ASIC
Australian Securities & Investments Commission

REPORT 04

Report on compliance with the Code of Banking Practice, Building Society Code of Practice, Credit Union Code of Practice and EFT Code of Practice

(April 1998 to March 1999)

January 2000

Published by the Australian Securities and Investments Commission
National Office Sydney, GPO Box 4866, Sydney, New South Wales, 1042
January 2000

www.asic.gov.au

ASIC Infoline 1300 300 630

Contents

1 Introduction/Compliance reporting to ASIC

This is ASIC's first report on industry's compliance with the:

- *Code of Banking Practice*
- *Building Society Code of Practice*
- *Credit Union Code of Practice and*
- *Electronic Funds Transfer Code of Practice.*

ASIC has been responsible for monitoring each of these Codes of Practice since 1 July 1998 as part of its new role as consumer protection regulator in the financial services industry. Before July 1998, the Australian Payments System Council monitored industry's compliance with the Codes. Previous reports on industry compliance are in Annual Reports of the APSC.

The reporting period for the Codes of Practice is from April to March of the following year. Because ASIC took over responsibility for the Codes mid-way through the reporting period, it has adopted the same monitoring and reporting process as used by the APSC for the first year. However, ASIC is currently reviewing this process and is considering some form of external monitoring of compliance in addition to the current self-assessment system. ASIC has sought submissions from all institutions as to whether the current monitoring process is adequate.

The industry codes of practice are voluntary codes of conduct and must be adopted by an institution in order to be binding on that institution. The Codes prescribe certain standards of behaviour and practice as between the institution and its customers. Each code addresses three main areas of the customer institution relationship, namely:

- disclosure
- general principles of conduct in relation to day-to-day banking requirements, and
- the resolution of disputes.

Each code also seeks to:

- describe standards of good practice and service and
- sets out the obligations and rights of each institution and customer in these areas.

One of ASIC's new responsibilities is to promote the adoption of industry standards and codes of practice. ASIC will continue to encourage institutions that have not adopted its' industry Code, to adopt and be fully compliant with the Code. ASIC views industry codes as important tools for consumer protection and market integrity.

Monitoring process — Industry codes of practice

The current reporting period for compliance with each of the industry codes of practice is 1 April 1998 to 31 March 1999 (the reporting period). This is the same period as used in previous years so that:

- statistics provided by each institution can be compared, and
- any trends or concerns with the operation of the Codes can be identified.

ASIC required that each institution responsible for reporting on its compliance with the relevant code of practice complete a return which comprised a:

- statement of compliance with the code during the reporting period, and
- report on the number and nature of any disputes that arose during the reporting period.

A copy of the statement of compliance sent to the banking industry is attached to this Report at Appendix 1. A similar statement was sent to credit unions and building societies, reflecting the appropriate code provisions.

Statement of compliance

The statement of compliance must be signed by the institution's chief executive or senior officer. The statement required the institution to report on compliance with the Code during the reporting period. The first part of the statement of compliance required that the institution report separately on whether:

- the institution's internal documents and/or information comply with each section of the Code;
- the institution's procedures comply with each section of the code; and
- appropriate staff are trained in respect of compliance with the code.

Each institution is also obliged to report on:

- whether it has internal assessment systems in place to monitor compliance
- whether it has identified any recurrent areas of non-compliance
- the nature of training provided to staff, and
- any general concerns about the operation of the code.

Disputes

In addition to reporting on compliance, each institution is also required to report to ASIC on:

- the number of disputes that have arisen during the reporting period
- the categories of disputes and
- how the institution has dealt with disputes.

The definition of what constitutes a 'dispute' is substantially the same in each code. A dispute arises and must be reported to ASIC when a customer has complained to the institution about a service and is not satisfied with the response given by the institution. The definition in the Credit Union Code of Practice is slightly wider and includes disputes about credit union products together with services. Complaints or disputes that do not fall within the definition are not required to be reported to ASIC.

Although institutions include in their report statistics on disputes about EFT transactions, it should be noted that the definition of 'dispute' in the industry

codes is much narrower than the definition of ‘complaints’ in the EFT Code of Conduct. All institutions are required to report separately on ‘complaints’ that have arisen in respect of EFT transactions in response to the EFT Code.

2 Code of Banking Practice

The Code of Banking Practice (the Code) covers banking retail operations. It describes standards of good practice and service, promotes disclosure of information and informed relationships between banks and customers and requires that dispute resolution procedures are in place. Currently, there are twenty banks which have significant retail operations and at 31 March 1999, seventeen have adopted the Code. The remaining three banks are continuing to move towards full adoption of the Code.

- The Bank of China has not yet taken action to ensure that its internal documents are fully compliant with the Code. However, an internal and external dispute resolution process is in place to resolve disputes that arise. ASIC has been advised that the Bank of China anticipates that it will be fully compliant with the Code by the end of the next reporting period.
- The AMP Bank has advised ASIC that it has joined the Australian Banking Industry Ombudsman scheme (ABIO) and anticipates being fully compliant with the Code by early 2000.
- The ING Bank adopted the Code in August 1999, after the current reporting period. It will report on compliance with the provisions of the Code in the next reporting period.

A list of banks that have adopted the Code is included later in this part. ASIC will continue to encourage banks to adopt the Code and to be fully compliant with the provisions of the Code.

Compliance with the Banking Code of Practice

Completed compliance statements were received from all banks that have adopted the Code.

The first part of the statement required that banks report to ASIC on any instances in which the bank's internal documentation and procedures failed to comply with the particular provisions of the Code.

Two banks reported on a failure in this regard during the relevant period:

- In the first instance, a bank reported that it had not notified customers of variations to interest rates in respect of money market deposits in accordance with the Code. Interest rates applicable to these products follow the changes to interest rates in the market so may change daily. The bank concerned submitted that it was not possible to notify customers about a change in interest rates prior to the date upon which the change is effected as required by the Code. In these circumstances, it was requested that the Code be reviewed to exclude money market deposits from the requirements in clause 9.3 of the Code, given that the terms and conditions of the product disclose that interest rates can vary daily. This issue will be considered during the review of the Code in 2000.
- One other instance of non-compliance was reported, but the issue was rectified immediately, once it was identified.

In addition to ensuring that internal documentation complies with the Code, banks are also required to report on any examples of recurrent non-compliance with the Code.

During this reporting period, three banks reported that there had been recurrent non-compliance with the Code. In each instance, the failure was either rectified or procedures have been implemented to ensure future compliance during the reporting period. In each case, the non compliance was identified through an internal compliance audit:

- In two instances, each bank had failed to provide Code compliant information to customers, and
- In the third case, the bank failed to systematically complete complaint forms. This arose as a result of staff not being aware of requirements and was rectified through additional training.

Each of the banks reported that internal procedures were compliant with the Code and that staff were properly trained to understand the requirements of the Code.

Monitoring compliance within banks

The majority of banks indicated that management, senior compliance officers or auditors had an active role in monitoring compliance with the Code. Some banks have in place formal internal reporting structures that require issues of compliance to be reported directly to the Board and appropriate compliance committees. This meets the standards set by the Australian Standards on Compliance Programs (AS 3806–1998) that the senior executive responsible for overseeing compliance have direct access to the chief executive and any audit or compliance committees.

Internal assessment systems are in place within each reporting bank to monitor compliance with the Code. The systems vary between different banks:

- Some banks have comprehensive assessment programs in place that actively identify non compliance with the Code across all aspects of the business.
- Other systems are activated periodically as part of an internal audit program.
- In some cases, exception reports are issued if there has been a failure to comply with a provision of the Code.

Banks have adopted various approaches to assess compliance. These include:

- detailed compliance plans and programs
- operational procedure and compliance manuals
- internal auditing
- incorporation of compliance into internal processes
- checklists and
- due diligence processes.

Most banks reported that compliance units were in place to monitor compliance with both the law, and the provisions of the Code in all aspects of the business.

Training of staff

All banks conduct training of staff in relation to the Code, although the extent to which ongoing training of staff is provided varies between individual institutions. Most banks reported on the methods of training and the materials used. It is clear that in some instances, comprehensive and ongoing training is conducted to ensure staff understand the practical effect of the Code.

Training initiatives include presentations and seminars, training manuals, internal communication, induction training, videos and computer based training programs.

Dispute statistics

Statistics on Code-related disputes dealt with internally by a bank and Code-related disputes referred to the ABIO must be reported to ASIC as part of the monitoring process.

A ‘dispute’ must be reported to ASIC if it arises as a result of a customer’s complaint about a banking service which has been rejected by the bank, and the customer has asked for the decision to be reviewed. Disputes are categorised according to the section of the Code which is applicable. The dispute may relate to a breach of the Code or about the provisions of services covered by the Code.

Banks are also required to report on the number of personal accounts open in the bank at the end of the reporting period and the number of transactions on those accounts during the period.

For the period April 1998 to March 1999, banks reported:

- 8551 disputes
- 40,012,410 personal accounts open as at 31 March 1999 and
- 2,922,670,655 transactions conducted through those accounts.

In the 1997–1998 reporting period, banks reported 4759 disputes as against 2.6 billion transactions.

This illustrates that in 1998–1999 the number of disputes as against transactions was higher than in 1997–1998. However, the number of total disputes is still low. This may, in part, be due to the narrow definition of ‘dispute’ within the Code.

Disputes resolved internally

Banks are only required to report on those disputes resolved internally — the ABIO reports separately on disputes referred to it. Of those disputes considered internally, the majority of disputes were resolved in favour of the customer or were resolved by mutual agreement.

The majority of complaints received during the 1998–1999 reporting period relate to the disclosure of fees and charges:

- This does not include disputes relating to the existence, application or level of fees and charges.
- However, it does include the disclosure of fees and charges in respect of an account or banking service.

Of the total disputes received, a significant number of disputes have also been recorded in relation to PIN-based EFT transactions. This includes disputes arising from unauthorised transactions and system malfunction (but does not include complaints in relation to which the decision of the institution has been accepted by the customer. These are, however, reported under the EFT Code.)

Other aspects of service delivery, such as loss of documents, failure to reply to correspondence, fraudulent transactions or bank error leading to dishonour of transactions, also featured prominently as a source of disputes.

ABIO statistics

The ABIO reports to ASIC on the number and types of disputes which were referred to it regarding breaches of the Code or the provision of services covered by the Code curing the reporting period. These disputes were referred to the ABIO in circumstances where the customer did not accept the decision of the internal resolution process offered by the bank and decided to take the matter further.

The ABIO considered 1886 disputes regarding the Code in the 1998–1999 reporting period, 500 of which carried over from the previous reporting period.

The majority of Code-related disputes referred to the ABIO arose from complaints that a bank has failed to act in accordance with the customer's instructions or authority or on undertakings given to the customer.

Most of these complaints were resolved by the bank after referral by the ABIO. A significant number of disputes were referred to the ABIO in relation to PIN-based EFT transactions and delivery of banking services. Around half of the complaints made about PIN-based EFT transactions were resolved by the ABIO during the reporting period. Some were resolved by the customer and bank directly, and others remain outstanding at the end of the reporting period.

Table 1: Code of Banking Practice
Dispute statistics, April 1998 – March 1999

Personal accounts open at 31 March 1999: 40,012,410

Transactions conducted during year: 2,922,670,655

		Disputes resolved			
Dispute category	*Total disputes during year*	*Customer's favour*	*Mutual ageement*	*Bank's favour*	*Disputes outstanding at 31 March 1999*
Disclosure					
Terms & conditions	542	120	178	227	17
General info	371	156	94	97	24
Fees & charges	1737	749	379	455	154
Cost of credit	136	31	42	52	11
Foreign currency transactions	54	25	14	10	5
Variations to terms & conditions	195	64	42	78	11
Total disclosure	*3035*	*1145*	*749*	*919*	*222*
Banking service delivery					
Statements	358	231	86	28	13
Account combination	516	295	61	131	29
Account debiting/crediting	514	266	117	84	47
Proper interest rate, fee, charge	913	369	205	276	63
Instructions	333	164	97	51	21
EFT(PIN based)	1157	228	212	351	366
Other service delivery	1150	236	666	149	99
Advertising	55	15	16	18	6
Total, banking services	*4996*	*1804*	*1460*	*1088*	*644*
Privacy & confidentiality					
Disclosure to related entities	18	6	7	5	0
Other aspects: privacy/confidentiality	163	50	44	36	33
Provision of credit	261	57	82	86	36
Guarantees	15	3	5	3	4
Dispute resolution process	63	21	28	10	4
Total, privacy & confidentiality	*520*	*137*	*166*	*140*	*77*

Total, all disputes	**8551**	**3086**	**2375**	**2147**	**943**

Banks which have adopted the Banking Code of Practice

Adelaide Bank

Arab Bank

Australia and New Zealand Banking Group Limited

Bank of Queensland Limited

BankWest

Bendigo Bank

Citibank Limited

Colonial State Bank

Commonwealth Bank of Australia

HongKong Bank of Australia

Macquarie Bank

National Australia Bank

Primary Industry Bank of Australia

St. George Bank

Suncorp-Metway Limited

Trust Bank

Westpac Banking Corporation

Banks intending to adopt the Banking Code of Practice

AMP Bank

Bank of China

ING Mercantile Mutual Bank

3 Building Society Code of Practice

The Australian Association of Permanent Building Societies released the Building Society Code of Practice (BSCP) in October 1994. The BSCP reflected the principles of the Code of Banking Practice, although it was subsequently amended to ensure compatibility with the Uniform Consumer Credit Code, and became fully operational on 1 November 1996.

There are currently 19 building societies in Australia. Of these:

- 10 have adopted the BSCP (one adopted the BSCP in November 1998, mid-way through the reporting period). One building society that amalgamated with a credit union adopted the Credit Union Code of Practice and reports in line with that Code.
- one intends to adopt the Code in the next reporting period.
- one building society has informed ASIC that it does not intend to adopt and code of practice.
- six building societies in Queensland have developed their own code of practice which is not monitored. This is of concern to ASIC as the consumer protection regulator of the financial services industry. Without a transparent and objective monitoring process, it is impossible to assess the level of compliance with the code's provisions. Although this code is similar to the BSCP, it does not require a building society to have in place an external dispute resolution process for customers which is a basic consumer protection principle. ASIC will liaise with individual building societies and the representative body of building societies to promote adoption of industry codes. These six building societies are listed at the end of this part.

Unlike the Credit Union Code of Practice and the Code of Banking Practice, a building society is not required to refer a customer's complaint to an external and independent dispute resolution process if it considers that the dispute is trivial, misconceived or lacking in substance. This reduces the protection afforded to consumers by the BSCP and it is an issue for ASIC that some consumers may have genuine disputes that are not adequately considered.

Statements of compliance

Completed statements of compliance were received from ten building societies, although one reported against the Credit Union Code of Practice. There were no reported deficiencies against any section of the BSCP, in respect of documentation or information, procedures or training.

Monitoring compliance within building societies

All reporting building societies have internal assessment programs in place, to monitor compliance although, as with banks, the standard and type of assessment differs between each institution:

- Some institutions conducted a thorough audit prior to adoption of the BSCP and any change or variation in documentation or procedures requires a legal

officer to check those changes to ensure compliance with the BSCP. This system does not, however, provide a check on ongoing compliance.

- Other institutions conduct regular audits (by checklists or questionnaires) to ensure compliance.
- Although many building societies are small institutions, and have a relatively small client base, several institutions reported the appointment of designated compliance officers who are responsible for ensuring retail operations comply with the BSCP.
- Other institutions nominate line management, auditors or other appropriate staff as being responsible for compliance with the BSCP.

No instances of recurrent non-compliance were reported by any building society.

Training of staff

All building societies have in place formal materials for training staff about the BSCP. Different institutions have different training methods including 'on the job' training, induction training, periodic training, internal communication and seminars.

Some societies require staff to attend regular training sessions, which include ongoing training on BSCP compliance.

None of the ten building societies expressed any concerns about the current operation of the BSCP.

Dispute statistics

The definition of 'dispute' in the BSCP is substantially the same as the definition in the Banking Code of Practice. All building societies reported to ASIC on the disputes received during the reporting period.

During the period April 1998 to March 1999, 84 code-related disputes were recorded by building societies. This is a substantial increase from the previous reporting period in which only 17 disputes were recorded. During the 1998–1999 reporting period:

- 973,244 personal accounts were reported as open and
- 55,430,950 transactions recorded.

Although these figures indicate that the number of open accounts has decreased slightly from the previous reporting period, the number of transactions have increased from 47,620,593, as recorded in the 1997–1998 reporting period.

The largest number of internal disputes related to the disclosure of fees and charges and, of these, most were resolved in favour of the customer. A number of disputes were also recorded in relation to the incorrect application of an interest rate, fee or charge, most of which were resolved through mutual agreement. However, given the small number of complaints involved, it is not possible to analyse the results to identify any trends or issues within the industry.

Unlike banks and credit unions, building societies do not have an industry-wide external dispute resolution process. Rather, each building society has a dispute resolution process that is based on a model developed by the Australian Association of Permanent Building Societies. Building societies were asked to report on disputes that were not resolved by the internal process and were referred to an external scheme for resolution. Only two building societies reported disputes that were referred to the external process: three disputes relating to the provision of credit, and four relating to PIN-based EFT transactions were resolved by external schemes.

Table 2: Building Society Code of Practice
Dispute statistics, April 1998 – March 1999

Personal accounts open at 31 March 1999 973,244
Transactions conducted during year 55,430,950

		Disputes resolved			
Dispute category	*Total disputes during year*	*Customer's favour*	*Mutual ageement*	*Building societies' favour*	*Disputes outstanding at 31 March 1999*
Disclosure					
Terms & conditions	4	3	1	0	0
General information	5	2	2	0	1
Fees & charges	37	28	5	2	2
Cost of credit	4	2	1	0	1
Variations to terms & conditions	0	0	0	0	0
Service delivery					
Statements	1	1	0	0	0
Account combination/closure	1	1	0	0	0
Account debiting/crediting	6	2	2	0	2
Proper interest rate, fee, charge	12	1	11	0	0
Instructions	4	0	1	3	0
EFT (PIN based)	4	1	0	3	0
Other service delivery	0	0	0	0	0
Advertising	0	0	0	0	0
Privacy & confidentiality					
Disclosure to related entities	0	0	0	0	0
Other aspects: privacy/confidentiality	0	0	0	0	0
Provision of credit	6	3	2	1	0
Guarantees	0	0	0	0	0
Dispute resolution process	0	0	0	0	0
Total, all disputes	**84**	**44**	**25**	**9**	**6**

Societies which have adopted the Building Society Code of Practice

Armidale Building Society Limited

Australian Unity Building Society Limited

Bass & Equitable Building Society Limited

GIO Building Society Limited

Home Building Society Limited

Hume Building Society Limited

Illawarra Mutual Building Society Limited

IOOF Building Society Limited

Lifeplan Australia Building Society Limited
(adopted the Credit Union Code of Practice)

Newcastle Permanent Building Society Limited

NRMA Building Society Limited

Societies intend adopting the Building Society Code of Practice

Greater Building Society Limited

Societies which have not adopted the Building Society Code of Practice but have adopted a separate code of practice.

First Australian Building Society Limited

Heritage Building Society Limited

Mackay Permanent Building Society Limited

Pioneer Permanent Building Society Limited

The Rock Building Society Limited

Wide Bay Capricorn Building Society Limited

Societies which have not adopted a code of practice

Maitland Mutual Building Society

4 Credit Union Code of Practice

The Credit Union Code of Practice (CUCP) was released in 1994 but became fully effective on 1 November 1996. During the reporting period, there were 248 credit unions in Australia:

- *242 which had adopted the CUCP. Of these, 196 are members of the Credit Union Dispute Reference Centre and 41 are members of other dispute resolution schemes.*
- *6 credit unions have not adopted a Code, although one has indicated that it will adopt the CUCP in the next reporting period.*

One building society that amalgamated with a credit union has also adopted the CUCP. There is a list of all credit unions at the end of this part.

Statements of compliance

Statements of compliance were returned to ASIC for each credit union that has adopted the CUCP. Six credit unions reported instances of non-compliance with the CUCP during the reporting period. In three instances, it was reported that the credit union's information or documents did not comply with the CUCP. In two cases, the credit union did not have procedures in place to ensure compliance with particular provisions of the CUCP and in three cases, the credit union did not train staff to comply with the CUCP.

In each instance, steps were taken to either correct the non-compliance, or measures were being considered to ensure compliance in the next reporting period.

Monitoring compliance

Some of the reporting credit unions are too small to require a separate assessment system to ensure compliance. However, in each of these cases, responsibility for compliance rests with the manager and staff are informed about provisions of the CUCP to ensure compliance in the day-to-day conduct of the business.

The majority of credit unions, however, have a compliance assessment system in place. However, the form of the compliance system varies between individual institutions and the extent to which it can assess the degree of compliance in the retail business divisions of the credit union:

- Some compliance units operate actively to check each division of the business to ensure compliance with each section of the CUCP.
- Other systems are only activated in the event that the institution develops new documents or varies existing documents.
- Some institutions rely on reports which identify anomalies or non-compliance with a particular provision of the CUCP.
- ASIC was advised that some credit unions incorporate compliance into their internal systems, but do not actively check to ensure each area of the business is compliant.

- Other institutions rely on staff's knowledge of compliance and do not actively check to ensure that he business unit complies with the CUCP.

The methods of monitoring compliance also vary:

- Some institutions have designated compliance officers or units which monitor compliance across all business areas.
- Other institutions use exception reports which highlight non-compliance.
- Most credit unions, however, appear to rely on internal auditing or 'checks' to monitor compliance.

There have been a few instances where recurrent non-compliance with the CUCP has been reported, but in each case, the breach was rectified once it was identified:

- In one case, the failure had arisen as a result of poor staff knowledge which was addressed through training.
- One credit union reported on the existence of an informal dispute resolution process which was addressed through the development and circulation of a dispute resolution policy.
- Three institutions reported on minor errors with documents, including the failure to issue terms and conditions. This was addressed through redesigning documents to minimise the number of documents to be issued to customers.

Training of staff

As with the compliance assessment systems in place, institutions reported a range of different training methods:

- Some institutions 'outsource' their training requirements, but ensure that CUCP compliance training is included in the external materials.
- Most institutions report that training is conducted internally though presentations, staff training sessions, internal testing, videos and the development of training manuals.
- A number of credit unions rely on the training support offered by the Credit Union Services Corporation of Australia Limited (CUSCAL).
- A few of the smaller institutions limit training to 'on-the-job' training or provide training for new staff members and circulate manuals should staff require up to date training on CUCP related issues.

Operation of the CUCP

Some credit unions took the opportunity to comment on the operation of the CUCP:

- A number of institutions commented on the amount of paperwork required by the CUCP and noted that members queried the relevance of the material provided.

- One credit union expressed the opinion that the CUCP discriminated against smaller credit unions which lacked the resources to have in place a comprehensive compliance system which recorded dispute statistics and met the disclosure requirements.
- Some credit unions expressed the view that some of the requirements of the CUCP were costly, onerous and unnecessary, such as notification to a customer of the fact that accounts may be combined.

However, the majority of credit unions had no comments in respect of the operation of the CUCP.

Dispute statistics

The CUCP defines a 'dispute' as arising where a credit union's response to a complaint by a member about a credit union product or service provided to that member is not accepted by that member. The CUCP requires a credit union to have an internal process for handling a dispute with Members and to make available an external and impartial dispute resolution process. Currently, this external process is provided by several different regional organisations. The largest dispute resolution scheme for credit union is the Credit Union Dispute Reference Centre (CUDRC). There are three other dispute resolution schemes: the Credit Union Ombudsman in Queensland, Financial Services (Tasmania) Pty Limited in Tasmania and End-dispute in Western Australia.

It was reported that during the 1998–1999 reporting period there were:

- 2,069, 568 personal accounts open at 31 March 1999
- 137,413,595 transactions.

Because of the large number of credit unions, ASIC has followed the procedure adopted by the APSC and relied on the CUDRC to provide statistics about the number and nature of disputes to credit unions within the reporting period. However, the statistics were not processed until mid-1998 and the CUDRC could only provide statistics for the period 30 June 1998 to 31 March 1999. End-dispute has provided statistics to ASIC and these have been incorporated in the final statistics. Statistics have not been provided by either Financial Services (Tasmania) Pty Limited or the Credit Union Ombudsman. ASIC will ensure that arrangements are made to obtain statistics from these schemes in future reporting periods.

A total of 767 disputes were received by the CUDRC in the reporting period:

- One-third of these disputes related to service delivery including credit union error leading to dishonour, faults in funds transfers or allegedly fraudulent transactions by third parties.
- A significant number of disputes were also received in relation to PIN-based EFT transactions, such as unauthorised transactions or ATM malfunction.
- Errors in crediting or debiting accounts, including payments to the wrong account, accounted for a significant number of disputes.

Table 3: Credit Union Dispute Reference Centre Dispute statistics, 30 June 1998–31 March 1999

Description of complaint	*Number of complaints*
Disclosure	
Terms & conditions	14
General Information	27
Fees and charges	43
Cost of credit	3
Foreign currency transactions	3
Variation to terms & conditions	10
Service delivery	
Statements	11
Account combination/closure	25
Account crediting/debiting	100
Proper interest rate, fees or charge	68
Instructions	50
EFT PIN-based	111
Other aspects	255
Advertising	0
Privacy	
Disclosure to related entities	8
Other aspects of privacy/confidentiality	20
Provision of credit	4
Guarantees	7
Dispute resolution schemes	8
Total, all complaints	**767**

Individual credit unions have also reported to ASIC on disputes that have been dealt with internally. These statistics are reported separately in Table 4.

Table 4: Credit union disputes dealt with internally
Dispute statistics, 1 April 1998–31 March 1999

Personal accounts **open at 31 March 1999: 2,069, 568**

Transactions **conducted during year: 137,413,595**

Dispute category		*Resolution*			
Dispute category	*Total disputes during year*	*Customer's favour*	*Mutual ageement*	*Credit Union's favour*	*Disputes outstanding at 31 March 1999*
Disclosure					
Terms & conditions	0	1	2	2	1
General information	0	0	0	0	0
Fees & charges	7	0	3	4	0
Cost of credit	1	1	0	0	0
Foreign currency transactions	5	1	1	2	1
Variations to terms & conditions	4	0	0	4	0
Service delivery					
Statements	0	0	0	0	0
Account combination/ closure	1	0	1	0	0
Account debiting/crediting	12	8	2	2	0
Proper interest rate, fee, charge	6	4	1	1	1
Instructions	4	2	1	0	1
EFT (PIN -based)	156	94	14	35	13
Other aspects of service delivery	23	6	13	3	1
Advertising	0	0	0	0	0
Privacy & confidentiality					
Disclosure to related entities	3	0	3	0	0
Other aspects: privacy & confidentiality	2	2	0	0	0
Provision of credit	*8*	*2*	*1*	*4*	*1*
Guarantees	*0*	*0*	*0*	*0*	*0*
Dispute resolution period	*0*	*0*	*0*	*0*	*0*
Total, all disputes	**232**	**121**	**42**	**57**	**19**

Credit unions which have adopted the Credit Union Code of Practice

Access Credit Union (NSW) Limited
ACT Hospitals & Health Employees' Credit Union Co-Operative
Advantage Credit Union
Albury Murray Credit Union
Amcor Credit Co-operative
AMP Employees' & Agents Credit Union Limited
Arlem Credit Co-operative
Auburn Municipal Council Employees' Credit Union
Austral Credit Union Co-operative
Australian Central Credit Union
Bananacoast Community Credit Union
Bankstown City Credit Union
Bemboka Community Credit Union
Berrima District Credit Union
BHP Group Employees' Co-operative
Big River Credit Union
Blue Mountains & Riverlands Community Credit Union
BP Employees' Credit Co-operative
Brookvale & Mona Vale Bus Depots Credit Union
BTR Employees' Credit Union
B-W Albury Employees' Credit Union
Calare Credit Union
Capral Credit Union
Capricornia Credit Union
Carboy (SA) Credit Union
Carboy Credit Co-operative
Central West Credit Union
Cessnock City Council Employee's Credit Union
Circle Credit Co-operative
City Coast Credit Union
Coastline Credit Union
Collie Miners' Credit Union
Combined Australian Petroleum Employees' Credit Union
Community First Credit Union
Companion Credit Union
Comtax Credit Union
Connect Credit Union
Country First Credit Union

Credit unions which have adopted the Credit Union Code of Practice

CPS Credit Union (SA)
CPS Credit Union Co-operative (ACT)
CPS Credit Union Co-operative (TAS) Ltd
Credit Union Australia
Credit Union Incitec
CSR Employees' Credit Union
Dairy Farmers Credit Union Ltd
Defence Force Credit Union
Dependable Credit Union
Discovery Credit Union
Dnister Ukrainian Co-operative Credit Society
Education Credit Union Co-operative
Elcom Credit Union
Electricity Credit Union
Encompass Credit Union Ltd
Endeavour Credit Union
Ericsson Employees' Credit Co-operative
Esso Employees' Credit Union
Eurobodalla Credit Union
Family First Credit Union Ltd
Fire Brigades Employees' Credit Union
Fire Service Credit Union
Firefighters Credit Co-operative
First Gas Employees Credit Union
First Option Credit Union
First Pacific Credit Union
Fitzroy & Carlton Community Credit Co-Operative
Flinders Credit Union Co-operative
Flying Horse Credit Union Co-operative
Ford Co-operative Credit Society
Forestry Commission Staff Credit Union
Gateway Credit Union Ltd (formerly C.B.O.A. Credit Union Ltd)
Geelong & District Credit Co-operative
Geelong Refinery Club Co-operative Credit Society Limited
GIO Staff Credit Union
GMH (Employees) QWL Credit Co-operative
Gold Credit Co-operative
Goldfields Credit Union

Credit unions which have adopted the Credit Union Code of Practice

Gosford City Credit Union
Goulburn Murray Credit Union Co-operative
Grand United Credit Union
Hardie Employees' Credit Union
Health Services Credit Union Society
Heritage Isle Credit Union
Hibernian Credit Union
Holiday Coast Credit Union Ltd
Horizon Credit Union
Hoverla-Ukrainian Credit Co-operative
Hunter United Employees' Credit Union
Intech Credit Union
Island State Credit Union
Kalyna Ukrainian Credit Union Society
Karpaty Ukrainian Credit Union
La Trobe Country Credit Co-operative
La Trobe University Credit Union Co-operative
Laboratories Credit Union
Latvian-Australian Credit Co-operative Society
Lifeplan Australia Credit Union
Lithgow Mutual Credit Union
Lithuanian Co-operative Credit Society Talka Limited
Lysaght Credit Union
Macarthur Credit Union
Macaulay Community Credit Co-operative
Macquarie Credit Union
Maitland City Council Employees' Credit Union
Maitland Community Credit Union
Maleny & District Community Credit Union
Manchester Unity (NSW) Credit Union
Manly Warringah Credit Union
Manning Local Government Employees' Credit Union
Maritime Workers of Australia Credit Union
Maroondah Credit Union
Media Credit Union Queensland
Melbourne Credit Union
Members Australia Credit Union Limited
Metropolitan Credit Union

Credit unions which have adopted the Credit Union Code of Practice

Money Wise Credit Union (formerly NSW Public Service Board Staff)
MSB Credit Union
NACOS Credit Union
New England Credit Union
Newcastle Bus Credit Union
Newcastle City Council Employees' Credit Union
Newcom Colliery Employees' Credit Union
North East Credit Union Co-operative
North West Country Credit Union Co-operative
Northern Districts Credit Union
Northern Inland Credit Union
Northern Rivers Credit Union Ltd
Northern Rivers Electricity Credit Union
Nova Credit Union
NRMA Employees' Credit Union
NSW Teachers Credit Union
Northern Territory Credit Union Ltd
Old Gold Credit Union Co-operative
Orana Credit Union
Orange Credit Union
Parkes District Credit Union Ltd
Peel Valley Credit Union
Phoenix (N S W) Credit Union
Plenty Community Credit Union
Point Henry Credit Co-operative
Police & Nurses Credit Society
Police Association Credit Co-operative
Police Credit Union
Polish Community Credit Union
Post-Tel Credit Union
Power Credit Union
Powerstate Credit Union
Professionals First Credit Union
Prospect Credit Union
Pulse Credit Union
Punchbowl Credit Union
Qantas Staff Credit Union
Queensland Community Credit Union

Credit unions which have adopted the Credit Union Code of Practice

Queensland Country Credit Union
Queensland Police Credit Union
Queensland Teachers' Credit Union
Queenslanders Credit Union
RACV Employees' Credit Union Co-operative
Raleigh Park Employees' Credit Union
Randwick Credit Union
Reliance Credit Union
Resources Credit Union
Rothville Credit Union
RTA Staff Credit Union Limited
Satisfac Direct Credit Union
Savings & Loans Credit Union (SA)
Savings & Loans Credit Union Co-operative Society
Select Credit Union
Shell Employees' Credit Union
Shoalhaven Paper Mill Employees' Credit Union
Snowy Mountains Credit Union
Softwoods Credit Union Co-operative
Sosecure Co-operative Credit Union
South East Community Credit Society
South West Credit Union Co-operative
South West Slopes Credit Union
Southern Cross Credit Union
St Marys Swan Hill Co-operative Credit Society
St Patrick's Mentone Co-Op Credit Society
St Philip's Credit Co-operative
Stanley Works Employees' Credit Co-operative
SGE The Service Credit Union
(formerly known as State Government Employees' Credit Union)
StateHealth Credit Union
StateWest Credit Society
Sutherland Credit Union
Sutherland Shire Council Employees' Credit Union
Sydney Credit Union
TAB Staff & Agents Credit Union
Tartan Credit Union
Telstra Credit Union

Credit unions which have adopted the Credit Union Code of Practice

The Breweries Union Co-Operative Credit Society
The Broken Hill Community Credit Union
The Credit Union of Canberra
The Gympie Credit Union
The Herald Credit Co-operative
The Illawarra Credit Union
The Manly Vale Credit Union
The Police Department Employees' Credit Union
The Queensland Railways Institute Credit Union
The Scallop Credit Union Co-operative
The Stafford Parish Credit Union
The Summerland Credit Union
The TAFE Credit Union
The United Ancient Order of Druids (NSW) Credit Union
The University Credit Society
Transport Industries Credit Union
Traditional Credit Union
Transcomm Credit Co-operative
Uni Credit Union
Unicom Credit Union
United Credit Union
Upper Hunter Credit Union
Victoria Teachers Credit Union
Waverley Bus Depot Employees' Credit Union
W.A.W. Credit Union Co-operative
Waverley Credit Union Co-operative
Welding & Gases Employees' Credit Co-Operative
Westax Credit Society
Western City Credit Union
Woolworths/Safeway Employees' Credit Co-operative
Wyong Shire Council Employees' Credit Union
Yarrawonga Credit Union Co-operative
Yennora Credit Union

Credit unions intending to adopt the Credit Union Code of Practice

Queensland Professional Credit Union

Credit unions not adopting the Credit Union Code of Practice

Bardon Parish Credit Union

Broadway Credit Union

Hardie Employees' Credit Union

Newcastle Credit Union

Wapet Staff Credit Union

5 Electronic Funds Transfer Code of Conduct

The Electronic Funds Transfer Code of Conduct (EFT Code) has been operative since 1989. Since its operation, the APSC has monitored compliance with the Code by card issuers. This is the first year in which ASIC has undertaken the monitoring process and coincides with a review of the EFT Code which is currently being undertaken by ASIC with industry and consumer representatives. This review of the EFT Code is aiming to expand the Code to cover all forms of consumer EFT technology.

Report by the Treasury and the ACCC on the operation of the EFT Code

The current review of the EFT Code follows from the recommendations of a general review of the Code conducted by the Australian Competition and Consumer Commission (ACCC) and Treasury in 1998 (the Review). As a result of this Review, the Code was amended and institutions were required to implement the amendments by October 1998, mid-way through the reporting period.

However, because some of the proposed changes required the reprinting of documents and technological changes, this date was extended until April 1999. There is a copy of the amended EFT Code later in this part.

In order to monitor the amendments, the statement of compliance developed by the APSC was amended to incorporate the changes to the EFT Code. Seven additional questions were incorporated into the EFT Code Checklist. A copy of the EFT Code Checklist is included later in this part. Institutions were only required to complete the additional questions if the changes had been incorporated into the system. Thirty-one institutions replied to the additional questions, although not all amendments had been fully implemented by all institutions. The remaining institutions were working towards full implementation of the changes by April 1999 and will report on this in the next reporting period.

The Review resulted in some substantive changes to the EFT Code and recommended some changes to the general operation of the Code. More specifically, the Review recommended that the monitoring process be reviewed to consider whether, among other things, rationalisation of the compliance checklist was needed and the appropriateness of external auditing and whether a new format for the complaint statistics was required. ASIC will consider these recommendations as part of the process of reviewing the procedures for the Code.

Scope of the EFT Code

The EFT Code currently covers consumer transactions involving the use of a card and a personal identification number (PIN). This includes ATM cash transactions, electronic payments (such as EFTPOS) and transactions made through terminals before a teller with the use of a card and PIN. The EFT Code regulates the rights and obligations of both card issuers and consumers (or cardholders) and establishes the liability for disputed transactions and the nature or extent of that liability. In addition to articulating the rights and obligations of

each party to a transaction, the EFT Code also sets out requirements for handling disputes, the requirement to disclose certain information to customers, privacy and security obligations and the necessity of an audit 'trail'.

Card issuers must provide to all cardholders, conditions of use documents which outline the rights and obligations between the parties and includes a warranty that the card issuer will comply with the Code. A list of all card issuers that have adopted the EFT Code appears at the end of this Part.

Monitoring process: methodology

In order to test compliance with the EFT Code, card-issuers were required to complete the following documents:

- EFT Code checklist
- Assessment of the EFT Security Guidelines and
- Dispute statistics.

Copies of these documents are include in this part. The first part of the documents, which contains the checklist for the EFT Code, is designed to assist institutions check that they have complied with all aspects of the Code. Most questions in this part require yes/no answers. Seven new questions were inserted into this section to cover the changes to the Code. There are 37 questions in the checklist, relating to each section of the Code, including training initiatives to train staff in relation to the Code requirements.

Part B of the report requires each card issuer to report on the implementation of EFT security guidelines and an assessment of the suitability of the guidelines.

The final part of the report, Part C, requires the institution to report on the total number of EFT transactions during the period and statistics on the complaints and resolution of complaints within this period.

Compliance report

There are fifty-eight card issuers who have adopted the Code, fifty-seven of which completed the monitoring report. No response has been received from one major card issuer, Diners Club International Pty Limited. Only two of the fifty-eight institutions are charge card issuers, the remaining participants were financial institutions. One finance company and one bank have recently adopted the Code and will report in the next reporting period.

The Code checklist indicates that most card-issuers complied with the requirements of the EFT Code. Thirty-three instances of non-compliance were reported to ASIC. In most cases, the breaches were minor matters that were rectified as soon as they were identified. Of these, only one card issuer reported a failure to rectify non-compliance during the reporting period. In this case, the matter related to the failure of receipts to show the balance in the account after a transaction, when accessed through an ATM. This institution is pursuing technical advice to remedy the fault. All other instances of non-compliance were corrected.

In respect of staff training, 50 card issuers reported on training. In all cases, the card issuer had a procedure manual available to staff detailing the EFT Code requirements. Most also had 'on-the-job' training which included team meetings, videos, material which could be 'self-taught' and a few institutions also had computer-based interactive training for staff.

EFT complaints

Card issuers reported a total of 1,710 million EFT transactions in the year to March 1999. From these transactions, there were 73,125 complaints:

- around two-thirds of the complaints (43,561) related to system malfunctions and
- around one-third related to unauthorised transactions (25,463).

Disputes arising in relation to system malfunctions were generally resolved in favour of the card holder. However, disputes regarding unauthorised transactions were generally resolved in favour of the card issuer.

Table 5: Incidence of EFT Complaints April 1998 to March 1999

(Per million transactions)

Complaint type	*Issuer liable*	*Customer liable*	*Outstanding*	*Total*
Unauthorised	5	11	1	16
System malfunction	23	3	1	26

The incidence of complaints about unauthorised transactions has slightly decreased from the previous reporting period, from 17 to 16 per million transactions.

When viewed against institutional types, the incidence of complaints about unauthorised transactions from building society and credit union customers has increased significantly since the last reporting period. The number of complaints from bank customers in the same period has decreased slightly.

Table 6: Major institutional groups Complaints about unauthorised transactions: April 1998 to March 1999

(Per million transactions)

Institution	*Issuer liable*	*Customer liable*	*Outstand-ing*	*Total (last year)*
Banks				
Major	6	12	1	18 (20)
Minor	1	5	0	6 (5)
Building societies	*12*	*15*	*0*	*27 (17)*
Credit unions	*15*	*5*	*2*	*20 (14)*
Total, all institutions	**5**	**11**	**1**	**16 (17)**

Of those transactions reported as unauthorised, and in relation to which the cardholder was found to have been liable, almost half arose from the customer's negligence or delay (8070) and half related to confusion over the processing date or merchant name (8168). Only 169 unauthorised transactions arose as a result of a cardholder's unreasonable delay in notification of loss or theft of card whereas, 7901 arose as a result of a cardholder's negligence with PIN.

In respect of disputes about unauthorised transaction in which the issuer was liable, most were settled without formal investigation, but in circumstances in which it was clear that the cardholder had not contributed to the loss.

Table 7: Liability for unauthorised transactions April 1998 to March 1999

Customer's liability (for at least part of the loss)	
1. Customer liability limited to $50 (s.5.5)	675
2. Customer negligent with PIN (s.5.6)	7901
3. Unreasonable delay in notification of loss or theft of card etc(s.5.7)	169
4. Other:	
(a) Reported initially as unauthorised due to confusion over processing date or merchant name:	8168
(b) ATM deposit shortfall	171
(c) Investigation terminated:	945
(d) Evidence of fraud or other offence:	240
Total all types of consumer liability liability	**18,269**

Issuer liable	
1. Settled without formal investigation	4241
2. Breach of Code by Institution (s11.10)	62
3. Conduct by employees of institution	
(a) Negligent conduct by employees of institution (s5.2(i))	7
(b) Fraudulent conduct by employees of institution (s5.2(i))	0
4. Conduct by employees/agents of merchants	
(a) Negligent conduct by employees/agents of merchants (s5.2(i))	28
(b) Fraudulent conduct by employees/ agents of merchants (s5.2(i))	10
5. Cards forged, faulty, expires or cancelled (s5.2(ii))	119
6. Losses occurred before cardholder received card or PIN (s5.2(iii))	185
7. Losses occurred after notification of loss or theft of card etc (s5.3)	257
8. Losses where it is clear neither the cardholder nor issuer contributed to loss (s5.4)	4750
Total, all types of issuer liability	**9659**

Training methods

ASIC also monitors staff training on the requirements and scope of the EFT Code. The EFT Code actively requires that institutions establish internal arrangements to ensure that staff receive adequate training on the requirements of the Code. Each institution is then required to report to ASIC on the training methods adopted.

During the reporting period, all institutions reported on procedures manuals that would be available to staff to promote knowledge and awareness of the provisions of the EFT Code. In addition, institutions reported that EFT Code training would be provided 'on-the-job' through team meetings or in the course of dealing with issues involving provisions of the EFT Code, and through internal testing. Some institutions also reported that external training was available for staff from time to time.

EFT security guidelines

In 1992, the APSC released Guidelines for EFT Security which addressed four key areas of EFT security — namely:

- the citing of EFT devices were PIN entry is required
- EFT customer education
- management of cryptographic keys for the protection of transactions, and
- communications security.

Card issuers were asked to incorporate the security guidelines into their EFT procedures and control systems and to report to the APSC on their implementation and suitability. ASIC has adopted the same implementation assessment document devised by the APSC for the first reporting period.

The implementation assessment document is included in the monitoring process. Institutions that have adopted the Guidelines are asked 12 questions which address the ongoing suitability of the Guidelines. In respect of each of the four guidelines, card issuers are asked whether:

- the Guideline has been adopted as policy
- it has been incorporated in procedures and processes and
- if further action in relation to the Guideline is proposed.

In the current reporting period, 52 institutions responded to the Guidelines assessment:

- Most of the card issuers indicated that the relevant Guidelines had been adopted as policy and incorporated into internal procedures and processes.
- A few institutions have indicated that further action is planned in respect of the Guidelines. This includes upgrading equipment and addressing a specific security requirement.

Table 8: Adoption of EFT security guidelines April 1998 to March 1999

Responses	*Yes*	*No*	*Not applicable*
Citing of EFT devices			
Adoption of guideline	40	1	11
Incorporation of guideline	40	1	11
Further action	4	36	12
EFT customer information			
Adoption of guideline	49	0	3
Incorporation of guideline	49	0	3
Further action	9	40	3
Cryptographic keys			
Adoption of guideline	48	0	4
Incorporation of guideline	46	1	5
Further action	5	43	4
Communications security			
Adoption of guideline	46	0	6
Incorporation of guideline	44	2	6
Further action	4	43	5

Almost all of the institutions have adopted the relevant guidelines as policy and incorporated them in their procedures, controls and internal assessment processes. Some of the smaller institutions had not fully adopted the changes although are considering full adoption within the next reporting period. ASIC will continue to monitor these developments within the next twelve months.

Most institutions recognise the need of guaranteeing security for EFT transactions, and continue to monitor the ongoing safety of existing equipment or controls to enhance security. During the next 12 months, ASIC will consider whether the EFT Guidelines need to be reviewed in line with the recommendation of Treasury and the ACCC in the review.

EFT Code: participating card issuers

Adelaide Bank
Australia and New Zealand Banking Group
Bank of New Zealand
Bank of Queensland
BankWest
Bendigo Bank
Citibank
Colonial State Bank
Commonwealth Bank of Australia
HongkongBank of Australia
Macquarie Bank
National Australia Bank
St George Bank
Suncorp-Metway
Trust Bank Tasmania
Westpac Banking Corporation
American Express International
Australian Guarantee Corporation
Avco Access
Armidale Building Society
Bananacoast Community Credit Union
Bass & Equitable Building Society
Broadway Credit Union
Capricornia Credit Union
Coastline Credit Union
Credit Union Services Corporation (Australia)
Diners Club International
First Australian Building Society
Greater Building Society (includes Greater Credit Union)
Herald Credit Co-operative
Heritage Building Society
Home Building Society
Hume Building Society
Hunter United Employees' Credit Union
Illawarra Mutual Building Society
IOOF Building Society
Mackay Permanent Building Society
Maitland Mutual Building Society
Newcastle Permanent Building Society
Phoenix (NSW) Credit Union
Pioneer Permanent Building Society
Police Association Credit Co-operative
Qantas Staff Credit Union
Queensland Country Credit Union
Queensland Police Credit Union
Queensland Professional Credit Union
Territory Mutual Building Society

The Rock Building Society
Upper Hunter Credit Union
Warwick Credit Union

Electronic Funds Transfer Code of Conduct

Part A:

Procedures to govern the relationship between the users and providers of Electronic Funds Transfer (EFT) Systems

1. COVERAGE

1.1 This Code applies to transactions intended to be initiated by an individual through an electronic terminal by the combined use of an EFT card and a personal identification number (PIN).

2. AVAILABILITY AND DISCLOSURE OF THE TERMS AND CONDITIONS OF USE APPLICABLE TO EFT TRANSACTIONS

2.1 Card-issuers will issue clear and unambiguous Terms and Conditions of Use which reflect the requirements of this Code; in particular, the clauses which deal with the cardholder's liabilities and responsibilities should be clearly and simply stated and highlighted in the text. The Terms and Conditions of Use are to include a warranty that the requirements of this Code will be complied with.

2.2 Card-issuers will encourage their cardholders to read and to be aware of the EFT Terms and Conditions; copies are to be readily available at all their branches, particularly when applications for EFT facilities are made by prospective cardholders, and the availability of terms and conditions is to be publicised by card-issuers. Card-issuers will provide a copy of the Terms and Conditions:

(i) with the notice of acceptance of the application for EFT facilities, or with the initial issue of the card or PIN to enable access to EFT facilities; and

(ii) on request.

2.3 Card-issuers will ensure that, before an EFT card is first used the cardholder has been provided with documentation on:

(i) any charges for the issue or use of an EFT card and PIN, separate from activity or other charges applying to the account generally;

(ii) the nature of any restrictions imposed by the card-issuer on the use of the EFT card (including withdrawal and transaction limits) and an indication that merchants or other institutions may impose additional restrictions;

(iii) a description of the types of transactions that may be made, and of the accounts that may be accessed, with the EFT card;

(iv) a description of any credit facility which may be accessed by the cardholder through an electronic terminal;

(v) the procedure for reporting the loss or theft of an EFT card (including the telephone number for reporting lost or stolen EFT cards outside of normal business hours); and

(vi) 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 Card-issuers wishing to vary or modify the EFT Terms and Conditions to:

(i) impose or increase charges relating solely to the use of an EFT card and PIN, or the issue of an additional or replacement card;

(ii) increase a cardholder's liability for losses relating to EFT transactions (subject to the liability limits established elsewhere in this Code); or

(iii) adjust the periodic transaction limits applying to the use of an EFT card;

will provide written notification to the cardholder, and allow a period of notice of at least 30 days before the change takes effect.

3.2 Card-issuers will advise other changes in advance either through:

(i) notices on, or with periodic account statements;

(ii) notices on EFT terminals or in branches; or

(iii) press advertisements.

Where (ii) and (iii) are used, subsequent written advice will be provided to customers at the time of their next account statements.

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 Card-issuers will issue a single document providing a consolidation of variations made to the Terms and Conditions.

3.5 When Card-issuers advise cardholders of an increase in the periodic transaction limit, they should, at the same time, advise cardholders that an increase in the periodic transaction limit may increase cardholder liability in the case of unauthorised transactions. This advice is to be clear and prominent.

4. PAPER RECORDS OF EFT TRANSACTIONS

A RECEIPTS AT ELECTRONIC TERMINALS

4.1 Card-issuers may choose to provide cardholders with the option to specify that a receipt is not required. At the time of an EFT transaction, and unless a cardholder specifically elects otherwise a receipt is to be 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', (codes may be used only if they are explained on the receipt);

(iv) an indication of the account(s) being debited or credited;

(v) data that enable the card-issuer to identify the customer and the transaction;

(vi) the general location of the terminal used to make the transaction or a number or code that enables that terminal to be identified;

(vii) in the case of an EFTPOS terminal receipt, the name of the merchant to whom payment was made; and

(viii) in the case of accounts accessed at an ATM, the balance of the account where possible.

B PERIODIC STATEMENTS

4.2 For an account, other than a passbook account, to or from which EFT transactions can be made, the account holding institution will provide a record of account activity at least every six months. Cardholders are also to be offered the option of receiving more frequent periodic statements. That option is to be brought to the attention of the cardholder at the time the card is first issued. As well, statements are to be available at the request of the cardholder.

4.3 The statement is to show:

(i) in respect of each EFT transaction occurring since the previous Statement:

— the amount of the transaction;

— the date the transaction was debited or credited to the account;

— the type of transaction;

— the receipt number, or other means, which will enable the account entry to be reconciled with a transaction receipt;

(ii) any charges relating solely to the use of an EFT card and PIN (identified as a separate item); and

(iii) the address or telephone number to be used for inquiries concerning the account or to report any errors in the statement.

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

C SECURITY ADVICE

4.5 Card-issuers must include on or with account statements at least annually a clear, prominent and self-contained statement summarising card and PIN security requirements.

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 cardholder. It does not apply to any transaction carried out by the cardholder or by anyone performing a transaction with the cardholder's knowledge and/or consent.

B NO CARDHOLDER LIABILITY IN RESPECT OF FRAUDULENT OR NEGLIGENT CONDUCT OF CARD-ISSUERS' EMPLOYEES OR AGENTS; FORGED, FAULTY, EXPIRED OR CANCELLED CARDS; LOSSES OCCURRING PRIOR TO RECEIPT OF CARD OR PIN; OR INCORRECT DOUBLE DEBIT TRANSACTIONS

5.2 The cardholder has no liability for:

(i) losses that are caused by the fraudulent or negligent conduct of employees or agents of the card-issuer or companies involved in networking arrangements or of merchants who are linked to the EFT system or of their agents or employees.

(ii) losses relating to cards that are forged, faulty, expired, or cancelled.

(iii) losses occurring before the cardholder has received his or her card and PIN. In any dispute about receipt of the card or PIN it is to be presumed that the item was not received by the cardholder, unless the card-issuer can prove otherwise. The card-issuer can establish that the cardholder did receive the card and PIN by obtaining an acknowledgment of receipt of the card and PIN from the cardholder whenever a new card and associated PIN are issued. If the card and/or PIN was sent to the cardholder by mail, the card-issuer is not to rely only on proof of delivery to the cardholder's correct address as proof that the card and/or PIN was received by that person. Nor will the card-issuer have any term in the Terms and Conditions of Use which deems a card or PIN sent to the cardholder at that person's correct address to have been received by the cardholder within a certain time after posting.

(iv) losses that are caused by the same transaction being incorrectly debited more than once to the same account.

C NO CARDHOLDER LIABILITY IN RESPECT OF UNAUTHORISED TRANSACTIONS OCCURRING AFTER NOTIFICATION

5.3 The cardholder has no liability for losses resulting from unauthorised transactions occurring after notification to the card-issuer that the card has been misused, lost or stolen or that PIN security has been breached.

D NO CARDHOLDER LIABILITY WHERE IT IS CLEAR THAT THE CARDHOLDER HAS NOT CONTRIBUTED TO THE LOSS

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

E CIRCUMSTANCES WHERE THE CARDHOLDER IS LIABLE

5.5 Where it is unclear whether or not the cardholder has contributed to losses resulting from unauthorised transactions, the cardholder's liability is not to exceed the lesser of:

(i) $50 (or such lower figure as may be determined by the card-issuer); or

(ii) the balance of the cardholder's account(s) including any prearranged credit); or

(iii) the actual loss at the time the card-issuer is notified of the loss or theft of the card.

In determining if it is unclear whether a cardholder has contributed to the loss, the card-issuer will consider all reasonable evidence, including all reasonable explanations for the transaction occurring.

The fact that the account has been accessed with the correct PIN, while significant, will not of itself be conclusive evidence that the cardholder has contributed to the loss.

5.6 Where the cardholder has contributed to losses resulting from unauthorised transactions by

- voluntarily disclosing the PIN to anyone, including a family member or friend; or
- indicating the PIN on the card; or

- keeping a record of the PIN (without making any reasonable attempt to disguise the PIN) with any article carried with the card or liable to loss or theft simultaneously with the card;

the cardholder is liable for the actual losses which occur before the card-issuer is notified that the card has been misused, lost or stolen or that PIN security has been breached, except for:

(i) that portion of the losses incurred on any one day which exceed the daily transaction limit applicable to the card or account(s); or

(ii) that portion of the total losses incurred which exceed the balance of the cardholder's account(s) (including any prearranged credit).

5.7 Where the cardholder has contributed to losses resulting from unauthorised transactions by unreasonably delaying notification of the misuse, loss or theft of the card, or that the PIN has become known to someone else; the cardholder is liable for the actual losses which occur between when the cardholder became aware (or should reasonably have become aware in the case of a lost or stolen card) and when the card-issuer was actually notified, except for:

(i) that portion of the losses incurred on any one day which exceed the daily transaction limit applicable to the card or account(s); or

(ii) that portion of the total losses incurred which exceed the balance of the cardholder's account(s) including any prearranged credit).

F NOTIFICATION OF THE LOSS, THEFT OR UNAUTHORISED USE OF CARDS OR PINS

5.8 Card-issuers will provide an effective and convenient means by which cardholders can notify a lost or stolen card or unauthorised use of a card or PIN; facilities such as telephone hot lines are to be available to cardholders at all times, with notice by telephone being an effective notice for limitation of the cardholder'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 card-issuer providing notification is made to the card-issuer within a reasonable time of the facility again becoming available.

5.9 Card-issuers will implement procedures for acknowledging receipt of notifications, including telephone notifications, by cardholders of the loss theft, or unauthorised use of cards or PINs. Such acknowledgments need not be in writing although they must provide a means by which cardholders can verify that they have made a notification and when such notification was made.

6. LIABILITY IN CASES OF SYSTEM OR EQUIPMENT MALFUNCTION

6.1 Card-issuers will be responsible to their cardholders for loss caused by the failure of an EFT system or equipment to complete a transaction accepted by a terminal in accordance with the cardholder's instructions.

6.2 The card-issuer is not to deny, implicitly or explicitly, a right to the cardholder to make claims for consequential damage which may arise as a result of a system or equipment malfunction however caused, except, where the cardholder should have been aware that the system or equipment was unavailable for use or malfunctioning, the card-issuer's responsibilities may be limited to the correction of any errors in the cardholder's account, and the refund or any charges or fees imposed on the cardholder as a result.

7. DEPOSITS AT ELECTRONIC TERMINALS

A DISCREPANCIES BETWEEN RECORDED DEPOSITS AND AMOUNTS RECEIVED

7.1 Where, in relation to a deposit of funds at an electronic terminal, there is a discrepancy between the amount recorded as having been deposited and the amount recorded as having been received, the cardholder 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 ELECTRONIC TERMINALS

7.2 The security of deposits received at electronic terminals is the responsibility of the financial institution receiving the deposit from the time the transaction at the electronic terminal 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 and other organisations offering EFT facilities to cardholders, as well as merchant acquirers and card-issuers. Merchant acquirers are the financial institutions which are responsible for the transmission to the card-issuers of value which has been captured by an electronic terminal.

8.2 Card-issuers may not avoid any obligations owed to their cardholders 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 A card-issuer shall not require its cardholders 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 their 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 card issuer concerned of the situation.

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

The card-issuer will provide to the cardholder, upon inquiry, any further details required by the cardholder concerning the transaction correction appearing on the cardholder's statement.

9. AUDIT-TRAILS

9.1 Card-issuers will ensure that their electronic transfer systems generate sufficient records to enable transactions to be traced, checked and where an error has occurred, to be identified and corrected.

10. PRIVACY

10.1 Card-issuers are to be guided by the following principles in respect of all EFT services they offer and in respect of all accounts from which EFT transactions can be made:

(i) customer records are to be treated in the strictest confidence;

(ii) no person other than an employee or agent of the financial institution which maintains the account, and the customer or any person authorised by the customer is to have access through an electronic terminal to information concerning the customer's account;

(iii) except where it is being operated by an employee or agent of the financial institution concerned no electronic terminal is to be capable of providing any information concerning a customer's account unless the request for information is preceded by the entry of the correct card/PIN combination for that account; and

(iv) except where it is provided pursuant to a legal duty or responsibility, no information concerning the use of EFT services by a customer is to be provided by any financial institution, except with the consent of that customer.

10.2 Where cameras may be used to monitor transactions Card-issuers are to display at each automatic teller machine terminal a sign indicating that transactions conducted at the terminal may be photographed.

11. COMPLAINT INVESTIGATION AND RESOLUTION PROCEDURES

11.1 The card-issuer is to establish appropriate procedures for the investigation and resolution of any complaint by a cardholder concerning matters covered by this Code. Such procedures are to contain at least the features specified in this clause.

11.2 The card-issuer will establish formalised procedures for the lodgment of complaints by cardholders. Card-issuers will provide advice in their documentation, including in their Terms and Conditions of Use, on the means and procedure to lodge a complaint and to have the matter investigated. Cardholders have the responsibility to disclose all relevant information available to them regarding matters which are the subject of complaints.

11.3 When a cardholder lodges a complaint and the matter is not immediately settled to the satisfaction of both cardholder and card-issuer, the card-issuer will advise the cardholder in writing of the procedures for the investigation and resolution of the complaint.

11.4 The card-issuer'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. Where a cardholder raises a complaint concerning the authorisation of a transaction, the card-issuer will obtain from the cardholder at least the information outlined in the attached schedule where such information is relevant and available.

11.5 The card-issuer will within 21 days of receipt from the cardholder of the relevant details of a complaint either complete its investigation and advise the cardholder in writing of the outcome or advise the cardholder in writing of the need for more time to complete its investigation. The card-issuer will, unless there are exceptional circumstances which it will advise the cardholder in writing, complete its investigation within 45 days of receipt from the cardholder of the relevant details of a complaint.

11.5a Where an investigation continues beyond 45 days, card-issuers will provide to the cardholder monthly updates on the progress of the investigation and a date when a decision can be reasonably expected, except in cases where the card-issuer is waiting for a response from the cardholder and the cardholder has been advised that the card-issuer requires such a response.

11.5b Where a card-issuer is a party to an industry dispute resolution scheme, and that scheme provides that a matter may be heard by the scheme if the card-issuer concerned does not give a final decision on that matter within a specific time limit, the card-issuer will advise cardholders in writing, and within five business days after the relevant time period expiring, about the option of taking the matter to the industry scheme.

11.6 On completing its investigation of a complaint the card-issuer will promptly advise the cardholder of the outcome of the investigation together with reasons for that outcome including references to relevant clauses of this Code as reflected in the card-issuer's Terms and Conditions of Use.

Such advice is to be in writing except where the complaint is settled immediately the card-issuer receives the complaint to the satisfaction of both the cardholder and card-issuer.

11.7 Where, as a result of the investigation of a complaint, a card-issuer discovers that the cardholder's account has been incorrectly credited or debited (having regard to the appropriate allocation of liability under clauses 5 or 6 of this Code as reflected in the card-issuer's Terms and Conditions of Use) the card-issuer will, where appropriate, forthwith adjust the cardholder's account(including appropriate adjustments for interest and/or charges) and notify the cardholder in writing of the amount with which his/her account has been debited or credited as a result.

11.8 Where, in the card-issuer's view of the appropriate allocation of liability, the cardholder is liable under clauses 5 or 6 of this Code for at least part of the amount of the transaction subject to complaint:

(i) the card-issuer is to make available to the cardholder copies of any documents or other evidence relevant to the outcome of its investigation including information from the log of the transaction;

(ii) the card-issuer is also to refer to the systems log to establish whether there was any system malfunction at the time of the transaction and advise the cardholder in writing of the outcome of its inquiry

11.9 The card-issuer's procedures will provide for:

(i) written advice from the card-issuer to the cardholder that the card-issuer's initial decision in relation to a complaint will be reviewed by the card-issuer's senior management upon request by the cardholder; and

(ii) written advice from the card-issuer to the cardholder of the external avenues of complaint resolution that exist, including the relevant industry dispute resolution scheme and its contact details. Where the card-issuer is not a member of an industry dispute resolution scheme, cardholders should be advised of the existence of Consumer Affairs Agencies and Small Claims Courts/Tribunals.

Advice about the external avenues of complaint resolution will be provided to the cardholder at least at the time referred to in clause 11.5b and at the time when the card-issuer advises the cardholder of its final decision, made by its senior management, in respect of a complaint made by the cardholder, and that final decision does not satisfy the cardholder's claim in whole or in part.

11.10 Where the card-issuer, its employees or its agents fail to observe the allocation of liability, and complaint investigation and resolution procedures, as set out in clauses 5, 6 and 11 of this Code; and where such failure prejudiced the outcome of the complaint or resulted in unreasonable delay in its resolution, the card-issuer will be liable for the full amount of the transaction which is the subject of the complaint by the cardholder.

11.11 The card-issuer 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 B of this Code.

Part B:

Administration and review

12. ADMINISTRATION

12.1 Card-issuers, or their representative associations, will report to the Commonwealth Government annually on compliance with this Code as outlined in clauses 12.2 and 12.3.

12.2 Card-issuers and/or their associations will report in accordance with the reporting guidelines for the industry sector, on compliance with this Code.

12.3 Card-issuers will establish administrative arrangements to ensure their staff receive adequate training on the requirements of this Code. Card-issuers and/or their associations will also report on initiatives in training staff in understanding and implementing the Code.

13. REVIEW

13.1 Periodic reviews of the requirements of the Code, including the administrative arrangements set out in section 12, will be undertaken by the Commonwealth Government in consultation with Card-issuers and their respective associations, relevant State and Territory government agencies and consumer representatives.

SCHEDULE TO CODE

Information to be obtained where available and relevant from cardholders making a complaint concerning the authorisation of an EFT transaction as required under clause 11.4.

1. Card type and account number
2. Name and address of cardholder
3. Principal card/additional card
4. Whether card signed
5. Whether card lost or stolen
   - date of loss,
   - time report to card-issuer,
   - time, date, method of reporting reported to police, time, date
6. PIN details
   - was record of PIN made
     a) how recorded
     b) where kept
   - was record of PIN lost or stolen
     a) date of loss, time
   - has PIN been disclosed to anyone
7. How loss occurred (eg housebreaking, stolen purse/wallet)
8. Where loss of card occurred, eg office, home
9. Details of transaction to be investigated
   - description, date, time, amount
   - source, ATM/ EFTPOS
10. Details of any
    - circumstances surrounding the loss or theft of the card or record of the PIN, or the reporting of such loss or theft; or
    - steps taken to ensure the security of the card or PIN;

    which the cardholder considers relevant to his/her liability in respect of the transaction
11. Details of last valid transaction

EFT Checklist

Part A
Australian Securities & Investments Commission
EFT Code of Conduct Checklist

Part B
Australian Securities & Investments Commission
Guidelines for EFT Security Implementation Assessment

Part C
Australian Securities & Investments Commission
Complaint Resolution Assessment

Insert Institution Name Here:

…….....…….....

As at: 31 March 1999

Part A
Australian Securities & Investments Commission
EFT Code of Conduct Checklist

*[**Please Note**: Questions **3(a), 9(a), 17(a), 27(a)(i) &(ii) , 27(b) and 29(a)** are only to be answered by institutions that have adopted the recommended changes to the EFT Code within the current reporting period]*

This check-list is designed to help institutions ensure that they have conformed with all aspects of the Code of Conduct.

There will inevitably be questions to which, for one reason or another, unequivocal responses cannot be given. Where this is the case, please provide separate qualifications and explanations.

Note: Questions 23-32, 36 and 37 concern institutions' internal systems and procedures. When answering those questions, institutions' internal auditors should ensure both that those systems and procedures:

. have been clearly spelled out; and

. that normal auditing procedures have not disclosed any material weakness in their implementation during the past year.

Where responses indicate the need for corrective action in order to conform with the Code, details of proposed changes, including a timetable, should be given.

You should return to your industry organisation or the Australian Payments System Council a completed check-list, <u>together with a covering letter from a senior executive of your organisation</u>:

. certifying that your internal auditors are satisfied that your organisation has conformed with the Code and, where it has not been able to do so, what is being done to rectify this;

. including any commentary necessary to qualify or clarify responses; and

. the completed statistical return.

	YES	NO

SECTION 1: INFORMATION DISCLOSURE

Terms and Conditions

1.	Have you reached agreement on your Terms and Conditions of Use document with the Trade Practices Commission and Treasury? **(Please attach a copy of your Terms and Conditions.)**		

Documents available to cardholders

2.	Have you provided copies of the Terms and Conditions of Use document to cardholders:		
	. with the notice of acceptance of the application for an EFT card or with the card/PIN?		
	. on request?		
3.	Are they readily available at all your branches?		
3(a)	**NEW EFT CODE QUESTION** **Have you publicised the availability of your Terms and Conditions of Use document?**		
4.	Do you impose any charges for the issue or use of an EFT card and PIN (separately from activity or other charges applying to the account generally)?		
	If so, before new EFT cards were first used, did you also provide copies of document(s) to cardholders indicating such charges?		
5.	Before new EFT cards were first used, did you also provide copies of document(s) to cardholders indicating:		
	. the nature of any restrictions imposed by you on the use of the EFT card (including withdrawal and transaction limits)?		
	. that merchants and other institutions may impose additional restrictions?		

		YES	NO
6.	Did these or other documents you provided to cardholders describe:		
	. the types of transactions that may be made, and the accounts that may be accessed using their EFT card?		
	. credit facilities which may be accessed by the cardholder through an electronic terminal?		
7.	Did the documents you provided to new cardholders also:		
	. explain what they should do to report the loss, theft or unauthorised use of an EFT card?		
	. include a telephone number for use outside normal business hours to report loss, theft or unauthorised use of an EFT card?		
	. explain how cardholders can lodge complaints (including queries about entries on a periodic statement) and have these investigated?		
8.	Has your system for acknowledging receipt of notifications, including by telephone, of lost, stolen or unauthorised use of cards, operated throughout the whole of the year?		
	Changing the Terms and Conditions of Use		
9.	Did you give cardholders written notice of at least 30 days of any changes or modifications to your EFT Terms and Conditions which:		
	. imposed or increased charges relating solely to the use of an EFT card and PIN, or to the issue of an additional or replacement card?		
	. increased a cardholder's liability for losses relating to EFT transactions?		
	. adjusted the periodic transaction limits applying to the use of an EFT card?		
		YES	**NO**

9(a)	**NEW EFT CODE QUESTION** **When advising cardholders of an increase in periodic transaction limits, did you, at the same time, advise them in a clear and prominent fashion, that such an increase may increase their liability in the case of unauthorised transactions?**		
10.	Did you make any changes to the Terms and Conditions of Use, other than those mentioned in Question 9, known to the cardholders in advance?		
	. If yes, did you do so by: including a notice on, or with, periodic account statements sent to them; placing notices on EFT terminals or in branches; or placing advertisements in newspapers?		
11.	Did you subsequently follow up any changes made known to cardholders by placing notices on terminals, or in branches, or in newspapers, with written notices on account statements?		
12.	Were there a significant number of changes made to your Terms and Conditions in the past 12 months?		
	If so, did you reprint your Terms and Conditions?		
	Paper records of EFT transactions		
13.	Except in case of malfunction of the receipt issuing mechanism, are receipts issued for all EFT transactions unless customers specifically elect otherwise at the time of the transaction?		
14.	Did transaction receipts issued by your ATMs and EFTPOS terminals show:		
	. the amount of the transaction?		
	. the date of the transaction?		
	. the time (if practicable) of the transaction?		
		YES	**NO**
	. the type of transaction, e.g. a deposit, withdrawal, transfer? (Codes may be used only if they are explained on the receipt.)		

	. the account(s) being debited or credited?		
	. information that would enable you to identify the customer and the transaction?		
	. the location of the terminal used to make the transaction, or a number or code that enables that terminal to be identified?		
15.	In the case of EFTPOS terminal receipts, did they also show the name of the merchant to whom payment was made?		
16.	In the case of accounts accessed at an ATM, where possible, did receipts show the balance of the accounts after the transactions?		
17.	Did you send a statement or record of account activity to cardholders at least every six months?		
17(a)	**NEW EFT CODE QUESTION** **Did you include on or with the statement or record of account activity, at least, annually, a clear, prominent and self-contained statement summarising card and PIN security requirements?**		
18.	Did you also give cardholders the option to receive statements:		
	. more frequently?		
	. on request?		
	Did you inform new cardholders of these options when the card was first issued?		
19.	Did customer statements show for each EFT transaction made since the previous statement:		
	. the amount of the transaction?		
		YES	**NO**
	. the date the transaction was debited or credited to the account?		
	. the type of transaction?		

. the receipt number, or other means, which will enable the cardholder to reconcile the account entry with a transaction receipt?		
. (as a separate item) any charges relating solely to the use of an EFT card and PIN?		
20. Did these periodic statements include:		
. suggestions to cardholders that they should check all entries on the statement and promptly notify you of any apparent error or possible unauthorised transaction?		
. an address or telephone number to be used for enquiries concerning the account or to report any errors in the statement?		
21. Did you conform with the Code's requirement that there should be no restrictions on cardholders' rights to make claims or any time limits for cardholders to detect errors or unauthorised transactions and report these to you?		

SECTION 2: COMPLAINT INVESTIGATION AND RESOLUTION PROCEDURES

22. Have you completed the statistical return on complaints and dispute resolution in Attachment 1?		
23. Did you have procedures to inform complainants about:		
. what steps you will take to investigate and to resolve complaints?		
. their responsibility to disclose all information relevant to the disputed transaction?		
	YES	**NO**
24. In the case of complaints which were not immediately settled to the satisfaction of both you and the cardholder, were your staff required to advise cardholders in writing of the procedures for the investigation and resolution of the complaint?		

25.	In the case of complaints of unauthorised transactions, were your staff required to obtain from complainants, where available and relevant, the information shown in Attachment 2?		
26.	Did your dispute resolution procedures require you to consider all information relevant to disputed transactions before deciding how liability should be allocated?		
27.	Has it been the practice, except where a complaint is settled immediately it is received to the satisfaction of both you and the cardholder, that staff;		
	write to cardholders within 21 days of receiving complaints to inform them **either of;**		
	- the outcome of your organisation's investigation; or		
	- that more time has been needed to complete investigations?		
	complete all investigations within 45 days of receiving a complaint unless there were exceptional circumstances of which you advised the cardholder in writing?		
	. write to cardholders informing them of the reasons for your decision in terms of the relevant parts of your Terms and Conditions of Use document?		
27(a)	**NEW EFT CODE QUESTION** **If the investigation continued beyond 45 days, did you provide the cardholder with:** (1) **monthly updates of its progress; and** (2) **a date when a decision can reasonably be expected?**		
27(b)	**NEW EFT CODE QUESTION** **Were you a party to an industry dispute resolution scheme that provides that a matter may be heard by the scheme if the card issuer does not give a final decision within a specified time limit?**	**YES**	**NO**
28.	If, as a result of investigations, cardholders have been held liable for at least part of any amount of a transaction in dispute, did your procedures require you to write to the cardholders including:		

. copies of documents or other evidence that you have that are relevant? _____ _____

. the outcome of your inspection of the system's log to establish whether there had been a system malfunction at the time of the transaction? _____ _____

29. Given the outcome as in Question 28, did your procedures require you to write to the cardholders and inform them that, if they are not satisfied:

. they can ask for the result to be reviewed by your senior management? _____ _____

. they can take the complaint to outside bodies such as Consumer Affairs Departments, Small Claims Tribunals or the Banking Industry Ombudsman? _____ _____

29(a) NEW EFT CODE QUESTION
Given the outcomes as in Question 28, did your procedures require you to write to the cardholders and inform them that, if they are not satisfied they can take the complaint to external avenues of complaint resolution, including any relevant industry resolution scheme, Consumer Affairs or Fair Trading Agencies and Small Claims Courts/ Tribunals? _____ _____

30. If, as the result of an investigation, you concluded that you were liable, did your procedures require that you:

. adjust the cardholder's account as soon as possible (including appropriate adjustments for interest and/or charges)? _____ _____

. notify the cardholder in writing of any such adjustments? _____ _____

YES **NO**

31. Did you resolve complaints in the customer's favour if your staff did not comply with the Code? _____ _____

SECTION 3: PRIVACY

32. (a) customer records are to be treated in the strictest confidence?

(b) no person other than an employee or agent of the financial institution which maintains the account, and the customer, or any person authorised by the customer, is to have access through any electronic terminal to information concerning the customer's account?

(c) except where it is being operated by an employee or agent of the financial institution concerned, no electronic terminal is to be capable of providing any information concerning a customer's account unless the request for information is preceded by the entry of the correct card/PIN combination for that account?

(d) except where it is provided pursuant to a legal duty or responsibility, no information concerning the use of EFT services by a customer is to be provided by any financial institution, except with the consent of that customer?

33. Did you receive complaints about breaches of privacy in customers' EFT transactions and accounts?

If yes, please give details and measures taken to avoid recurrence:

……
……
……

34. Are cameras used to monitor transactions?

If so, are signs displayed at each ATM terminal indicating that transactions may be photographed?

INFORMATION ON STAFF TRAINING

35. Please indicate which of the following methods are utilised by your institution in EFT staff training and have the person with overall responsibility for staff training certify the response.

Training Initiatives

	YES	NO
. Procedures Manual detailing EFT requirements available to all relevant staff.		
. On the Job Training:		
- passive		
- video		
- active (e.g. team meeting)		
- testing		
. External Training		
. Resource Material Check-list		
- special handout		
- video		
- computer-based training		
. Other (please specify)		

	YES	NO

SECTION 5: MISCELLANEOUS

Deposits at electronic terminals

36. Did your procedures require staff, when verifying funds deposited at an electronic terminal, to notify cardholders as soon as possible of any discrepancy between the amount recorded as having been deposited and the amount recorded as having been received (at the same time stating the actual amount which has been credited to the nominated account)? _____ _____

Audit trails

37. Except in cases of malfunction, did your EFT systems generate sufficient records to enable transactions to be traced, checked and, where an error occurred, to be identified and corrected? _____ _____

Part B
Australian Securities & Investments Commission
Guidelines for EFT Security Implementation Assessment

Guide-line	Yes/No	Comments[1]
1. Siting of EFT devices where customer PIN entry is required: (a) Have you adopted this Guide-line as policy? (b) Have you incorporated this Guide-line into your procedures, controls and internal audit/assessment processes? (c) Are there any aspects of this Guide-line where further action is proposed?	....	.....
2. EFT customer education: (a) Have you adopted this Guide-line as policy? (b) Have you incorporated this Guide-line into your procedures, controls and internal audit/assessment processes? (c) Are there any aspects of this Guide-line where further action is proposed?	....	.....

[1] Comments from institutions will assist the Council in identifying any areas of difficulty in the implementation of the Guide-line and in assessing their on-going suitability.

Part C
Australian Securities & Investments Commission
Complaint Resolution Assessment

Guide-line	Yes/No	Comments[2]
3. Management of cryptographic keys for the protection of transactions: (a) Have you adopted this Guide-line as policy? (b) Have you incorporated this Guide-line into your procedures, controls and internal audit/assessment processes? (c) Are there any aspects of this Guide-line where further action is proposed?	....	.... … ....

[2] Comments from institutions will assist the Council in identifying any areas of difficulty in the implementation of the Guide-line and in assessing their on-going suitability.

B.	Transactions Complaints Resolution Data									
	TYPE	Total	+	Complaints held over	=	Issuer liable	+	Customer liable	+	Complaints outstanding
1.	**SYSTEM MALFUNCTION**									
	(a) ATM cash dispensing problem	_____		.....		.....		.....		.....
	(b) Other system malfunction (i.e. system failed to complete transaction in accordance with customer's instructions)	_____		.....		.....		.....		.....
	TOTAL	_____		_____		_____		_____		_____
2.	**UNAUTHORISED TRANSACTIONS**									
	(a) Card or PIN lost or stolen	_____		.....		.....		.....		.....
	(b) Card or PIN not lost or stolen	_____		.....		.....		.....		.....
	(c) Other	_____		.....		.....		.....		.....
	TOTAL	_____		_____		_____		_____		_____
	TOTAL COMPLAINTS (System Malfunction plus Unauthorised Transaction)	_____	+	_____	=	_____	+	_____	+	_____

C.	**Unauthorised transactions where customer liable for at least part of loss**	**Number**
	1. Customer liability limited to $50 (s5.5)	.....
	2. Customer negligent with PIN (s5.6)	.....
	3. Unreasonable delay in notification of loss or theft of card etc. (s5.7)	.....
	4. Other (a) Initially reported as unauthorised due to confusion over processing date or merchant name	.....
	(b) ATM deposit shortfall	.....
	(c) Investigation terminated (at customer's request or due to loss of contact)	.....
	(d) Evidence of fraud or other offence	.....
	TOTAL (Equals the total of "Customer liable" column in B2 above)	_____ _____

D.	**Unauthorised transactions where issuer liable**	**Number**
	1. Settled without formal investigation	.....
	2. Breach of Code by institution (s11.10)	.....
	3. (a) Negligent conduct by employees of institution (s5.2(i))	.....
	(b) Fraudulent conduct by employees of institution (s5.2(i))	.....
	4. (a) Negligent conduct by employees/agents of merchants (s5.2(i))	.....
	(b) Fraudulent conduct by employees/agents of merchants (s5.2(i))	.....
	5. Cards forged, faulty, expired or cancelled (s5.2(ii))	.....
	6. Losses occurred before cardholder received card or PIN (s5.2(iii))	.....
	7. Losses occurred after notification of loss or theft of card etc. (s5.3)	.....
	8. Losses where it is clear neither the cardholder nor issuer contributed to loss (s5.4)	.....
	TOTAL (Equals the total of "Issuer liable" column in B2 above)	_____ _____

Attachment 1

DATA ON COMPLAINTS AND DISPUTE RESOLUTION

Complaints about EFT transactions are defined as **all** complaints about matters falling within the EFT Code of Conduct where the issue of liability arises, or may arise, and include the following:

. ATM cash dispensing problems;

. other technical malfunctions resulting in failure to complete the transaction in accordance with the customer's instructions;

. unauthorised transactions, distinguishing whether the card or PIN was/was not lost or stolen; and

. all other complaints (excluding such matters as availability of ATMs etc.).

"Complaints" as defined are therefore wider than "disputes", i.e. those complaints which are not immediately settled.

"EFT transactions" relevant to your institution are transactions initiated through your own or others' electronic terminals (or devices) using a PIN and card and which affect the account balances of your customers. Transactions will include:

. ATM withdrawals and deposits;
. transfers between accounts;
. EFTPOS (or EFTPOB) payment and cash-out transactions; and
. cardphone transactions.

Transactions do not include:

. account enquiries;
. statement requests;
. PIN sessions; and
. those using pre-paid transaction cards.

Attachment 2

SCHEDULE TO CODE

Information to be obtained where available and relevant from cardholders making a complaint concerning the authorisation of an EFT transaction as required under clause 11.4.

1. Card type and account number.

2. Name and address of cardholder.

3. Principal card/additional card.

4. Whether card signed.

5. Whether card lost or stolen:

   . date of loss, time;

   . reported to card issuer, time, date

     method of reporting;

   . reported to police, time, date.

6. PIN details:

   . was record of PIN made

     - how recorded;

     - where kept;

   . was record of PIN lost or stolen

     - date of loss, time;

   . has PIN been disclosed to anyone.

7. How loss occurred (e.g. housebreaking, stolen purse/wallet).

8. Where loss of card occurred, e.g. office, home.

9. Details of transaction to be investigated:

   . description, date, time, amount;

   . source, ATM/EFTPOS.

10. Details of any:

    . circumstances surrounding the loss or theft of the card or record of the PIN, or the reporting of such loss or theft; or

    . steps taken to ensure the security of the card or PIN;

    which the cardholder considers relevant to his/her liability in respect of the transaction.

11. Details of last valid transaction.

Appendix 1
Example of compliance statement (Code of Banking Practice Statement of Compliance)

For the period ended 31 March 1999

Name of Institution:

In completing this statement, an institution is to have regard to all the products/services it offers which are covered by the Code. A separate statement is not required to be completed for each individual product/service.

To be completed by the Chief Executive or his/her nominee.

Part 1

For each product/service covered by the Code[3]:

Code of Banking Practice - Relevant Section	does your institution have documents &/or information which comply with the Code in relation to:		does your institution have procedures in place to enable compliance with the Code in relation to:		does your institution train appropriate staff in the requirements of the Code in relation to:	
	Itsar Office Use Only	(Yes/No/NA)	*Itsar Office Use Only*	(Yes/No/NA)	*Itsar Office Use Only*	(Yes/No/NA)
Part A - Disclosures						
Terms and conditions (s 2)	1.1		1.2		1.3	
Cost of credit (s 3)	2.1		2.2		2.3	
Fees & charges (s 4)	3.1		3.2		3.3	
Payment services (s 5)	4.1		4.2		4.3	
Operation of accounts (s 6)	5.1		5.2		5.3	
Part B - Principles of Conduct						
Pre-contractual conduct (s 7)	6.1		6.2		6.3	
Opening of accounts (s 8)	7.1		7.2		7.3	
Variation to terms & conditions (s 9)	8.1		8.2		8.3	
Account combination (s 10)			9.2		9.3	
Foreign exchange services (s 11)	10.1		10.2		10.3	
Privacy & confidentiality (s 12)	11.1		11.2		11.3	
Payment instruments (s 13)	12.1		12.2		12.3	
Statements of account (s 14)	13.1		13.2		13.3	
Provision of credit (s 15)			14.2		14.3	
Joint accounts & subsidiary cards (s 16)	15.1		15.2		15.3	
Guarantees (s 17)	16.1		16.2		16.3	
Advertising (s 18)	17.1		17.2		17.3	
Closure of accounts (s 19)			18.2		18.3	

[1] If for any question, a negative response is appropriate for one or more products/services, a negative overall response should be entered on this statement and details of the product(s)/service(s) which gave rise to that response attached.

Part C - Resolution of disputes

Dispute resolution (s 20)	19.1		19.2		19.3	

Part 2

Please attach responses to the following questions:

1. Is a system of internal assessment in place within your institution which monitors compliance with each of the Code's provisions and enables you to identify areas of non-compliance? Please provide a brief description of the overall system.

2. Has this internal assessment system identified any areas of recurrent non-compliance? (if yes, please provide a brief explanation along with details of corrective action; taken, under way or planned)

3. Could you provide a brief report on staff training, citing examples of the methods and materials used to train staff about the Code and its requirements and how these methods and materials vary according to staff function.

4. Are there any concerns you wish to raise regarding the operation of the Code?

Subject to any exceptions noted above and in any attachment, I certify that this institution is complying with the Code.
Signed on behalf of .....
Chief Executive/nominee[4] .....
Date: .....

[4] Nominee should be an appropriate, senior officer; please indicate position held.