbook accounts are exempted for sub-clause (a) where there is no charge for having the passbook updated manually or checking account balances and activity electronically.

[Historical note: EFT Code amended 18 March 2002 by replacing para 4.2. The para formerly read:
 "4.2 For an account to or from which EFT transactions can be made, the account institution will provide a record of account activity at least every six months. Account holders are also to be offered the option of receiving more frequent periodic statements. That option is to be brought to the attention of the account holder at the time the access method is first issued. As well, statements are to be available at the request of the account holder."*]*

- 4.3 Except for statements issued outside the usual statement cycle the statement is to show:
- (a) in respect of each EFT transaction occurring since the previous statement:
 - (i) the amount of the transaction;
 - (ii) the date the transaction was debited or credited to the account;
 - (iii) the type of transaction;
 - (iv) the receipt number, or other means, which will enable the account entry to be reconciled with a transaction receipt;
 - (b) any charges relating solely to the use of an access method (identified as a separate item); and
 - (c) the address, telephone number or other contact details to be used for inquiries concerning the account or to report any errors in the statement;

but a statement issued outside the usual statement cycle is to show as much of the above information as possible.

- 4.4 Account institutions will suggest to account holders that all entries on statements be checked and any apparent error or possible unauthorised transaction be promptly reported to the account institution. This suggestion will be contained on the account statement. Institutions will not seek to restrict or deny account holders their rights to make claims or to attempt to impose time limits on users to detect errors or unauthorised transactions.

C Security advice

- 4.5 Account institutions must include on or with account statements at least annually a clear, prominent and self-contained statement summarising access method security guidelines which are consistent with clause 5 of this Code and which complies with paragraph 5.8(b).

D Notice of surcharges for using "foreign" electronic equipment

- 4.6 An account institutions shall include in its agreements with any person who makes electronic equipment available to a user so that the user may perform an EFT transaction, a requirement that the person disclose to the user (at a time which enables the user to cancel the EFT transaction without cost to the user) the amount of any fee (such as a surcharge) charged by the person for the use of its electronic equipment which will be directly passed on to the user or account holder.¹⁵

5. Liability for unauthorised transactions

A Definition of unauthorised transaction

5.1 This clause deals with liability for transactions which are not authorised by the user. It does not apply to any transaction carried out by the user or by anyone performing a transaction with the user's knowledge and consent.

B No account holder liability in respect of fraudulent or negligent conduct of account institutions' employees or agents; forged, faulty, expired or cancelled access method; losses occurring prior to receipt of access method; or incorrect double debit transactions

5.2 The account holder has no liability for:

- (a) losses that are caused by the fraudulent or negligent conduct of employees or agents of the account institution or companies involved in networking arrangements or of merchants or of their agents or employees;
- (b) losses relating to any component of an access method that are forged, faulty, expired, or cancelled;
- (c) losses that arise from transactions which required the use of any device or code forming part of the user's access method and that occurred before the user has received any such device or code (including a reissued device or code). In any dispute about receipt of a device or code it is to be presumed that the item was not received by the user, unless the account institution can prove otherwise. The account institution can establish that the user did receive the device or code by obtaining an acknowledgment of receipt from the user whenever a new device or code is issued. If the device or code was sent to the user by mail or email, the account institution is not to rely only on proof of delivery to the user's correct address as proof that the device or code was received by that person. Nor will the account institution have any term in the Terms and Conditions which deems a device or code sent to the user at that person's correct address (including an email address) to have been received by the user within a certain time after sending; or
- (d) losses that are caused by the same transaction being incorrectly debited more than once to the same account.

C No account holder liability in respect of unauthorised transactions occurring after notification

5.3 The account holder has no liability for losses resulting from unauthorised transactions occurring after notification to the account institution that any device forming part of the access method has been misused, lost or stolen or that the security of codes forming part of the access method has been breached.

D No account holder liability where it is clear that the user has not contributed to the loss

- 5.4 The account holder has no liability for losses resulting from unauthorised transactions where it is clear that the user has not contributed to such losses.

E Circumstances where the account holder is liable

- 5.5 Where sub-clauses 5.2, 5.3 and 5.4 do not apply, the account holder is liable for losses resulting from unauthorised transactions only as provided in paragraphs (a), (b) and (c).

- (a) Where the account institution can prove on the balance of probability that the user contributed to the losses through the user's fraud or the user's contravention of the requirements in sub-clause 5.6, the account holder is liable for the actual losses which occur before the account institution is notified that a device forming part of the access method has been misused, lost or stolen or that the security of the codes forming part of the access method has been breached, but is not liable for any of the following amounts:
- (i) that portion of the losses incurred on any one day which exceed the applicable daily transaction limit(s);
 - (ii) that portion of the losses incurred in a period which exceeds any other periodic transaction limit(s) applicable to that period;
 - (iii) that portion of the total losses incurred on any account which exceeds the balance of that account (including any prearranged credit);
 - (iv) all losses incurred on any accounts which the account institution and the account holder had not agreed could be accessed using the access method.

Where an access method includes more than one code and the account institution proves that the user contravened the requirements of subclause 5.6 by voluntarily disclosing or by keeping a record of one or more codes but not all the codes in the access method, the account holder is liable under this paragraph only if the account institution also proves on the balance of probability that the user's contravention of sub-clause 5.6 was the dominant contributing cause of the losses.¹⁶

- (b) Where the account institution can prove on the balance of probability that a user has contributed to losses resulting from unauthorised transactions by the user unreasonably delaying notification after becoming aware of the misuse, loss or theft of a device forming part of the access method, or that the security of all the codes forming part of the access method has been breached; the account holder is liable for the actual losses which occur between when the user became aware (or should reasonably have become aware in the case of a lost or stolen device) and when the account institution was actually notified, but is not liable for any of the following amounts:

- (i) that portion of the losses incurred on any one day which exceed the applicable daily transaction limit(s);
 - (ii) that portion of the losses incurred in a period which exceeds any other periodic transaction limit(s) applicable to that period;
 - (iii) that portion of the total losses incurred on any account which exceeds the balance of that account(s);
 - (iv) all losses incurred on any accounts which the account institution and the account holder had not agreed could be accessed using the access method.
- (c) Where a code was required to perform the unauthorised transactions and neither paragraph (a) nor (b) applies, the account holder is liable for the least of:
- (i) \$150 (or such lower figure as may be determined by the account institution); or
 - (ii) the balance of those account(s) (including any pre-arranged credit) from which value was transferred in the unauthorised transactions and which the account institution and the account holder have agreed may be accessed using the access method; or
 - (iii) the actual loss at the time the account institution is notified (where relevant) that the device has been misused, lost or stolen or that the security of the codes has been breached (excluding that portion of the losses incurred on any one day which exceed any applicable daily transaction or other periodic transaction limit(s)).

In determining whether an account institution has proved on the balance of probability that a user has contributed to losses under paragraph (a), all reasonable evidence must be considered, including all reasonable explanations for the transaction occurring.

The fact that the account has been accessed with the correct access method, while significant, will not of itself constitute proof on the balance of probability that the user has contributed to losses through the user's fraud or through the user contravening the requirements in sub-clause 5.6.

In determining whether a user has unreasonably delayed notification under paragraph 5.5(b), the effect on the user of any charges imposed by the account institution relating to the notification or the replacement of the access method must be taken into account.

5.6 Where an access method utilises a code or codes, a user contravenes the requirements of this sub-clause if:

- (a) the user voluntarily discloses one or more of the codes to anyone, including a family member or friend; or

- (b) where the access method also utilises a device, the user indicates one or more of the codes on the outside of the device, or keeps a record of one or more of the codes (without making any reasonable attempt to protect the security of the code records) on the one article, or on several articles, carried with the device or liable to loss or theft simultaneously with the device; or
- (c) where the access method comprises a code or codes without a device, the user keeps a record of all the codes (without making any reasonable attempt to protect the security of the code records) on the one article, or on several articles so that they are liable to loss or theft simultaneously;
- (d) where, after the adoption of this revised Code by the account institution, the account institution permits the user to select or change a code and, immediately before the user's selection or change of the code, specifically instructs the user not to select a numeric code which represents the user's birth date or an alphabetical code which is a recognisable part of the user's name and warns the user of the consequences of such a selection and the user selects such a numeric or alphabetical code; or
- (e) the user acts with extreme carelessness in failing to protect the security of all the codes.¹⁷

Where 5.6(d) applies, the onus will be on the account institution to prove on the balance of probabilities that it gave the specific instruction and warning to the user at the time specified and in a manner designed to focus the user's attention specifically on the instruction and consequences of breaching it. The user means the actual user, taking into account the capacity of the user to understand the warning.¹⁸

- 5.7 (a) Where an account institution expressly authorises particular conduct by a user (either generally or subject to conditions), the engaging in that conduct by the user (within any applicable conditions) is not a contravention of the requirements of sub clause 5.6.
- (b) Where an account institution expressly or impliedly promotes, endorses or authorises the use of an account access service by a user (including by hosting an account access service at the account institution's electronic address), no disclosure, recording or storage of a code by a user that is required or recommended for the purposes of using that account access service is a contravention of the requirements of sub clause 5.6.¹⁹
- 5.8 (a) For the purposes of this clause, a reasonable attempt to protect the security of a code record includes either or both of:
 - (i) making any reasonable attempt to disguise the code(s) within the record; or
 - (ii) taking reasonable steps to prevent unauthorised access to the code record.²⁰
- (b) An account institution in its Terms and Conditions and other communications to its users may provide guidelines for its users on ensuring the security of an access method which are consistent with clause 5 but it must:

- (i) clearly differentiate those guidelines from the circumstances in which an account holder is liable for losses resulting from unauthorised transactions as set out in this clause; and
- (ii) include a statement that an account holder's liability for such losses will be determined under the EFT Code of Conduct rather than the guidelines.

F Notification of the loss, theft or unauthorised use of devices or codes

- 5.9 Account institutions will provide an effective and convenient means by which users can notify a lost or stolen device or unauthorised use of a device or breach of security of a code; facilities such as telephone hot lines are to be available to users at all times, with notice by telephone being an effective notice for limitation of the user's liability. Where such facilities are not available during particular periods any losses occurring during these periods that were due to non-notification are deemed to be the liability of the account institution providing notification is made to the account institution within a reasonable time of the facility again becoming available.
- 5.10 Account institutions will implement procedures for acknowledging receipt of notifications, including telephone notifications, by users of the loss, theft, or unauthorised use of a device or breach of security of a code. Such acknowledgments need not be in writing although they must provide a means by which users can verify that they have made a notification and when such notification was made.

G Unauthorised credit card and charge card account transactions

- 5.11 Where an account holder complains that there is an unauthorised transaction on a credit card account or a charge card account, the account institution shall not hold the account holder liable for losses under clause 5 for an amount greater than the liability the account holder would have to the account institution if the account institution exercised any relevant rights it had under the rules of the credit card or charge card scheme at the time the complaint was made against other parties to that scheme.²¹

H Discretion to reduce account holder's liability where no reasonable daily or periodic transaction limits

- 5.12 (a) This clause applies where a transaction is alleged to be unauthorised and the account institution has not applied a reasonable daily or other periodic transaction limit in respect of that transaction. The reasonableness of a transaction limit is to be determined having regard to prevailing industry practice.
- (b) Where this clause applies, the account institution or an external dispute resolution body may reduce any liability that the account holder has for the unauthorised transaction under sub clause 5.5 by such amount as it considers fair and reasonable having regard to:
- (i) whether the security and reliability of the means used by the account institution to verify that the relevant transaction was authorised by the user adequately protected the account holder from losses in the absence of reasonable daily or other periodic transaction limits protection; and

- (ii) if the unauthorised transaction was a funds transfer that involved drawing on a line of credit accessible by the access method (including drawing on repayments made to a loan account), whether at the time of making the line of credit accessible by the access method, the account institution had taken reasonable steps to warn the account holder of the risk of the access method being used to make unauthorised transactions on that line of credit.²²

6. Liability in cases of system or equipment malfunction

- 6.1 Account institutions will be responsible to their users for loss caused by the failure of an institution system or institution equipment to complete a transaction accepted by an institution system or institution equipment in accordance with the user's instructions.
- 6.2 The account institution is not to deny, implicitly or explicitly, a right to the user to make claims for consequential damage which may arise as a result of a malfunction of an institution system or institution equipment however caused, except, where the user should have been aware that the system or equipment was unavailable for use or malfunctioning, the account institution's responsibilities may be limited to the correction of any errors in the account, and the refund of any charges or fees imposed on the account holder as a result.

7. Deposits to accounts by funds transfers

A Discrepancies between recorded deposits and amounts received

- 7.1 Where, in relation to an EFT transaction which is a deposit of funds to an account, there is a discrepancy between the amount recorded by the electronic equipment or access method as having been deposited and the amount recorded by the account institution as having been received, the account holder will be notified of the difference as soon as possible and will be advised of the actual amount which has been credited to the nominated account.

B Security of deposits at institution equipment

- 7.2 The security of deposits received at institution equipment is the responsibility of the account institution receiving the deposit from the time the transaction at the institution equipment is completed (subject to verification of amount(s) deposited).

8. Networking arrangements

- 8.1 For the purposes of clause 8, parties to the shared EFT system include retailers, merchants, communications service providers, and other organisations offering EFT facilities to users, as well as merchant acquirers and account institutions. Merchant acquirers are the institutions which provide EFT transaction facilities for merchants.

- 8.2 Account institutions may not avoid any obligations owed to their users by reason only of the fact that they are party to a shared EFT system and that another party to the system has actually caused the failure to meet the obligations.
- 8.3 An account institution shall not require its users to raise complaints or disputes in relation to the processing of EFT transactions with any other party to the shared EFT system, or to have those complaints or disputes investigated by any other party to the shared EFT system.
- 8.4 Where a merchant acquirer is advised by another party to the shared EFT system, or forms the view, that a transaction has been debited or credited incorrectly to a particular account, the merchant acquirer will notify the account institution concerned of the situation.

The account institution will then, following any investigation it may undertake pursuant to the advice received from the merchant acquirer, make any correction to a user's account it considers appropriate in the circumstances, and any such correction will be included in the user's account statement subsequently issued in the normal course. The account institution will also notify the account holder as soon as practicable after reversing an incorrect credit.

The account institution will provide to the account holder, upon inquiry, any further details required by the account holder concerning the transaction correction appearing on the account holder's statement.

9. Audit-trails

- 9.1 Account institutions will ensure that their EFT transaction systems generate sufficient records to enable transactions to be traced, checked and where an error has occurred, to be identified and corrected.

10. Complaint investigation and resolution procedures

- 10.1 Account institutions will establish internal complaint handling procedures which comply with Australian Standard AS4269-1995 or any other industry dispute resolution standard or guideline which ASIC declares to apply to this clause.
- 10.2 The account institution shall advise users in their Terms and Conditions, upon request and in their general documentation of the procedures for lodging a complaint.
- 10.3 When a complaint is lodged and is not immediately settled to the satisfaction of both user and account institution the account institution will advise the user, in writing, of the procedures for investigating and handling the complaint.
- 10.4 (a) The account institution's decision in relation to a complaint is to be made on the basis of all relevant established facts and not on the basis of inferences unsupported by evidence.

- (b) Where a user raises a complaint concerning the authorisation of a transaction, the account institution will make reasonable efforts to obtain from the user at least the information outlined in the attached schedule where such information is relevant and available.
- (c) Where a user raises a complaint concerning the authorisation of a transaction or a system or equipment malfunction, the institution must investigate whether there was any system or equipment malfunction at the time of the transaction.

10.5 Within 21 days of receipt of a complaint, the account institution will:

- (a) complete the investigation and advise the user, in writing, of the outcome of the investigation; or
- (b) advise the user, in writing, of the need for more time to complete its investigation.

Unless there are exceptional circumstances, the account institution should complete its investigation within 45 days of receipt of the complaint.²³

10.6 If an account institution is unable to resolve a complaint within 45 days, it must:

- (a) inform the user of the reasons for the delay;
- (b) provide the user with monthly updates on progress with the complaint; and
- (c) specify a date when a decision can be reasonably expected;

unless the account institution is waiting for a response from the user and the user has been advised that the account institution requires such a response.

10.7 If an account institution decides to resolve a complaint concerning a credit card account or a charge card account by exercising its rights under the rules of the credit card or charge card scheme:

- (a) the time limits under the rules of the scheme apply in lieu of the time limits in sub-clause 10.5;
- (b) sub-clause 10.6 applies to the complaint with the following modifications:
 - (i) "60 days" replaces "45 days"; and
 - (ii) "updates once every two months" replaces "monthly updates"; and
- (c) the account institution shall:
 - (i) inform the user, in writing, of those time limits and when a decision can be reasonably expected; and
 - (ii) shall suspend the account holder's obligation to pay any amount which is the subject of the complaint and any credit and other charges related to that amount until the complaint is resolved and inform the account holder of that suspension.

- 10.8 When an account institution is a member of an external dispute resolution scheme, and the scheme's rules provide that a matter may be referred to it if a decision is not made within a specified time period, then the account institution must inform the user that a complaint may be lodged with the scheme no more than 5 business days after the expiry of the relevant time period.
- 10.9 On completing its investigation of a complaint, the account institution will promptly inform the user of:
- (a) the outcome of the investigation;
 - (b) the reasons for the outcome including references to relevant clauses of the Code;
 - (c) except where the complaint has been resolved completely in favour of the user, the further action the user can take in respect of the Code, including the contact details of any external dispute resolution body which the institution belongs to or, if it does not belong to such a body, the contact details for the Consumer Affairs Agency and Small Claims Courts/Tribunals in the consumer's jurisdiction.

Such advice is to be in writing except where the complaint is settled immediately the account institution receives the complaint to the satisfaction of both the user and account institution.

- 10.10 Where as a result of the investigation of a complaint, an account institution decides that the account holder's account has been incorrectly credited or debited, having regard to the provisions of this Code, the account institution will, where appropriate, forthwith adjust the account holder's account (including appropriate adjustments for interest and/or charges) and notify the account holder in writing of the amount with which their account has been debited or credited as a result.
- 10.11 Where on completion of an investigation the account institution decides that the account holder is liable under clauses 5 or 6 of this Code for at least part of the amount of the transaction subject to complaint:
- (a) the account institution is to make available to the account holder copies of any documents or other evidence relevant to the outcome of its investigation including information from any logs or audit trails relating to the transaction; and
 - (b) the account institution must advise the account holder in writing whether there was any system or equipment malfunction at the time of the transaction.
- 10.12 Where:
- (a) the account institution, its employees or its agents fail to observe the applicable complaint investigation and resolution procedures set out in this clause, or fail to determine the allocation of liability in accordance with clauses 5 and 6, or fail to communicate the reasons for that determination by reference to relevant aspects of clauses 5 and 6; and

- (b) the failure contributed to an institution decision on the complaint (including an initial decision) against the account holder, or the failure delayed the resolution of the complaint (including by contributing to the account holder referring the complaint to external dispute resolution);

the account institution or an external dispute resolution body may determine that the account institution is liable for part or all of the amount of the transaction in dispute as compensation for the effects of that decision or delay on the account holder or the user, even if the account institution or external dispute resolution body ultimately determine that the institution was not liable under clauses 5 and 6.²⁴

10.13 Where the account institution:

- (a) decides to resolve a complaint concerning an unauthorised transaction under sub-clause 5.2, 5.3, 5.4 or paragraph 5.5(c); and
- (b) within 7 business days of receipt of the complaint, adjusts the account holder's accounts pursuant to sub-clause 10.10 to give effect to that decision and provides the user and account holder with the information required by sub-clauses 10.9 and 10.10;

the account institution is not required to comply with sub-clauses 10.3, 10.5, or 10.11 in respect of the complaint concerning the unauthorised transaction.²⁵

10.14 The account institution is to provide for the recording of complaints and their resolution so that aggregate data on the type, frequency and resolution of such complaints can be made available as required in Part C of this Code and so that account institutions can identify and address systematic problems.

Part B

Rules for consumer stored value facilities and stored value transactions

11. Scope and interpretation

11.1 Part B of this Code applies to the use by a person of a stored value facility but does not apply to any use of a stored value facility designed primarily for use by a business and acquired primarily for business purposes.

If an aspect of a use of a stored value facility is an EFT transaction to which Part A of this Code applies, Part B of this Code does not apply to that aspect of the use of the stored value facility.²⁶

11.2 In this Part:

“authorised deposit-taking institution” has the same meaning as in the *Banking Act 1959* (Cth).

“issuer” means an entity, which, in the course of its business, provides a stored value facility to a user.

“payment facilitator” means an entity, which is contractually bound to a user to facilitate the payments the user initiates by using a stored value facility.²⁷

“stored value” means a representation of value that:

- (a) is intended to be used to make a payment (for example digital cash or units of value recorded in a computer chip on a card); and
- (b) may or may not be denominated by reference to units of a currency.²⁸

“stored value facility” means a facility (for example software) which:

- (a) is designed to control:
 - (i) the storage of stored value; and
 - (ii) the release of that stored value from the facility in the course of making a payment using that stored value;
- (b) is intended to be in the possession and control of a user; and
- (c) contains a value control record.²⁹

“stored value operator” means, in respect of a stored value facility, an entity which subscribes to this Code and which is an issuer or a payment facilitator or both an issuer and a payment facilitator in respect of that stored value facility.³⁰

“system participant” means a party to a stored value system and includes issuers, payment facilitators, holders of value received in exchange for stored value, originators of stored value, distributors of stored value, transaction processors, communications service providers and merchants who receive stored value as payment.

“user” means an individual intended by a stored value operator to use a stored value facility (whether or not the identity of the individual is known to the stored value operator) and, in the case of anonymous and transferable stored value facilities, includes the holder of the stored value facility from time to time.³¹

"value control record" in a stored value facility means an adjustable record of the amount of stored value available to be released from the stored value facility that has the following features:

- (a) the determination of whether there is sufficient stored value available for each payment to be initiated using the stored value facility is made solely by reference to the amount in the value control record and not by reference to any other record of the amount of available stored value (for example a separate value record held by a stored value operator); and
- (b) the amount in the value control record is reduced by the amount of stored value released from the facility.³²

11.3 In this Part, references to an “exchange” of stored value for a payment of money or for a credit to an account:

- (a) are not intended to characterise or limit the legal nature of that exchange or the relationship between the parties involved; and
- (b) includes exchange by way of purchase and sale or repayment of a debt or other types of exchange.

11.4 A stored value operator who is obliged to, or elects to, pay money to a user under a provision in Part B has the choice of paying it:

- (a) in the form of Australian currency; or
- (b) by crediting an account at an authorised deposit-taking institution nominated by the user; or
- (c) in any other manner agreed with the user.

12. Availability and disclosure of information and terms and conditions applicable to stored value facilities

- 12.1 Stored value operators will prepare for their users clear and unambiguous Terms and Conditions for the use of stored value facilities which reflect the requirements of this Code. In respect of the subject matters dealt with in this Code, the Terms and Conditions will not provide for greater liabilities or lesser rights for users than those set out in this Code. The Terms and Conditions are to include a warranty that the requirements of this Code will be complied with.
- 12.2 Stored value operators will provide a copy of the Terms and Conditions to the user:
- (a) at the time of first providing a stored value facility to a user or, if that is not practical in the circumstances, provide a summary of the main rights and liabilities of users under the Terms and Conditions and a notice of where the user may obtain a copy of the Terms and Conditions; and
 - (b) at any other time when requested to do so by a user.

The availability of Terms and Conditions is to be publicised by stored value operators.

- 12.3 Stored value operators will ensure that, before a stored value facility is used for the first time after issue, the user to whom it is issued has been provided with information on at least the following matters or, if that is not feasible, a summary of the information and a notice of where the user may obtain the full information:
- (a) any charges (imposed or controlled by the stored value operator) for the issue or use of a stored value facility, or the issue, exchange, transfer, loading or unloading of stored value.³³

Charges for the issue, exchange, transfer, loading or unloading of stored value do not include charges for funding the stored value (eg. credit charges for obtaining stored value on credit);
 - (b) the period or date (if any and if determinable at the time of issue) after which the stored value facility or the stored value controlled by the facility will not be usable to make a payment;
 - (c) the user's rights and the procedure to be followed by the user in relation to exchanging the stored value for money or for replacement stored value;
 - (d) whether there is a procedure (and, if so, a description of the procedure) for reporting a malfunction or error in the operation of a stored value facility or the loss or theft of a stored value facility or of stored value controlled by the stored value facility;

- (e) whether there are any circumstances (and, if so, a description of the circumstances) in which the stored value operator may pay to the user some or all of the amount of lost or stolen stored value; and
- (f) where the user can obtain more information and the Terms and Conditions for the stored value facility.³⁴

13. Changing the terms and conditions of use

13.1 Subject to sub-clause 13.4, stored value operators wishing to vary or modify the Terms and Conditions for the use of stored value facilities will provide notification of the change to users in advance.

- 13.2 (a) Where the stored value operator knows the identity and contact details of a user and the change relates to the matters set out in sub-clause 13.3, the stored value operator will provide the information directly to the user.
- (b) In all other cases, the stored value operator will publicise the changes in a manner which is likely to come to the attention of as many users as possible and which has previously been advised to users.³⁵

13.3 Where the change will:

- (a) impose or increase charges (imposed or controlled by the stored value operator) relating solely to the use of a stored value facility, or the issue of an additional or replacement stored value facility, or the issue, exchange, transfer, loading and unloading of stored value;
- (b) adjust the load or value storage limits applying to the use of a stored value facility;
- (c) affect the user's ability to exchange stored value, notify the loss or theft of stored value or be paid the amount of lost or stolen stored value; or
- (d) reduce the period (if any) during which the stored value facility or stored value controlled by the facility will be useable to make a payment;

the stored value operator will allow a period of notice of at least 20 days (or, where applicable legislation requires a longer notice period, that longer period) before the change takes effect except where the user has specifically agreed to a change described in paragraphs (b) or (c).

13.4 Advance notice need not be given when changes are necessitated by an immediate need to manage, restore or maintain the integrity or the security of the system or individual accounts or stored value facilities.

14. Record of available balance

- 14.1 Stored value operators must ensure that an undamaged stored value facility (either by itself or together with other equipment reasonably available to users) enables a user to ascertain the amount of stored value controlled by the stored value facility, which is available for use.

15. Rights to exchange stored value

Right to exchange stored value for money or replacement stored value

- 15.1 The user of a stored value facility may require the stored value operator to accept stored value controlled by the facility and in exchange (at the option of the user):
- (a) if the stored value is denominated by reference to a currency, pay the user the equivalent amount of money; or
 - (b) credit the amount of that stored value towards providing replacement stored value which is usable for the same purposes.

The stored value operator may charge a reasonable fee for such an exchange but not where sub-clause 15.2 applies.³⁶

Right of exchange applies where stored value or facility is unusable

- 15.2 Where the user's stored value facility or the stored value controlled by the facility is no longer able to be used to make a payment:
- (a) the right in sub-clause 15.1 applies provided the amount of stored value controlled by the stored value facility can be ascertained by the stored value operator using its own equipment; and
 - (b) subject to paragraph 15.3(b), the Terms and Conditions may provide that the right must be exercised within a specified period of at least 12 months after the date the stored value or stored value facility is no longer able to be used.³⁷

Limits on the right of exchange

- 15.3 (a) The stored value operator may refuse to exchange the stored value under sub-clause 15.1 if the stored value operator can prove that:
- (i) the stored value has not been created by a system participant authorised to create stored value;
 - (ii) a copy of the stored value has previously been exchanged for money; or
 - (iii) the user presenting the stored value for exchange is not doing so in good faith.
- (b) The Terms and Conditions may provide for the manner of exercising the right under sub-clause 15.1 and, in particular, may provide that where a

stored value scheme is suspended or terminated for security reasons, the right in sub-clause 15.1 must be exercised within a reasonable time (not less than 14 days) after users are advised of the suspension or termination of the scheme.³⁸

16. Refund of lost or stolen stored value

16.1 Where:

- (a) a stored value operator, together with relevant system participants, has or can create a reliable record of the amount of stored value controlled by a stored value facility from time to time; and
- (b) the stored value operator and any relevant system participants can prevent any further transfers of stored value from the facility;

the stored value operator must:

- (c) provide a means for a user to notify the stored value operator (or other entity specified by the stored value operator) at any time of the loss or theft of the stored value facility; and
- (d) where a user gives notice under paragraph (c), pay the user the amount of stored value which the stored value operator could have prevented from being transferred from the facility.³⁹

17. System or equipment malfunction

17.1 The stored value operator is liable to the user of a stored value facility for any losses (including any amount of lost stored value) arising from a failure to execute or the defective execution of the user's transactions, where the failure to execute or the defective execution is attributable to a malfunction of the facility or of a device, terminal or other equipment controlled or provided by or on behalf of the stored value operator, provided the malfunction was not caused by the user knowingly or in breach of the Terms and Conditions of use of the facility.

18. Stored value operator's obligations

18.1 A stored value operator:

- (a) may not avoid its responsibility to meet any obligation owed to users by reason only of the fact that another system participant has caused or contributed to the failure to meet the obligation; and
- (b) shall not require users to raise complaints or disputes regarding the use of a stored facility with, or have these complaints or disputes investigated by, any other system participant.

19. Complaint investigation and dispute resolution

- 19.1 Clause 10 of this Code (other than sub-clauses 10.10, 10.11, 10.12 and 10.13) applies to stored value operators under Part B of the Code as if they were account institutions under Part A of the Code.

Part C

Privacy, electronic communication, administration and review

20. Interpretation and Multiple Disclosure Obligations

20.1 In this Code:

“Code subscriber” means an account institution as defined in Part A or a stored value operator as defined in Part B.

“electronic communication” means a message transmitted and received electronically in a manner and a format that:

- (a) allows the message information to be presented to the recipient in a manner and format (eg. visual display or sound recording) that is clear and readily understandable; and
- (b) allows the recipient of the message to retain the message information for subsequent reference (eg. by printing the message information or storing the message information for later display or printing or listening).

20.2 In this Code, unless the contrary intention appears:

- (a) the singular includes the plural and vice versa; and
- (b) a reference to an access method includes a reference to each of the individual components that are part of the access method (including devices, identifiers and codes); and
- (c) inclusive definitions of a term and examples used to illustrate or amplify the meaning of a term do not limit the meaning of the term.

20.3 Explanatory notes to provisions in this Code do not form part of the Code but may be used to interpret the provisions of the Code.

20.4 Where legislation and this Code both require a Code subscriber to provide notice of changes to Terms and Conditions of use at different times:

- (a) the Code subscriber shall provide that notice at the earliest time it is required under the legislation or this Code; and
- (b) the provision of that notice under the legislation at or before the time required by this Code, will satisfy the Code's requirements for notice.⁴⁰

21. Privacy

- 21.1 From 21 December 2001 Code subscribers will comply with the National Privacy Principles in the *Privacy Act* 1988 (Cth) or with Codes to which the Code subscriber has also subscribed which are approved and operative under that legislation.⁴¹
- 21.2 The following *guidelines* are provided to assist in interpreting the National Privacy Principles and any approved Code referred to in sub-clause 21.1 and in applying them to EFT transactions under Part A:
- (a) *where surveillance devices (including visual, sound or data recording) may be used by or on behalf of an account institution to monitor EFT transactions, account institutions should notify users, before the commencement of each transaction or of each session of transactions, that the transaction may be recorded by surveillance devices and the nature of the surveillance;*
 - (b) *account institutions shall take reasonable steps to ensure that, except where it is being operated by an employee or agent of the account institution concerned, no institution equipment or institution system is capable of providing any information concerning an account unless the correct access method for that account has been used;*
 - (c) *transaction receipts should not disclose information which would reveal the full account number, name or address of the account holder; and*
 - (d) *if EFT transactions can be conducted through an account institution's electronic address (eg. a web site), the account institution should ensure that clear privacy policies are made available at or through that electronic address and can be provided to a user by electronic communication if the user so requests.*

In this sub-clause, terms have the same meaning as in Part A of this Code.

- 21.3 In deciding whether a Code subscriber has complied with the relevant principles under sub-clause 21.1, the terms of the principles (and not the terms of any applicable guidelines in sub-clause 21.2) are determinative.

22. Electronic communications

- 22.1 Unless prohibited by legislation, a user (as defined in Part A or Part B) may agree that any information which this Code requires the Code subscriber to provide (by writing or other means) may be provided:
- (a) by electronic communication to the user's device, electronic equipment or electronic address nominated by the user; or
 - (b) by being made available at the Code subscriber's electronic address for retrieval by electronic communication to the user on the condition that:

- (i) the Code subscriber promptly notifies the user by electronic communication under paragraph (a) that the information is available for retrieval at the electronic address and the nature of the information; and
- (ii) the Code subscriber provides the user with the ability to readily retrieve the information by electronic communication (eg by providing an electronic link to the relevant information at the Code subscriber's electronic address or the URL of the Code subscriber's website).⁴²

The user's agreement to the provision of information under paragraph (a) or (b) or both must be by a specific positive election after receiving an explanation of the implications of making such an election. The user may by notice to the Code subscriber vary the user's nominated device, electronic equipment or electronic address or terminate the agreement to the provision of information under paragraph (a) or (b) or both and the Code subscriber must inform the user of those rights.⁴³

- 22.2 (a) Except in respect of a user and Code subscriber who have a current agreement that satisfies 22.1(b), and subject to paragraphs (b) and (c), making information available at a Code subscriber's electronic address (eg a web site) does not satisfy any requirement of this Code that the information be provided to a user.
- (b) Where a user has viewed information available at a Code subscriber's electronic address (eg. a web site), and has:
- (i) been given the opportunity to retain that information for subsequent reference (eg. by saving or printing it); and
 - (ii) specifically agrees that the user has viewed the information and has been given the opportunity to retain that information and that the user will not be otherwise provided with a copy of the information by the Code subscriber (without a separate request by the user under sub-clause 22.3);
- the Code subscriber is to be treated as having provided that information to the user at the time the user specifically agreed.
- (c) Where an EFT transaction is initiated by a user through an electronic address, the account institution may satisfy its obligation to provide a receipt under sub-clause 4.1 by making the receipt available to the user at the same electronic address immediately on completion of the transaction in the manner and format described in the definition of "electronic communication" in sub-clause 20.1.⁴⁴

- 22.3 Where a Code subscriber has provided, or is treated as having provided, information (other than a receipt under clause 4.1) to a user by electronic communication under sub-clauses 22.1 or 22.2, the Code subscriber shall provide a paper copy of that information to the user if the user so requests within 6 months of the receipt of the electronic communication.

23. Commencement and administration

- 23.1 (a) Subject to (b), the Code shall become binding on Code subscribers on 1 April 2002.
- (b) Clause 4.6 shall become binding on Code subscribers on 1 April 2003.
- (c) Code subscribers can choose to be bound by this Code at an earlier date than that set down in (a) or (b).
- 23.2 Code subscribers shall notify ASIC of the fact that they have subscribed to the Code by using the form available from ASIC's website www.asic.gov.au (choose 'Policy and Practitioners'). Completed forms should be sent to Consumer Protection Directorate, ASIC, GPO Box 4866, Sydney NSW 1042.⁴⁵
- 23.3 (a) A Code subscriber, or prospective Code subscriber, may separately or jointly with another Code subscriber or prospective Code subscriber, apply to ASIC for a modification of the application of the provisions of Part B of this Code in relation to particular products, services or activities of that entity.
- (b) ASIC may consult with any third party that might be materially or adversely affected by a decision on the application and with consumer representatives.
- (c) If ASIC wants to consult a third party it must obtain the consent of the Code subscriber or prospective Code subscriber before releasing any confidential information that they have provided to ASIC.
- (d) ASIC may require any party with which it consults to sign a confidentiality agreement as a condition of being consulted.
- (e) In considering whether or not to grant the modification ASIC will give consideration to any relevant matters, including:
- (i) whether or not the modification would significantly undermine the consumer protection objectives of the Code;
 - (ii) whether relevant Code objectives can be achieved in some other way;
 - (iii) whether failure to grant the modification would cause unreasonable expense to the institution or make a product unviable;
 - (iv) whether the modification is needed to prevent the Code interfering with technological and product innovation;
 - (v) the need to avoid confusion in relevant markets; and
 - (vi) the need to ensure competitive neutrality in relevant matters.

- (f) If ASIC grants the modification and publishes a notice setting out the modification on its Website, at www.asic.gov.au, the relevant provisions of the Code apply as modified to that entity for the period specified in the notice.
- 23.4 After consultation with interested parties, ASIC may publish an order modifying:
- (a) the application of one or more of the disclosure requirements in clauses 2, 3, 12 and 13 of this Code in relation to some or all products of some or all Code subscribers in order to avoid Code disclosure obligations operating inconsistently with, or duplicating, disclosure obligations in legislation; and
 - (b) clause 4.6 to ensure consistency with future legislative or industry practices; and
 - (c) the standards for industry dispute resolution that apply under sub clause 10.1.
- 23.5 Code subscribers, or their representative associations, will report to the Commonwealth Government annually on compliance with this Code as outlined in sub-clauses 23.6 and 23.7.
- 23.6 Code subscribers and/or their associations will report in accordance with the reporting guidelines for the industry sector, on compliance with this Code.
- 23.7 Code subscribers will establish administrative arrangements to ensure their staff receive adequate training on the requirements of this Code. Code subscribers and/or their associations will also report on initiatives in training staff in understanding and implementing the Code.

24. Review

- 24.1 ASIC, in consultation with Code subscribers and their respective associations, relevant State and Territory government agencies and consumer representatives and relevant independent industry dispute resolution schemes:
- (a) will undertake periodic reviews of the requirements of the Code, including the administrative arrangements set out in clause 23 and the first review of the Code as revised in 2001 will commence not later than 2 years after the date determined under paragraph 23.1(a);
 - (b) may issue guidelines interpreting the provisions of the Code.

Schedule to Code

Information to be obtained where available and relevant from users making a complaint concerning the authorisation of an EFT transaction as required under clause 10.4.

1. account type and number, type of access method used
2. name and address of user
3. other users authorised to operate on the relevant account(s)
4. whether device signed
5. whether device lost or stolen or security of codes(s) breached
 - date and time of loss, theft or security breach
 - time of report to account institution,
 - time, date, method of reporting reported to police or other authority
6. code details
 - was record of code made
 - how recorded
 - where kept
 - was record of code lost or stolen
 - date of loss, time
 - has code been disclosed to anyone
7. How loss occurred (eg housebreaking, stolen purse/wallet)
8. Where loss of device occurred, eg office, home
9. Details of transaction to be investigated
 - description, date, time, amount
 - type and location of electronic equipment used
10. Details of any
 - circumstances surrounding the loss or theft or security breach of the device or codes, or the reporting of such loss or theft or security breach; or

- steps taken to ensure the security of the device or codes;
which the user considers relevant to his/her liability in respect of the transaction

11. Details of last valid transaction

End notes

¹ An instruction may be given directly to an account institution (eg. through the institution's own electronic terminal or Interactive Voice Recognition (IVR) system or electronic address) or indirectly (eg. the instruction is given through an electronic terminal or IVR system or electronic address belonging to a third party, such as a merchant or another account institution, and then on-sent for ultimate delivery to the account institution which maintains the account).

Where the instruction from the person to the account institution is given indirectly through one or more intermediaries, it is an EFT transaction if the account institution relies for its authority to debit or credit an EFT account on the use (by the person or by an intermediary) of an access method authorised by the institution to be used directly by a user but not if the account institution relies on a different form of authority used by an intermediary (eg. a direct debit authority held by the intermediary): see the definition of "access method". E.g. If the account institution issues a password to a user who gives it to an intermediary (such as an account aggregator) and the intermediary uses that password to give an instruction to the account institution and the account institution relies on the use of that password as authority to debit an EFT account, it is an EFT transaction. But if the intermediary (eg a merchant) transmits a user's payment instruction to an account institution which relies for its authority to debit an EFT account on a different form of authority not authorised for direct use by a user (eg. the merchant's direct debit authority given by the user), it is not an EFT transaction.

² The definition of "funds transfer" is broad but the Code does not apply to a funds transfer unless it is initiated by giving an instruction, through electronic equipment and using an access method, to an account institution to debit or credit an EFT account.

A "funds transfer" does include:

- a transaction which is a user-initiated transfer of value by the account institution to a third party (eg in payment for goods or services supplied by the third party to the user) and a debit by the account institution to the customer's EFT account to reimburse the account institution for the amount of value transferred (eg. a credit card payment to the third party). The debit to the customer's EFT account is the relevant funds transfer for the purposes of Part A. It is irrelevant whether the customer's EFT account has a credit or debit balance before the debit was made;
- a credit card cash advance/withdrawal if initiated through electronic equipment using an access method because value is transferred from the cardholder's EFT account by debiting that account.

A "funds transfer" does not include:

-
- balance inquiries;
 - a transfer of value from a customer's biller account to the biller account institution to pay the account institution for goods or services (other than financial services) provided *by the account institution* to the customer: see paragraph 1.4(b);
 - a transfer of stored value unless this also effects the transfer of value to or from an EFT account at an institution (eg exchanging stored value for a debit or credit to an EFT account). Thus Part A does not cover transfer of stored value between two stored value facilities as defined in Part B (eg. between two stored value cards) because a stored value facility (as defined) is not an EFT account (see definition of "EFT account").

A physical payment instrument delivered as a transfer of value could include a traveller's cheque or bank cheque.

³ Many companies (eg. electricity suppliers and department stores) maintain customer accounts to record the amounts owing and paid by the customer for goods or services provided by the company. These accounts are defined as "biller accounts" in sub-clause 1.5 if the customer can initiate a funds transfer from or to the accounts using an access method through electronic equipment.

- **Receipt of funds for credit of biller accounts not regulated by Part A except clause 7**
Where the customer makes a funds transfer (eg. by BPay from a bank account) to the company for credit to the customer's biller account (eg. to pay an electricity bill or pre-pay for anticipated future purchases), Part A may apply to the bank in debiting the bank account but under paragraph 1.4 (a), Part A will not apply to the receipt by the company of the funds transfer for credit to the biller account except for clause 7. Clause 7 deals with the security of deposits received through the company's electronic equipment and with discrepancies between amounts recorded as having been deposited through electronic equipment and amounts recorded as received.
- **Transfer of Funds from a Biller Account to Pay the Biller Usually Not Covered by Part A.**
In some cases a company may be paid for goods or services it supplies to a customer by the customer initiating a debit to the customer's biller account and transferring funds to the company (eg. where the customer has prepaid an ISP account and the customer initiates a debit to that account, using an access method, as the customer uses the service). Paragraph 1.4(b) makes it clear that these funds transfers are not covered by Part A. (The only exception is where there is a customer-initiated funds transfer from the customer's biller account to pay for financial services supplied by the company to the customer. This exception has been included to maintain competitive neutrality with financial institutions.)
- **Transfer of Funds from Customer Accounts to Pay Third Parties May Be Covered by Part A**
Some companies permit their customers to use a customer account as a means of making payments **to third parties** eg a customer charges the price of a CD or

financial information (supplied by a third party) to the customer's telephone account. The telephone company pays the third party supplier and debits the customer's telephone account and the customer reimburses the telephone company by paying the amount (with any fees) to the telephone company to be credited to the customer's telephone account. This use of a customer account to pay third parties is effectively the same as a credit card or charge card account. (A customer account which can be used to make payments to third parties is not a "biller account" as defined.) If the customer account is an EFT account (eg. the customer can initiate a funds transfer from the customer account using an access method through electronic equipment), the use of the customer account to pay third parties is covered by Part A. Sub-clause 1.4 does not alter this coverage.

⁴ "Access method" includes but is not limited to physical "devices", non-secret "identifiers" (such as account numbers, card numbers, expiry dates) and secret "codes" (such as a PIN or password which is known only to the user or only to the user and the account institution). It includes a biometric of the user such as a fingerprint, or retinal pattern or voice pattern, whether or not the biometric is an "identifier" as defined.

- It does not include a method where the intended means of user authentication is based on requiring a user's manual signature and comparing the appearance of that signature with a written specimen signature (eg. cheques, signed withdrawal slips, signed credit card vouchers) on the grounds that the common law already covers liability allocation for manual signatures. Note that the comparison need not have occurred in any particular transaction (eg. signature is not actually compared on many cheques or credit card vouchers but manual signature is the intended means of authentication). Other signature authentication methods not based on comparison of appearance with a written specimen will come within the definition (eg. signature dynamics where the signer is authenticated by comparing the pressure, speed and stroke order of the signature against a previously obtained electronic record of this data).
- The inclusion of non-secret "identifiers" means that the use of an account number or card number at electronic equipment without a device or secret code, now comes within the scope of the EFT Code (eg. use of a credit card number through a telephone or personal computer to make a purchase).
- The user is not liable for unauthorised transactions based on the use of an identifier without a code or a device (see sub-clauses 5.5 and 5.6). The user is liable for unauthorised transactions based on the use of a device (or a device and an identifier) without a code only where the user unreasonably delays in notifying loss or theft of the device (see paragraph 5.5(b)).
- The access method or some of its components need not have been issued by the financial institution eg a PKI private key on a smart card issued by a third party.
- An access method such as a code or identifier could be provided by voice communication through electronic equipment.

⁵ An account institution need not be a traditional financial institution. The term includes companies which maintain customer accounts and bodies which pay third parties on the instruction of users and debit users' accounts to cover the amount of those payments (provided the accounts are "EFT accounts").

⁶ Examples of a biller account may be an electricity company's or a department store's customer account. A regular deposit account at a financial institution is not a biller account under this definition.

⁷ A code:

- does not include codes or cryptographic keys the content of which is not known to the user eg. a PKI private key on a smart card or computer hard drive because it is too long to be memorised;
- does include a code used to access a device eg. a PIN used to unlock a card or token even if the code is not used separately to access the electronic equipment.

⁸ The definition excludes accounts not belonging to a customer (eg. suspense or internal accounts). It also clarifies that in stored value systems where the stored value facility contains a value control record, neither the value control record nor other value records are EFT accounts for the purposes of Part A. However, products branded as stored value products which do not have value control records in the product are not covered by this exclusion and may in fact be remote account access products covered by Part A.

⁹ An identifier may be, for example, an account number, card number, card expiry date.

¹⁰ There are additional interpretation provisions applicable to the whole Code in clause 20.

¹¹ Sub-clause 20.4 deals with overlapping legislative disclosure requirement.

¹² For example, privacy and security concerns may preclude providing balance information at EFTPOS terminals but not at ATMs.

Account institutions should avoid adding non-required information to receipts (such as credit card expiry dates) which increase the risk of unauthorised transactions.

¹³ Clause 22 permits electronic provision of receipts.

¹⁴ Eg. The user initiates a credit card payment over the Internet at a merchant's web site. The account institution may not be able to ensure a receipt is provided under paragraph 4.1(a)

but must use its best endeavours (eg through the merchant's acquiring institution or the card association) to see that the merchant provides a receipt.

¹⁵ This provision only applies to those agreements which would ordinarily be entered into.

¹⁶ The dominant contributing cause of the losses is the cause that is more than 50% responsible for the losses when assessed together with all other contributing causes.

A daily transaction limit may apply to the use of an access method, an account or particular electronic equipment or a combination of these. Paragraphs 2.3(b) and 3.1(c) contain relevant notice requirements.

¹⁷ “Extreme carelessness” means a degree of carelessness with the security of the codes which greatly exceeds what would normally be considered careless behaviour. For example, 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".

Paragraph (e) does not apply to the selection of codes – paragraph (d) covers this.

An access method may also include identifiers but the security of identifiers is irrelevant to liability under clause 5.5.

¹⁸ Institutions may also technically restrict available self-selection choices by users in whatever way they wish.

¹⁹ Eg an account institution may decide to let its users provide their codes to the institution's own or an associated company's account aggregator service or store the codes in an electronic wallet on the user's personal computer. If the institution promotes or endorses that service or authorises its users to use that service, such conduct by the user is not a contravention of 5.6. If the institution does not promote, endorse or authorise the use of the service, the user's use of the service may breach sub-clause 5.6.

(Note that, while account aggregation services raise a number of issues which could possibly be addressed in the EFT Code, the revised Code does not attempt to deal in any detail with this issue as the services only began emerging towards the end of the 2000 review process and a rushed response was not considered to be appropriate. It may be that the Code will be amended at a later date to deal with account aggregation issues or these issues could be dealt with elsewhere. The matters addressed in 5.7 were included to address one narrow aspect of the PIN security which was thought to need immediate attention.)

²⁰ Reasonable steps to prevent unauthorised access may involve hiding or disguising the code record among other records or in places where a code record would not be expected to be found, by keeping a record of the code in a securely locked container or preventing unauthorised access to an electronically stored record of the code.

²¹ Account institutions may be able to resolve unauthorised transaction disputes on credit card or charge card accounts by exercising rights (such as the right to charge back a transaction) against other parties to credit card or charge card schemes. This clause does not require account institutions to exercise any such rights. However they cannot hold account holders liable under clause 5 for a greater amount than would apply if they had exercised those rights. The relevant rights under the rules are those that exist at the time the complaint was made. A delayed complaint may mean the rights have expired by the time of the complaint.

²² Account institutions may impose other periodic transaction limits as they wish eg. by reference to access method, account or institution equipment used. Other periodic transaction limits apply in addition to the daily transaction limit.

²³ Exceptional circumstances may include delays caused by foreign account institutions or foreign merchants being involved in resolving the complaint.

²⁴ The purpose of this clause is to provide an incentive to institutions to implement good investigation and decision-making procedures in accordance with the Code and to compensate account holders for the effects of prejudicial decisions or delays.

Because this clause is about procedural compliance, the institution may be made liable under this sub-clause even if the institution ultimately is not found liable on the substance of the complaint under clauses 5 and 6. Liability under this sub-clause might arise for example where an account institution did not obtain from the user the information listed in the Schedule to the Code, did not analyse the liability of the user in terms of clause 5 and informed the user that she or he was liable simply because the correct code was used to access the account. If those failures led to the user seeking senior management review or external review of the decision, then an award of some portion of the amount in dispute against the institution may be justified for the inconvenience and expense caused to the account holder and the user by the institution's failure to properly investigate, analyse and explain its decision on the complaint. An award may be justified for inconvenience and expense even if the institution's decision is upheld on other properly reasoned grounds after full investigation. The amount of the award would be a matter for the senior management or external review body having regard to all the circumstances.

²⁵ Sub-clause 10.13 is designed to reduce compliance obligations and transaction costs and the risk of liability under clause 10.12 for account institutions which decide quickly to allocate no liability to the account holder or use the no-fault apportionment route in clause 5.5(c).

²⁶ Eg. the amount of stored value recorded in the value control record of a stored value facility may be increased (or "loaded") in exchange for a debit to an EFT account. The debiting of and transfer of value from the EFT account may be an EFT transaction - if so, it is regulated by Part A, not Part B. The operation of the stored value facility, including the adjustment of the value control record, is regulated by Part B.

²⁷ A payment facilitator may facilitate a payment for example by facilitating the reduction of a liability it has to the payer in the amount of the payment and

- (a) facilitating the increase of a liability it has to the payee in the amount of the payment; or
- (b) procuring another entity to increase a liability that entity has to the payee in the amount of the payment.

²⁸ Different stored value systems may use different representations of value eg. a balance record of units of value which is decremented or incremented in a payment; or digital tokens assigned a fixed nominal value.

Stored value may be denominated by reference to units of a currency but a stored value unit need not equate to one currency unit. A stored value unit may represent 22¢ or \$5.60 or six stored value units may represent \$1.00. Stored value need not be denominated by reference to units of a currency eg, beenz, MyPoints.

Stored value may be issued in exchange for money or as a gift or on credit.

²⁹ A “release” of stored value from a facility constitutes part but not the whole of a transfer of stored value from the facility to another person in the course of paying the other person. A stored value facility must control the release of value but need not control the completion of the transfer to another person.

A “release” of stored value includes (without limitation):

- decrementing the balance of stored value on the facility; or
- sending digital tokens of fixed nominal value such as digital coins from the facility.

A transfer of stored value includes a release of stored value from a facility and the receipt of stored value by a payee’s facility or terminal. Without limitation, the receipt may occur by incrementing a balance on the payee’s facility or the receiving and storage of digital tokens by the payee’s facility.

A stored value facility includes, for example, software for controlling storage and release of stored value whether that software is supplied to a user for installation on the user’s computer (eg. purse software to manage digital coins) or is supplied to a user already installed on a computer or device (eg. software that operates the stored purse function on a smart card containing a microprocessor chip).

The stored value facility may also control the receipt of value to the facility (eg. a reload or receipt of a payment).

³⁰ Stored value systems may have:

- a single entity who is both the issuer and payment facilitator - that entity is the stored value operator if it subscribes to the Code eg. a bank that issues digital cash stored value facilities and is the payment facilitator.
- one or more issuers and one or more payment facilitators - those entities can determine which one or more of them should subscribe to the Code and become a stored value operator or stored value operators.

Each issuer and payment facilitator who subscribes to the Code is subject to all the obligations under the Code. Each such entity should ensure it has in place rights against other system participants (including other Code subscribers) which it needs to meet its obligations under the Code (eg. a right to call on the holder of the funds received in exchange for stored value to meet exchange for money obligations under clause 15) - see clause 18.

³¹ For example, a stored value operator may intend that a stored value facility be used:

- only by the identified individual to whom it is issued;
- by another individual authorised by the individual to whom it is issued;
- by any individual within a group or class (eg. public transport users, students at a university); or
- by any member of the public.

³² The type of record in a value control record will vary according to the stored value system, eg. it may be a single balance record or may be the sum of the nominal values of the digital tokens controlled by the stored value facility.

The key feature in the definition is paragraph (a). A stored value operator may maintain a shadow account mirroring the value record on a stored value card or software product such as digital coin purse.

If transfers of value initiated by the card or software product are authorised by reference to the value record on the card or software product rather than any shadow balance, the card or software product is a stored value facility (assuming it meets the rest of the definition) regulated by Part B and neither the value control record nor the shadow account is an EFT account for the purposes of Part A (see definition of "EFT account" in Part A). Part A will only be relevant to a stored value facility where it transfers value to or receives value from an EFT account.

But if transfers of value initiated by the card or software product are authorised by reference to a shadow account or other value record instead of a value control record, then the card or software product is not a stored value facility but more akin to an access device used to access an account record maintained by an institution. The intention is that such cards and software products will be regulated by Part A as access methods used to initiate funds transfers from the shadow account or other value account if that is an EFT account under Part A.

The value control record is the sole determinant of whether there is sufficient stored value available to make a payment. However, reference may be made to a stored value operator's records for other authorisations, eg. whether the card has been reported as lost or stolen and hence disabled.

³³ A Code subscriber may also be required to disclose some of this information under cl. 2.3 in Part A (eg. charges for loading or unloading to an account) to a “user” as defined in Part A. If that person is also a “user” as defined in Part B, only one disclosure of the same information is required.

³⁴ Information provided under sub-clause 12.2 prior to first use of a facility which covers items in sub-clause 12.3 need not be re-supplied under 12.3.

All information can be provided by electronic communication in accordance with Part C.

³⁵ All information can be provided by electronic communication in accordance with Part C.

³⁶ Any fee must be disclosed under sub-clause 12.3. If the stored value is not denominated by reference to a currency (eg loyalty points), there is no obligation to exchange the stored value for money but the obligation to credit the stored value towards replacement stored value still applies.

³⁷ A stored value facility or stored value may be unusable to make a payment for many reasons eg. the facility is damaged or malfunctioning, the facility or the value has expired or the amount of stored value remaining is below the minimum needed for a transaction.

³⁸ Sub-clause 15.1 gives users the right to require the stored value operator to exchange stored value either for credit towards replacement stored value or for the equivalent amount of money. If the amount of the credit is below the minimum issue amount of stored value, the user will have to “top it up” to the minimum issue amount by using other credits or paying money. The stored value operator can charge a reasonable fee for providing replacement stored value or money in exchange unless sub-clause 15.2 applies. Money may be paid (at the option of the stored value operator) in the form of currency or as a credit to an account at an ADI nominated by the user or in another manner agreed with the user (sub-cl. 11.4).

³⁹ Under clause 12.3 the stored value operator must inform users whether any action can be taken to prevent unauthorised use of lost or stolen stored value and whether any refund will be made. The ability to provide a refund will turn on technical capabilities including prevention of unauthorised use and having an independent record of the balance on the facility at any time.

⁴⁰ Legislation such as the proposed *Financial Services Reform Bill 2000* may require notice of changes to be provided at a different time than the Code requires the same

information to be provided. Sub-clause 20.4 makes clear that Code subscribers should comply with the earliest disclosure obligation (e.g. the Financial Services Reform Bill's) and thus satisfy the timing of all disclosure obligations.

⁴¹ The National Privacy Principles may be found at www.privacy.gov.au.

⁴² Information can be readily available from an electronic address for the purposes of sub-paragraph 22.1(b)(ii) even if the user is required to input a code (as defined in Part A) to retrieve the information.

⁴³ The agreement referred to in sub clause 22.1 may be formed by electronic communications. A user's electronic address could be eg. an email address or a facsimile number.

⁴⁴ Paragraph 4.1(c) imposes only a best endeavours obligation on the institution where the user's communication is with a third party (eg an online merchant) and does not use institution equipment.

⁴⁵ Subscribers to the existing Code will need to re-subscribe to the new Code. The new Code will apply to a Code subscriber in lieu of the old Code on the date the Code subscriber subscribes to the new Code. The old provisions of the Code cease to operate from 1 April 2002.