

# Your guide to the EFT Code



**ASIC**

Australian Securities & Investments Commission

Whenever you get money out of an ATM; buy goods or services on EFTPOS; do telephone or internet banking; or use your credit card over the phone or internet, you are using electronic means of transferring money. These are known as “electronic funds transfers” (EFT). If you use a stored value facility, such as a prepaid phone card, this is also an electronic funds transfer.

The EFT Code is an important code of practice that protects you when using electronic funds transfers. This guide explains your rights and responsibilities under the EFT Code.

- **A. The EFT Code:** what it is, what’s covered, what’s in it, who’s signed up. p. 3
- **B. EFT transactions:** your right to information, what happens about unauthorised transactions, protecting your password, account aggregation, system malfunctions, ATM deposits. p. 5
- **C. Stored value facilities:** what they are, your right to information, account balances, exchanging value, loss or theft, system malfunctions. p. 14
- **D. Complaints:** how to complain, problems caused by third parties, extra rules about EFT. p. 18
- **E. Privacy:** your protection.. p. 21
- **F. Electronic communication:** from your account institution. p. 22
- **G. How to get more information.** p. 22

## A. The EFT Code

### What is the Electronic Funds Transfer (EFT) Code?

The EFT Code is a code of practice which sets out rules about how electronic funds transfers should work. Businesses may choose whether to sign up to the Code. If they do, they must follow the Code in their dealings with you. The Code sets out what the business must do, what your rights and responsibilities are and what happens if something goes wrong.

### What types of electronic funds transfer services are covered?

The EFT Code is designed to cover all types of electronic funds transfers including:

1. getting money out of an ATM (automatic teller machine) or paying money into one
2. buying goods or services on EFTPOS (electronic funds transfer at point of sale)
3. buying goods or services with a credit card when you don’t need to sign for them

This means that credit card transactions over the internet and telephone are covered. However, if you pay in person and authorise the transaction with your signature, the EFT Code won’t apply. Other rules cover these transactions.

4. computer/mobile phone internet banking
5. telephone banking
6. transactions using stored value facilities such as prepaid phone cards.

Are there any electronic funds transfers not covered?

The EFT Code does not cover business accounts or biller accounts. Biller accounts are accounts maintained solely to record amounts owed or paid for non-financial goods or services (eg a prepaid electricity account).

What is in the EFT Code?

The EFT Code sets out rules about:

- the information you must be given and when and how it is provided
- what happens when things go wrong, including who is liable when there is an unauthorised transaction on your account
- your responsibility to look after your PINs and passwords and keep them secret
- procedures for making complaints
- special rules to protect the users of stored value facilities
- privacy
- when institutions can contact you electronically rather than on paper.

Who has signed up to the EFT Code?

We expect all account institutions (such as banks, building societies and credit unions) and a growing number of stored value facility providers will agree to sign up to the EFT Code.

Businesses that have signed up to the EFT Code must tell you, in their contract with you, that they will comply with the EFT Code.

Businesses must also tell us when they sign up to the EFT Code.



We list on our website those businesses that have signed up to the EFT Code - check it out at [www.fido.asic.gov.au](http://www.fido.asic.gov.au).

## B. EFT transactions that access your account electronically

Part B of this guide tells you the rules that apply to EFT transactions which access your account electronically. You access your account electronically when you use your card and/or PIN or password to tell your bank that you want to pay in or withdraw money from your account. For example, you are undertaking an EFT transaction which accesses your account electronically when you use your card to get money out of an ATM, when you purchase goods with a credit card

over the internet or you transfer money between two of your bank accounts via the internet. Rules for stored value products are covered later in this guide.

**What information do you have to be given and when?**

You are entitled to a copy of the contract (or terms and conditions) for your account. As well as setting out what you can expect from the institution you have your account with, the contract also sets out your rights and responsibilities.

Your account institution must give you the contract at the time of, or before, you use a new way of accessing your account. You can also get a copy at any time if you ask for it.

Your account institution must also give you certain information about your new card or PIN. This must include information about:

- the fees you will have to pay for using it
- any restrictions that apply, such as limits on how much money you can withdraw in a day
- what accounts you can access with the card or PIN
- how to report the loss, theft or unauthorised use of the card or PIN
- how to make a complaint.

This information must be given to you before you use your card or PIN for the first time.

It might sometimes be necessary for your account institution to change the rules for

your account, card or PIN. If it does, it must tell you about the proposed changes within a certain amount of time. Changes to charges or daily transaction limits must be given at least 20 days before they take effect.

If you deposit, withdraw, or transfer money electronically, your account institution must offer you a receipt. However, if you choose not to take a receipt, the institution does not have to give you one.

Receipts must include the date of the transaction, the type of transaction, accounts and amounts involved, subject to privacy considerations the amount remaining in the account you withdrew from and, where possible and relevant, the location of the machine involved or the name of the merchant involved.

Receipts are important as they help you keep track of your finances and identify transactions when you receive your statement.

You must be sent an account statement at least every six months. You must also be offered the choice of getting it more often.

**What happens if there is an unauthorised transaction on your account?**

An unauthorised transaction is a transaction that is made by someone else without your knowledge or consent.

Unauthorised transactions are rare (less than 20 in every million transactions). However, you should always check your statements to make sure that none have occurred.

Remember some transactions that look unfamiliar may just appear so because the merchant's banking is done under a different name to their trading name. Check with your account institution if you are unsure.

If you find an unauthorised transaction, contact your account institution as soon as possible. This is important both to fix up the problem and to prevent any more unauthorised transactions.

The EFT Code sets down who is liable if there is an unauthorised transaction.

The rules for allocating liability for unauthorised transactions don't apply to the stored value facility transactions discussed in Section C of this guide.

#### When will you get your money back for unauthorised transactions?

There are a number of situations where you will get back any money that has gone out of your account as a result of an unauthorised transaction. These include where:

- there was fraudulent or negligent conduct by the employees or agents of your account institution
- a forged, faulty, expired or cancelled card, PIN or password was used
- the transaction took place before you received your card, PIN or password
- a merchant incorrectly debited your account more than once for a sale

- the transaction took place after you told your account institution that your card had been lost or stolen, or that someone else may know your PIN or password.

The account institution must provide easy and effective ways for you to let them know at any time that your card has been lost or stolen or that someone else may know your PIN or password. Most institutions have a 24-hour phone number for this. They must acknowledge they have received your notification so that you have proof of when you told them.

- no PIN or password was required to conduct the transaction (except where the situations listed under "When won't you get your money back?" apply)

- it is clear that you haven't contributed to the loss

- the account institution expressly authorises the conduct that contributed to the unauthorised transaction.

If any of these circumstances apply, your account institution must repay you the money that has gone out of your account because of the unauthorised transaction.



### When won't you get your money back?

You will not get your money back for losses resulting from unauthorised transactions where your account institution can show that you contributed to the loss. For example, if:

- you act fraudulently or you do not keep your PIN or password secret (See 'What should you do to protect your PIN or password' below.)
- you do not tell your account institution that your card has been lost or stolen or that someone else may know your PIN or password.

However, you will not be responsible for:

- any money that has gone out of your account in one day that is more than your daily transaction limit for withdrawals or any other transaction limit applying to your account
- any money that has gone out of your account that is more than the balance of your account at the time of the transaction (including any prearranged credit)
- any money that has gone out of accounts which you and your account institution had not agreed could be accessed by the card, PIN or password
- any money that has gone out of your account which occurred before you became aware (or should reasonably have become aware) that your card had been lost or stolen or that someone else may know your PIN or password, or any money that went out after you told your account institution. Remember, tell your account institution immediately when you do find out.

Special rules apply where you need more than one PIN or password to access your account.

If there is no daily transaction limit on your account, your account institution and/or the external complaints schemes may decide to reduce your liability even if your negligence allowed the unauthorised transaction to occur.

### When will liability be split between the account institution and you?

If a PIN or password was needed to perform the unauthorised transaction and none of the above circumstances apply, that is, it's unclear whether or not you contributed to the loss, you will only be responsible for the lowest of the following:

- \$150, or any lower figure set by your account institution; or
- the balance of the account(s) at the time of the transaction (including any prearranged credit) affected, provided you had agreed with your account institution that the account(s) could be accessed with the PIN or password
- the amount of money that had gone out of your account before you let your account institution know that your card had been lost or stolen or that someone else knew your PIN or password (except for any money lost that is more than the daily transaction limit).

Your account institution must repay any money you have lost above this amount.

What should you do to protect your PIN or password?

It is very important that you keep your PIN or password secret. As explained above, if you don't, you might not get the money back for losses resulting from unauthorised transactions.

The EFT Code includes the following rules for protecting your PIN or password. If you break them, you will be liable for unauthorised transactions.

- You must never tell your PIN or password to anyone, including a family member or friend.

Most unauthorised transactions occur because a person gave someone else their PIN or password.

- Where you use a card to access your account, you mustn't write your PIN or password on the card or keep an undisguised record of your PIN or password together with items you may lose or have stolen at the same time as the card.
- Where you don't need a card to access your account but do need more than one PIN or password, you must not keep an undisguised record of the PIN/s or password/s on items that you are likely to lose or have stolen at the same time.
- Where your account institution tells you after 1 April 2002:
  - not to choose a PIN or password which represents your birth date or a recognisable part of your name, and

- what will happen if you choose a PIN or password of this kind

you must not go ahead and choose such a PIN or password.

- You must not act with "extreme carelessness" in failing to keep your PIN or password secret.

Example: storing your internet banking password in your diary or personal organiser or computer under the heading of Internet banking password might be extreme carelessness.

Your account institution may provide you with extra advice on how to protect your PIN or password. It is sensible to follow this advice, however, you will not be in breach of the EFT Code if you don't.

What if you use an account aggregation service?

Some account aggregation services require you to give them your PIN or password. If you do this, then you should check with your account institution whether this will mean you will be liable for any unauthorised transactions that result. You will not be liable if your account institution promotes, endorses, or authorises the account aggregation service that you use or explicitly gives you permission to tell the aggregator your PIN or password.



### What if the equipment or system malfunctions?

Your account institution is normally responsible for any losses caused by the failure of their equipment or the system they use to complete your transaction properly. However, if you knew (or should have known) that the system wasn't working properly but went ahead and used it anyway, the account institution may only have to correct any errors and refund relevant fees.

### What if there is a shortfall in your ATM deposit?

Your account institution must tell you, as soon as possible, if the amount of money that they received is different to the amount you think you deposited at the ATM. It must tell you how much money has been credited to your account. If you disagree, you can make a complaint.

## C. Stored value facilities

### What are stored value facilities?

Stored value facilities include things such as smart cards (eg prepaid telephone and transport cards) and digital cash that allow you to transfer money from them, and sometimes to them, without needing to access an account.

Where stored value facilities access an account (eg to reload them with value), the Code rules for EFT transactions in Section B apply. Otherwise, specific requirements apply to stored value facilities under the code. These are set out here.

### What information do you have to be given and when?

You are entitled to either:

- a copy of the contract (terms and conditions) which sets out your rights and responsibilities for the stored value facility, or
- a summary of the main rights and responsibilities and information about where you can get a copy of the complete contract if you want to.

This information must be given to you when you first get your stored value facility. It must also be given to you at any other time that you ask for it.

Before you first use the stored value facility, you must also be given information about:

- all associated fees and charges
- the expiry date, if any, of the facility
- your rights to exchange stored value for money or replacement stored value
- any procedure to report problems with the operation of the stored value facility or its loss or theft
- when (if at all) the stored value operator will repay you if value is stolen or lost from the facility

- where you can obtain more information or a copy of the contract.

You also have to be notified at least 20 days in advance of specific changes to these terms and conditions. The stored value facility operator must tell you directly about these changes if it knows how to contact you. Otherwise, and for all other changes, it must provide information about the change in a way that is likely to come to the attention of as many users as possible.

#### How will you know the balance on your stored value facility?

You have a right to be able to find out the balance on your stored value facility. You must be able to do this either through a feature of the facility itself, or by using the facility with other equipment, such as a reader, which must be made reasonably available to you.

Example: a facility for checking the balance on a prepaid telephone card will be reasonably available if the reader is available on public phones which take such cards.

#### What right do you have to exchange value?

You have a right to exchange any unused value on your stored value facility for an equivalent amount of money if the value is in money terms. Alternatively, you can have the unused value credited towards replacement stored value.

If you wish to be paid money the operator can choose to give you cash or to deposit the money at a bank, building society or credit union nominated by you. The operator can charge a reasonable fee for doing this unless the exchange is because the facility is no longer useable.

#### What are your rights of exchange where the stored value or facility is unusable?

If the facility or the value on it can no longer be used, you have a right of exchange if the remaining amount can be calculated. Operators can require you to make this exchange within a specific time, but must give you at least 12 months.

The operator can refuse to exchange stored value where it can prove that:

- the stored value was not created by an authorised system participant
- the stored value is just a copy of value that has already been exchanged
- you are not acting in good faith.



### Do you have a right to a refund of lost or stolen stored value?

You only have a right to a refund of lost or stolen stored value where the operator and other system participants:

- have, or can create, a reliable record of the amount of stored value in the facility; and
- can stop further transfers of stored value from the facility.

In these situations, the operator must provide a way for you to let them know about the loss or theft at any time. The operator must pay you the amount they could have prevented from being transferred.

### What happens if there is a system or equipment malfunction?

The stored value facility operator is liable to you for any losses to the amount of stored value caused by system or equipment malfunction unless you knowingly caused the malfunction.

## D. Complaints

What if you have a complaint about an EFT transaction or a stored value facility?

If you have a complaint, you should start by raising the matter directly with the account institution or stored value operator. All account institutions and stored value

operators that sign up to the EFT Code must have procedures for handling complaints which must meet certain minimum standards.

The EFT Code imposes time limits for resolving complaints. The account institution or stored value operator should resolve your complaint within 21 days. If it doesn't, it must write to you and explain that it needs more time. If this is the case, then unless there are exceptional circumstances, it must complete its investigation within a total of 45 days. If it does not, you must be told the reasons for the delay, be given monthly updates, and be told when you can expect an answer to your complaint.

If your complaint involves a credit or charge card, different rules might apply which mean that it may take a longer period of time to resolve the complaint.

Account institutions and stored value operators must make sure that their systems can generate sufficient records so that transactions can be traced and checked and errors can be identified and corrected. When considering your complaint, they must rely upon established facts and not inferences unsupported by evidence.

You must be told of the outcome of the investigation into your complaint and the reasons for that outcome.

If the account institution or stored value operator finds it owes you money, it must recredit your account at once and let you know it has done so.

If your complaint is excessively delayed or you are not satisfied with the answer, you must also be given contact details for the external complaints scheme, such as the Australian

Banking Industry Ombudsman, that your account institution or stored value operator belongs to. You can then refer the matter to the external complaints scheme, which will look independently at your complaint and try and resolve the problem.

If your account institution or stored value operator doesn't belong to an external complaints scheme, it must give you contact details for the Consumer Affairs Agency or Small Claims Court/Tribunal in your State or Territory so that you may pursue the matter there.

#### What if a merchant or other party causes the problem?

Your account institution or stored value facility operator can't get out of their obligations to you because another party involved in the transaction caused the problem. Possible other parties include other account institutions, telephone companies, internet providers and merchants.

You don't have to also make a complaint to one of these other parties. You can simply make the complaint to your account institution or stored value facility operator and require them to follow-up on your complaint with the other parties.

#### What are the additional rules when the complaint is about an EFT transaction?

There are some additional rules for dealing with complaints about EFT transactions that

involve accessing an account (ie transactions covered in Section B). These rules do not apply to complaints about stored value facilities.

If the account institution decides that you are partly liable, you are entitled to see certain documents and other evidence (eg transaction logs) relevant to the outcome.

If the account institution does not properly follow the rules about handling complaints in the EFT Code, they may be held liable for part of the transaction in dispute regardless of the eventual result of the complaint. This is to compensate for their inaction or delay.

## E. Privacy

#### How is your privacy protected?

Account institutions and stored value facility operators must comply with the Commonwealth Government's Privacy legislation or with approved Codes established under that legislation.

The EFT Code also contains guidelines for applying the legislation to EFT transactions that access an account. These include telling you if surveillance devices such as visual, sound or data recording may be used in conjunction with your EFT transaction.



## F. Electronic communication

Can your account institution or stored value operator communicate with you electronically?

If you clearly give permission, your account institution or stored value operator can communicate with you electronically (eg by e-mail) rather than on paper through traditional mail. This means, for example, that they can give you the contract in electronic form rather than a paper copy.

Simply posting the information on their website, however, without letting you know that the information is there will not amount to acceptable electronic communication.

## G. How to get more information

Get the EFT Code from ASIC's consumer website at [www.fido.asic.gov.au](http://www.fido.asic.gov.au) or call our Infoline on 1300 300 630.

### Disclaimer.

This guide is only intended to provide you with a general overview of your rights and responsibilities under the EFT Code. You should consult the actual EFT Code or get further advice if a dispute arises.

## ASIC at a glance

The Australian Securities and Investments Commission enforces company and financial services laws to protect consumers, investors and creditors.

We are an independent Commonwealth government body, responsible for consumer protection in shares and other financial investments including managed funds, superannuation, insurance, credit and deposit taking.

We work with other financial, consumer and law enforcement bodies in Australia and internationally.

Like some help on other  
financial matters?

For tips and safety checks on a wide range of  
consumer finance matters, visit fido, our  
consumer web site at

[www.fido.asic.gov.au](http://www.fido.asic.gov.au)



**fido**

Australian Securities & Investments Commission's  
financial tips & safety checks

[www.fido.asic.gov.au](http://www.fido.asic.gov.au)

© Copyright 2002. Australian Securities and Investments  
Commission, GPO Box 9827, Sydney NSW 2001



**ASIC**

Australian Securities & Investments Commission